Table of Contents

**Volume II Revisions**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smoking &amp; Tobacco Use Policy</td>
<td>3</td>
</tr>
<tr>
<td>Acceptable Use of College Computer and Network Systems Policy</td>
<td>3</td>
</tr>
<tr>
<td>Access Control Policy</td>
<td>5</td>
</tr>
<tr>
<td>Cloud Computing Policy</td>
<td>19</td>
</tr>
<tr>
<td>Computer Asset Disposal Policy</td>
<td>30</td>
</tr>
<tr>
<td>Computer Asset Replacement Policy</td>
<td>35</td>
</tr>
<tr>
<td>Electronic Accessibility Policy</td>
<td>40</td>
</tr>
<tr>
<td>Information Security Program Policy</td>
<td>42</td>
</tr>
<tr>
<td>Information Technology Change Control Policy</td>
<td>46</td>
</tr>
<tr>
<td>Mobile Device Use and Support Policy</td>
<td>56</td>
</tr>
<tr>
<td>Password Policy</td>
<td>63</td>
</tr>
<tr>
<td>Information Technology Maintenance Policy</td>
<td>71</td>
</tr>
<tr>
<td>Wireless Access Points Policy</td>
<td>76</td>
</tr>
<tr>
<td>Contact With Government Agencies Policy</td>
<td>82</td>
</tr>
<tr>
<td>Photography, Digital Recording, &amp; Filming Policy</td>
<td>88</td>
</tr>
<tr>
<td>Social Media Policy</td>
<td>90</td>
</tr>
</tbody>
</table>

**Volume III Revisions**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMLA Policy</td>
<td>105</td>
</tr>
<tr>
<td>Moving Expenses Policy</td>
<td>105</td>
</tr>
</tbody>
</table>

**Volume V Revisions**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Subjects Research Policy</td>
<td>115</td>
</tr>
</tbody>
</table>

**Proposed Policies**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>College Intern Policy</td>
<td>143</td>
</tr>
<tr>
<td>Admission of Applicants With Prior History of Criminal Behavior or Disciplinary Action for Conduct</td>
<td>149</td>
</tr>
<tr>
<td>Notice of Nondiscrimination Policy</td>
<td>152</td>
</tr>
<tr>
<td>Website Privacy Policy</td>
<td>153</td>
</tr>
<tr>
<td>Audit &amp; Accountability Control Policy</td>
<td>165</td>
</tr>
<tr>
<td>Configuration Management Policy</td>
<td>173</td>
</tr>
<tr>
<td>Personnel Security Policy</td>
<td>180</td>
</tr>
</tbody>
</table>
Data Classification Policy

Identification & Authentication Policy

Media Protection Policy

Information Security Awareness & Training Policy

Information Technology Physical & Environmental Protection Policy

Confidentiality of Library Records Policy

Reportable Business Relationships Policy

Secondary Assignments Policy
VOLUME II REVISIONS

SMOKING AND TOBACCO USE POLICY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>May 8, 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number:</td>
<td>II – 2.2.4</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>Smoking Policy</td>
</tr>
<tr>
<td>Issuing Authority:</td>
<td>President</td>
</tr>
<tr>
<td>Responsible Officer:</td>
<td>Associate Vice President for Human Resources and Compliance and Vice President for Student Affairs</td>
</tr>
<tr>
<td>Applicability:</td>
<td>All members of the Canisius College community.</td>
</tr>
<tr>
<td>History:</td>
<td></td>
</tr>
</tbody>
</table>

PURPOSE

The purpose of this policy is to assist in the creation of a healthy and comfortable environment for all students, employees, visitors, and any other members of the college community.

POLICY

It is the policy of Canisius College to provide a smoke and tobacco-free environment on campus. The use of smoking and tobacco products of any sort shall be prohibited on all college-owned and operated campus grounds, both indoors and outdoors. This smoking ban does not apply to public rights-of-way (sidewalks, streets) on the perimeter of the campus. Moreover, the sale, distribution, and sampling of all tobacco products and tobacco-related merchandise is prohibited on all college-owned and operated property and at college-sponsored events. Littering of campus property with the remains of any smoking products is similarly prohibited.

Canisius encourages all users of tobacco, in any form, to quit. Information on smoking cessation programs is available in the Student Health Center and Office of Human Resources, as well as via the Employee Assistance Program.

It is the responsibility of all members of the campus community to comply with this policy. Department supervisors are responsible for workplace administration of the policy. Complaints regarding employee and volunteer non-compliance should be directed to the violating employee or volunteer’s immediate supervisor. Complaints regarding student non-compliance should be directed to the vice president for student affairs, senior associate dean/director of student life, or designee. All other violators should be reported to Public Safety.

Any member of the college community can voice objections to smoking or tobacco use on campus in violation of this policy without fear of retaliation.

DEFINITIONS

*College-Owned and Operated Campus Grounds*—include, but are not limited to, all outdoor common and educational areas; all college buildings; college-owned on-campus housing; campus sidewalks; campus parking lots; recreational areas; outdoor stadiums; and college-owned and leased vehicles (regardless of location).
Smoking and Tobacco Use— means smoking or vaporizing any substance, including but not limited to, tobacco, cloves, or marijuana (e.g.,—the use or possession of a lighted cigarette, lighted cigar, lighted pipe, or any other lighted tobacco, clove or marijuana or smokeless tobacco product), or the use of an hookah, pipe, or electronic inhaler that employs a mechanical heating element, battery, or electronic circuit to heat a liquid nicotine solution contained in a vapor cartridge, such as an electronic cigarette, electronic cigar, electronic cigarillo, or electronic pipe.

Smoking and Tobacco Products—include, but are not limited to, all cigarette and tobacco products (cigarettes, cigars, bidis, kreteks, e-cigarettes, etc.), all smoke-producing products (cigars, hookah, pipe, or electronic inhaler that employs a mechanical heating element, battery, or electronic circuit to heat a liquid nicotine solution contained in a vapor cartridge, such as an electronic cigarette, electronic cigar, electronic cigarillo, or electronic pipe), and smokeless tobacco products.

PROCEDURES/GUIDELINES

Exceptions

Smoking and the use of tobacco products is permitted when traveling in a private vehicle through campus or parked on campus in an unenclosed parking lot while in a vehicle that is not owned or leased by the college.

Any product that has been approved or otherwise certified for legal sale by the United States Food and Drug Administration for tobacco use cessation or other medical purposes and is being marketed and sold solely for that approved purpose is also permitted.

Violations of Policy

Violations of this policy will result in the college taking appropriate disciplinary action against the violator. Disciplinary actions will be taken in accordance with the college’s policies and procedures that apply to the violator.

RELATED POLICIES

Community Standards
Residential Life Standards of Conduct
Owned or Leased Vans and Motor Vehicles Policy
ACCEPTABLE USE OF COLLEGE COMPUTER AND NETWORK SYSTEMS
POLICY

Effective Date: May 6, 2019
Policy Number: II – 2.4.1
Supersedes: Not Applicable.
Issuing Authority: President
Responsible Officer: Chief Information Officer

Applicability: All students, staff, faculty, contractors, consultants, and other workers at Canisius college, including all personnel affiliated with third parties. This policy applies to all college-owned or college-leased information systems, including but not limited to, computer and network systems, equipment.

History:

PURPOSE

The purpose of this policy is to outline the acceptable use of the college’s information systems, including but not limited to, its computer and network systems and to promote the efficient, ethical, and lawful use of the college’s electronic information systems and equipment.

POLICY

Canisius College information systems, including but not limited to its computer and network systems (hereinafter collectively referred to as “information systems”), are intended for use in college-related research, instruction, learning, enrichment, and administrative activities. Authorized Users must use only those information systems that they are authorized to use and are permitted to use them only in the manner and to the extent authorized. Ability to access such systems does not, by itself, imply authorization to do so. Authorized Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. See the Access Control Policy for additional information.

Further, the college expects college employees, students, and other Authorized Users to utilize the college’s computer and network information systems and resources in a lawful and responsible manner consistent with the college’s mission of education, research, and service. While the college makes its computer and network information systems available primarily for use in college-related research, instruction, learning, enrichment, and administrative activities, it realizes the need for personal use of its systems for the convenience of the campus community. Any personal use of these systems may not violate any college practice or policy, including but not limited to the
procedures and policy guidelines set forth in this policy. Moreover, the use of the college’s systems by employees for purposes unrelated to their college positions, however, must be limited and not interfere with their official responsibilities or college functions. It is the responsibility of college employees to consult their supervisors if they have any questions in this respect.

The college recognizes that Authorized Users may use personal devices when conducting college business or accessing the college’s computer and network information systems. Authorized Users are still responsible for following the Acceptable Use Policy when using personal devices. See also the Mobile Device and Support Policy for more information.

If an Authorized User is not clear as to what constitutes an appropriate use, the user should contact the college’s chief information officer to determine whether a particular activity is permissible.

DEFINITIONS

**Authorized User**—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

**Cardholder Data**—full magnetic stripe or the Primary Account Number (PAN) plus any of the following: cardholder name; expiration date; service code; CVC2/CVV2/CID (a three- or four-digit number displayed on the signature panel of the card or, in the case of American Express, on the face of the card.

**College Data**—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

**College Information System**—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

**College Information**—is any data related to the business of the college including, but not limited to: financial, personnel, student, alumni, communication, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. Examples include: credit card information; tax identification numbers; payroll information; check requests and associated paperwork; student, parent, and employee tuition; financial aid and loan accounts information; student educational records as defined by FERPA; photographic images (especially of face or other identifying characteristic); fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); medical or financial information for any employee, temporary worker, or student; other personal information to include date of birth, address, phone numbers, maiden names, customer numbers, social security numbers; college contracts; college research data; alumni and donor records; personnel records; college financial data; passwords; college proprietary information/data; and any other information for which access, use, or disclosure is not authorized by: a) federal, state, or local law; or b) college policy or operations.

**College Personnel**—Canisius College trustees, executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.
Computer and Network Systems—any college-owned or leased computer, mobile device, or software, as well as any part of the college’s computer, data, voice or video networks (including all information systems) physically located on any college owned, leased, or rented property or located on the property of any third-party with the permission of that party or the college. This includes devices on such networks assigned any routable and non-routable IP addresses and applies to the college’s wireless network and the network serving the college’s student residence housing and any other vendor supplied network made available to the college community.

 Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any Cardholder Data received in the course of business by the college, whether or not such Cardholder Data is covered by GLBA. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

 Data Custodians—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

 Data Owners—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

 Media—includes, but is not limited to, paper, hard drives, random access memory (RAM), read-only memory (ROM), disks, flash drives, memory devices, phones, Mobile Devices, networking devices, and all-in-one printers.

 Members of the College Community—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

 Mobile Device—any handheld or portable computing device including running an operating system optimized or designed for mobile computing, such as Android, Blackberry OS (RIM), Apple’s iOS, or Windows Mobile. Any device running a full desktop version operating system is not included in this definition.

 Non-Public Personal Information—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.
**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to this policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, Cardholder Data, and Sensitive Authentication Data. See the College Data Classification Policy for additional information.

**Public College Data**—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

**Sensitive Authentication Data**—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

**Software**—any programs used to operate computers and related devices. Software is frequently divided into two categories: system software and application software. System software includes the operating system and the utilities that enable the computer or device to operate. Application software consists of programs that perform productive work for users. Application software includes such items as word processors (e.g., Word, WordPerfect), spreadsheets (e.g.: Excel), graphic and data management programs (e.g.: Photoshop, Access), and statistical packages.

**Student Education Records**—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

**Users**—any individual granted access by Information Technology Services to a college computer and network system.

**PROCEDURES/GUIDELINES**
I. Conditions of Use

In using the college’s computer and network information systems, Authorized Users agree to the following conditions of use:

1. Authorized Users of the college’s information systems do so subject to applicable laws and the college’s policies and procedures;

2. The college will endeavor to safeguard the confidentiality of Authorized Users and the possibility of loss of information within the college’s information systems but will not be liable to the user in the event of any such loss. The user must take all reasonable measures to further safeguard against any loss of information within the college’s computer and network information systems;

3. Authorized Users of the college’s computer and network information systems recognize that when they cease to be formally associated with the college (e.g., no longer an employee, student, contractor, or visitor to the college), their information/data may be removed from the college’s computer and network information systems without notice. Exceptions will be reviewed by the chief information officer;

4. The college reserves the right to limit permanently or restrict any Authorized User’s usage of the college’s computer and network information systems; to copy, remove, or otherwise alter any information/data or system that may undermine the authorized use of the college’s computer and network information systems; and to do so with or without notice to the user in order to protect the integrity of the college’s computer and network information systems against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage;

5. The college, through authorized individuals, reserves the right to periodically check and monitor its computer and network information systems, including but not limited to the right to review, access, audit and monitor files/messages on Authorized Users’ assigned computers, mobile devices, and emails;

6. The college reserves the right to take emergency action to safeguard the integrity and security of its computer and network information systems. This includes but is not limited to the termination of a program, job, or on-line session, or the temporary alteration of Authorized User account names and passwords.

Canisius College disclaims any responsibility and/or warranties for information and materials residing on non-college computer and network information systems or available over publicly accessible networks, except where such responsibility is formally expressed. Such materials do not necessarily reflect the attitudes, opinions, or values of the college, its employees, or students.

II. Acceptable Uses

A. General Guidelines

General guidelines for the acceptable use of college information systems are based on the following principles and Authorized Users are expected to:

1. Behave in a manner consistent with the college’s mission and comply with all applicable laws, regulations, and college policies, as well as applicable licensing and contractual agreements:
2. Behave responsibly and respect the name of the college and the integrity and security of college information systems at all times;

3. Respect the rights and property of others, including privacy of person-to-person communication in all forms, including voice (telephone), text (electronic mail and file transfer), and images (graphics and video), confidentiality, and intellectual property (e.g., do not violate copyright laws or use software procured with academic use licenses for commercial applications or development, unless the license explicitly permits such use);

4. Use college information systems for the activities or purposes for which they are assigned (e.g., college information systems are not to be used for personal commercial purposes without written authorization from the college);

5. Guard against abuses that disrupt or threaten the viability of any college information systems, including those at the college and those on networks to which the college’s information systems are connected or accessible;
   a. Abuses include but are not limited to the use of unauthorized equipment such as wireless access points, wireless routers, cable routers, etc. or utilizing shared resources such as CPU cycles or network bandwidth to a degree that adversely impacts academic or research activities;

6. Comply with information technology security policies and associated controls employed by the college and protect assigned accounts and non-public College Data from unauthorized access by others; and

7. Report violations of this policy to the chief information officer.

If an Authorized User is not clear on what constitutes an appropriate use, the user is expected to contact Information Technology Services (“ITS”) to determine whether a particular activity is permissible.

B. Security Habits

In addition to the above, Authorized Users are expected to adhere to reasonable and necessary security habits when using college resources. These habits include:

1. Accessing Private College Data only to conduct college business and only as authorized by the applicable Data Owner;

2. Keeping account information, including passwords, confidential;

3. Logging out of computers or using a password-protected screensaver when leaving the office;

4. Running college-provided antivirus and antispyware software;

5. Installing operating system updates when prompted;

6. Using caution when opening email attachments and other unexpected data;

7. Storing Private College Data, whenever feasible, on a centrally managed server, rather than a local hard drive or portable device (see the Media Protection Policy);

8. In cases when an Authorized User must create or store Private College Data on a local hard drive or a portable device such as a laptop computer, tablet computer, smart phone, or other
mobile device, the Authorized User must ensure the data is encrypted in accordance with System and Communication Protection, Media Protection and Mobile Device Use and Support policies;

9. Encrypting Private College Data during transmission over an unsecured network:
   a. Email sent to and received from college email accounts are automatically encrypted. ITS provides tools and processes for Authorized Users to send encrypted data over unsecured networks to and from other locations;
   b. Authorized Users who store College Data using commercial cloud services must use services provided or sanctioned by College, rather than personally obtained cloud services;

10. Disconnecting devices determined by ITS to lack required security software or otherwise pose a threat to college information systems;

11. Returning all college information systems that are no longer being used productively for college business to ITS for reallocation, repair, or disposal.

12. Authorized Users may not directly give, lend, rent, donate, or dispose of college information systems. See also the Media Protection and Mobile Device Use and Support policies;

13. Authorized Users in units approved to accept and/or access Cardholder Data or utilize devices or systems that store or access Cardholder Data must adhere to the standards and controls; and

14. Adhering to the standards and controls set forth in the Payment Card Information Security Policy; and

12. Adhering to the standards of outside resources accessed from the Canisius network.

III. Privacy and Personal Use

Since the college’s communication systems are the property of the college, all communications are subject to review by appropriate and authorized employees at any time. Data may be retained in backup systems, even after its apparent deletion.

Users should be aware that personal privacy in their use of the college’s computer and network information systems sent to or from, or stored in, the college’s systems cannot be guaranteed in the event of legal or disciplinary proceedings.

If it appears that the integrity, security, or functionality of the college’s computer and network systems are at risk, Canisius College reserves the right to take any necessary action to investigate and remediate the problem. This action may include monitoring network activity or viewing user-generated files. In such cases, a written report of the findings will be forwarded to the appropriate college officials. In order to assure continuity for academic and administrative departments, similar procedures may be used after an employee is separated from the college or no longer able to perform required duties. Authorized Users are responsible for exercising good judgment regarding the personal use of the college’s computer and network information systems. If there is any uncertainty regarding personal use of the college’s computer and network information systems, users should consult the ITS Help Desk. College personnel may also consult with their supervisor.
or manager. At no time should the college’s computer and network information systems be used in a way that is at odds with college policy or applicable state or federal law.

IV. Unacceptable Use

Certain actions are strictly forbidden when an Authorized User is granted access to a college computer and network information systems. Under no circumstances shall a user of the Canisius College’s computer and network information systems:

1. Engage in any illegal activity using college computer and network information systems assets;

2. Engage in any activity contrary to college policy using College computer and network information systems assets;

3. Introduce malicious software into the campus computer and network information systems;

4. Reveal college information or allow the unauthorized use of college computer and network information systems by people outside of the Canisius community;

5. Attempt to breach, disrupt, eavesdrop on, circumvent the security of, or otherwise tamper with network communications, the personal devices of others in use at the college, or technology external to the college;

6. Access a college computer and network information systems using another user’s account information;

7. Use college computer and network information systems to violate intellectual property laws;

8. Use Canisius College computer and network information systems assets for personal commercial or for-profit activities, or to promote political causes;

9. Use Canisius equipment or network resources for viewing or exchanging pornography or sexually explicit materials except when engaged in the study of such material as part of an approved academic activity;

10. Acquire college computer and network information systems assets on behalf of the college, whether by purchasing, licensing, or subscribing to them, or by donating or accepting donations, whether their use is for a fee or free. In addition, users may not unilaterally dispose of college technology resources. See the Computer Asset Disposal and Computer Replacement policies for more information;

11. Contact information technology vendors seeking additional products or services on behalf of the college except for individuals authorized to do so as part of an approved ITS project or activity and faculty exploring instructional technologies to enhance individual courses. All additions and changes to college computer and network information systems (especially systems and software) are to be governed by an organized methodology;

12. Attempt to modify or repair college computer and network information systems, or arrange with technology vendors or private individuals for modifications or repairs. Authorized Users must contact the ITS Help Desk promptly to report problems with technology;
13. Connect personal equipment (e.g. networking equipment, keyboards, monitors, printers, scanners, etc.) to computer and network information systems assets at college locations, with the exception of external storage devices;

14. Give, loan, or relocate college computer and network information systems assets without ITS approval;

15. Use any software on personal devices connected to college computer and network information systems that provides network or file services to others (such as web servers, file servers, network protocols);

16. Use the college’s computer and network information systems to assume the identity of another (e.g., by sending forged electronic mail);

17. Utilize the college’s computer and network information systems to interfere with the proper functioning or the ability of others to make use of such systems, of others’ personal technology, or of technologies external to the college;

18. Utilize the college’s computer and network information systems to engage in any conduct that is likely to result in retaliation against the computer and network information systems, the personal devices of others, or technology external to the college, including engaging in behavior that results in any server being the target of a denial of service attack; and

19. Attempt to decrypt encrypted information unless they are authorized staff performing security reviews or investigations. The use of network “sniffers” is restricted to authorized system administrators or contractors tasked with solving network problems or conducting security audits. Network tools must not be used to monitor or track any individual’s network activity except under special authorization by the chief information officer.

Canisius College strongly protects the right of all members of the college community to be free from any form of electronic harassment or abuse. Members of the college community receiving any such unwanted or threatening electronic messages should immediately contact ITS so that appropriate disciplinary and/or legal action may be taken. In the event of an incident of Sexual or Gender-based Misconduct, the college’s Title IX coordinator may be contacted. Responsible Employees who become aware of such incidents are required to report the incident to the Title IX coordinator. See the college’s Sexual and Gender-Based Misconduct Policy for additional information, including confidential reporting procedures.

V. Withdrawal of Access

Access to the college’s information systems, from both remote and on campus site, is a privilege granted to Authorized Users. Access to college’s information systems may be granted, limited, or withdrawn by the college at any time.

A partial list of possible factors for termination include:

1. Observance of relevant college policies and associated controls, guidelines, laws, and contractual obligations;

2. The requester’s need to know;

3. The information’s sensitivity;

4. System load;
5. Availability of training;
6. Risk of damage to or loss by the college; and
7. The Authorized User’s previous history of use.

The College reserves the right to monitor, extend, limit, restrict, or deny privileges and access to its information systems for any reason at any time.

If it appears that the integrity, security, or functionality of the college’s information systems are at risk, Canisius College reserves the right to take any necessary action to investigate and remediate the problem. This action may include monitoring network activity, or viewing user-generated files, and/or terminating access. In such cases, a written report of the findings will be forwarded to the appropriate college officials. In order to assure continuity for academic and administrative departments, similar procedures may be used after an employee is separated from the college or no longer able to perform required duties.

VI. Use of College Email Systems

A. Access to College Email System(s)

1. Account Creation

College email accounts are created based on the official name of the employee as reflected in Human Resource records. Student and alumni accounts are created based on the name on file with the Registrar.

Requests for name changes to correct a discrepancy between an email account name and official college records will be processed, in which case the email account name will be corrected. Requests for email aliases based on name preference, middle name, etc., are evaluated on a case-by-case basis.

Employees or departments may request temporary email privileges for individuals outside of the college (i.e., guests, third-party contractors, volunteers). Such requests must be approved in writing by the appropriate area vice president or designee.

2. Account Termination

Individuals may leave the college for a variety of reasons, which gives rise to differing situations regarding the length of electronic mail privileges or expiration of electronic mail accounts. Guidelines governing those privileges are set forth below. Notwithstanding the guidelines below, access to college’s email system(s) may be limited or withdrawn by the college at any time.

1. **Faculty who leave before retirement**—full-time faculty who leave before retirement may keep their electronic mail account for one year from the end of the last term in which they taught. If such separation is for cause, email privileges may be immediately revoked without notice.

2. **Staff who leave before retirement**—staff who leave the college will have email privileges removed effective on their last worked day. If such separation is for cause, email privileges may be immediately revoked without notice.

3. **Retired Faculty**—full-time faculty who have retired from the college will be permitted to retain their email privileges if their account remains active. All email accounts that are inactive for a period of one year will be removed. These accounts are renewable on a 5-year
cycle. At the end of each cycle the faculty member will receive a notification to which they must respond, otherwise the account will be subject to deletion.

4. **Retired Staff**—staff who have retired from the college will have email privileges removed effective on their last worked day. Exceptions for business continuity may be made upon request of the department head and approval by the chief information officer.

5. **Volunteers and Guests**—volunteers and guest who leave the college will have email privileges removed effective on their last day with the college. If such separation is for cause, email privileges may be immediately revoked without notice.

6. **Students who leave before graduation**—students who leave the college without completion of their degree or other program may keep their email privileges for one academic year from the last term when they were registered.

7. **Expelled students**—if a student is expelled from the college, email privileges will be terminated immediately.

8. **Alumni**—students who have graduated from the college will be permitted to retain their email privileges for life if their account remains active. All email accounts that are inactive for a period of greater than one year will be subject to removal. Alumni wishing to reconnect with the college may request an account and one may be provided to them.

B. **Acceptable Use of College Email Systems**

1. **Authorized Users** are expected to read their college email on a regular basis and manage their email accounts appropriately. Authorized Users are presumed to have received and read all email messages sent to their official college email account.

2. Authorized Users must ascertain, understand, and use their accounts in accordance with the acceptable use policies outlined above and other applicable college policies, as well as those laws, regulations, contracts, and licenses applicable to the use of email systems and accounts.

3. To avoid confusing official college business with personal communications, college employees may not use non-college email accounts to conduct college business.

4. Authorized Users must comply with security measures employed by the college and protect assigned electronic mail accounts from access by others.

5. College email accounts may not be used to send mass emailing or commercial solicitations (a.k.a “spam”) to individuals, newsgroups, or mailing lists where such content is not part of the purpose of the group or list or for the purpose of college business (see the Mass Email Policy).

6. Microsoft Exchange email accounts are subject to the same retention policy as paper records and the college’s Email Retention Policy. Authorized Users who receive a notice of a legal hold are responsible for keeping copies of all relevant documents, including email.

7. If an Authorized User is not clear on what constitutes an appropriate use, the user is expected to contact his/her supervisor or ITS to determine whether a particular activity is permissible.
Note: Authorized Users who use email communications with persons in countries outside the United States should be aware that they may be subject to the laws of those other countries and the rules and policies on other systems and networks.

C. Unacceptable Uses of College Email Systems

The following specific actions and uses of college email systems are improper:

1. Any use of a college email account that interferes with college activities and functions or does not respect the mission, image, and reputation of the college;
2. Alteration of a source or destination address of email;
3. Use of a college email account for commercial or private business purposes that have not been approved in writing by the appropriate area vice president;
4. Use of a college email account in violation of college policy or applicable laws and regulations;
5. Use of a college email account to harass, threaten, incite violence, threaten violence, defraud, or defame other individuals;
6. Use of a college email account to infringe on another person’s copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
7. Email content that violates, or encourages the violation of, the legal rights of others or federal and state laws;
8. Use of a college email account to intentionally distribute viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
9. Purposefully interfering with the use of the college’s email system(s), or the equipment used to provide the email services by customers, authorized resellers, or other Authorized Users;
10. Purposefully altering, disabling, interfering with, or circumventing any aspect of the college’s email system(s);
11. Testing or reverse-engineering the college’s email system(s) in order to find limitations, vulnerabilities or evade filtering capabilities;
12. Use of a college email account to create a risk to a person’s safety or health, create a risk to public safety or health, compromise national security, or interfere with an investigation by law enforcement;
13. Use of a college email account to improperly expose trade secrets or other confidential or proprietary information of another person;
14. Sending unsolicited email messages, junk mail, spam, or advertising material to individuals who did not specifically request such material, as well as sending mass or chain messages in violation of the Mass Email Policy;
15. Forging or the unauthorized use of email header information;
16. Use of a college email account to unlawfully discriminate against another individual on the basis of age, race, religion or creed, color, sex, national or ethnic origin, sexual orientation,
marital status, military status, genetic predisposition or carrier status, gender identity, 
gender expression, familial status, domestic violence victim status, pregnancy, citizenship 
or immigration status, disability, criminal conviction or any other status protected by local, 
state or federal law;

17. Sending, viewing, or downloading offensive content of any kind, including pornographic 
material or messages of a sexist, obscene, harassing, threatening, or racist nature;

18. Sending, viewing, or downloading messages of a political nature for the purpose of 
proselytizing and/or soliciting funds or donations;

19. Creating or forwarding chain letters, Ponzi, or other pyramid schemes of any type;

20. Transmitting Private College Data without appropriate encryption Data, including but not 
limited to Cardholder Data, without appropriate encryption protection (see the System and 
Communications Protection Policy); and

21. Use of a college email account for illegal gambling.

Authorized Users are responsible for the content of their email messages and must understand that 
others can use such content as evidence against them.

Any questions as to whether the use of a college email account for academic, research, or 
educational purposes could violate the spirit of this policy should be brought to the attention of the 
user’s supervisor or ITS.

VII. Enforcement

ITS is responsible for the appropriate enforcement of this policy. During the course of any 
investigation of alleged inappropriate or unauthorized use, it may be necessary to temporarily 
suspend a user’s system privileges, but only after determining there is at least a prima facie case 
against the individual, as well as a risk to college’s computer and network information systems if 
privileges are not revoked. This is a necessary action taken to prevent further misuse and does not 
assume that the account holder initiated the misuse. Unsubstantiated reports of abuse will not 
result in the suspension of user account or network access unless sufficient evidence is provided 
to show that inappropriate activity occurred.

Any employee found to have violated this policy may be subject to disciplinary action, up to and 
including termination of employment.

Any student found to have violated this policy will be subject to disciplinary action through the 
Community Standards.

Visitors and others third party users who violate the provisions of the policy are subject to loss of 
access to the college’s computer and network information systems. They may also be subject to 
criminal and/or civil proceedings. In addition, the vice president for business and finance may 
administer other appropriate sanctions.

VIII. Notification

Users must report any identified weakness in college computer security and any incident of 
possible misuse or violation of this policy to ITS.

RELATED POLICIES

Access Control Policy
Revision Feedback for 2.4.1.: Acceptable Use of College Computer Policy

Submit Feedback
ENTERPRISE RESOURCE PLANNING (ERP) ACCESS CONTROL POLICY

Effective Date: May 9, 2019
Policy Number: II – 2.4.2
Issuing Authority: President
Responsible Officer: Chief Information Officer
Applicability: All College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data (“applicable information system(s)”), as well as all Authorized Users who access, use, or handle those resources. All Canisius College employees including student workers who require access to the ERP System as part of their employment duties.

History:

PURPOSE
The purpose of this policy is to protect information systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data. Access control ensures that an authenticated user accesses only the systems and Private College Data for which that user is authorized to access.

The purpose of this policy is to outline the access requirements for the Canisius College Enterprise Resource Planning (ERP) system. Note that this applies only to the administrative ERP software, not to the web interface used for self-service by the college community.

This policy will outline the means by which access to the administrative ERP software, as well as specific protected information accessible through the ERP system, is granted or rescinded.

POLICY
It is the policy of Canisius College to limit access to College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data to authenticated Authorized Users. The college employs the principle of least privilege, allowing access only to those authenticated Authorized Users (or processes acting on behalf of Authorized Users) necessary to accomplish assigned tasks in accordance with the college’s mission and business functions. Only authorized College employees are permitted to access the college’s ERP system. College employees granted access to the ERP system must adhere to the procedures and policy guidelines set forth in this policy.

DEFINITIONS
Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college...
computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

**Cardholder Data**—full magnetic stripe or the Primary Account Number (PAN) plus any of the following: cardholder name; expiration date; service code; CVC2/CVV2/CID (a three- or four-digit number displayed on the signature panel of the card or, in the case of American Express, on the face of the card).

**College Information**—is any data related to the business of the college including, but not limited to: financial, personnel, student, alumni, communication, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. Examples include: credit card information; tax identification numbers; payroll information; check requests and associated paperwork; student, parent, and employee tuition, financial aid and loan accounts information; student educational records as defined by FERPA; photographic images (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); medical or financial information for any employee, temporary worker, or student; other personal information to include date of birth, address, phone numbers, maiden names, customer numbers, social security numbers; college contracts; college research data; alumni and donor records; personnel records; college financial data; passwords; college proprietary information/data; and any other information for which access, use, or disclosure is not authorized by: a) federal, state, or local law; or b) college policy or operations.

**College Data**—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

**College Employees**—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

**College Information System**—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

**Covered Data and Information**—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 ("GLBA"), including Student Financial Information. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any Cardholder Data received in the course of business by the college, whether or not such Cardholder Data is covered by GLBA. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.

**Data Custodians**—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

**Data Owners**—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with
the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

*Members of the College Community*—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

*Non-Public Personal Information*—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

*Personally Identifiable Information or PII*—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

*Private College Data*—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the College Data Classification Policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, Cardholder Data, and Sensitive Authentication Data. See the Data Classification Policy for additional information.

*Public College Data*—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

*Sensitive Authentication Data*—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/ CVV2/CID, and PINs/PIN blocks.

*Student Education Records*—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has
visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

Student Financial Information—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

PROCEDURES/GUIDELINES

I. Role Based Access Control

Access to a given resource in the applicable information system is authorized based on the individual’s job classification and function (also called “role-based access control”) and is approved by the applicable Data Owner in accordance with the granting of access procedures set forth below. An Authorized User is given the minimum access level to a given resource in the ERP system in order to perform his/her job or contracted duties.

A. Granting of Access

Access to the ERP college information systems is granted by the applicable security administrator Data Owner. The request for access must be submitted, in an email message to bannersecurity@canisius.edu, by the supervisor of the employee who needs access. This request must include a delineation of the College Data that the employee (or vendor or other third-party contractor) needs to access, so that proper accommodations can be made. See the Information Technology Personnel Security Policy for additional information.

Access to forms containing Private College information, including social security numbers, date of birth, bank account numbers, or salary data, etc. must be approved by the controller.

B. Rescinding of Access

Access to the ERP information system will be removed by Information Technology Services (“ITS”) immediately upon termination of employment or, in the case of a vendor or other third-party, cessation of the individual’s engagement with the college. Additionally, access to the ERP information system will be removed when an employee’s position changes within the college, regardless of whether there is a change in department. See the Information Technology Personnel Security Policy for additional information.

Access to the software, for purposes of the new position, will be granted through the standard Granting of Access procedure above.

C. Special Consideration for Student Access

Because of the higher turnover among student employees, ERP information system software access for all students will be terminated at the end of every semester. Departments that need access for their students will apply for that access at the beginning of the next semester through the Granting of Access procedure above.
There is to be no write access to the ERP system for undergraduate student employees. Graduate students may have write access, in keeping with the standards outlined in Granting and Rescinding of Access procedure above. While “generic” accounts may exist for data lookup purposes, any data modification must be done with an approved Authorized User account.

**D. Sharing of Access**

In keeping with the college’s Acceptable Use Policy, sharing of login credentials in an attempt to circumvent access restrictions is a serious offense. Authorized Users who need access to particular forms or data should contact the applicable Data Owner so that accommodations may be made. Authorized Users issued login credentials are responsible for any actions, including data access, manipulation, modification, or deletion that takes place under the auspices of those credentials.

**II. Access Enforcement**

Access to applicable information systems is managed using the following controls:

1. Access to Private College Data via a college information system is controlled through centralized authentication and overseen by the applicable Data Owner to ensure only Authorized Users are allowed access to the data (see Section I above);

2. College information systems are configured by ITS to authenticate user credentials prior to allowing access to the system:

   a. All systems with College Data not entirely classified as Public in accordance with the Data Classification Policy must be accessed by a unique Login ID issued by ITS and an associated account; and

   b. Shared accounts must be assigned to a primary responsible Authorized User and issuance requires the approval of the chief information officer or designee;

See Section I above for additional information.

**III. Separation of Duties**

Where feasible, the college separates duties of individuals for tasks that are susceptible to fraud or other unauthorized activity.

1. ITS, in collaboration with applicable Data Owners, considers separation of duties when approving access within applicable information systems. Separation of duties include, but are not limited to, the following:

   a. Mission functions and distinct information system support functions are divided among different individuals/roles;

   b. Different individuals perform information system support functions (e.g., system management, configuration management, quality assurance and testing, network security);

   c. ITS staff who administer access control functions do not administer audit functions; and

   d. Different administrator accounts are issued for different roles.

2. ITS The Data Owner is responsible for ensuring and documenting separation of duties.
IV. Least Privilege

The college employs the principle of “least privilege” when assigning access to Authorized Users. This means that Authorized Users are assigned only the minimum rights necessary to perform the roles and responsibilities of the job function.

1. Authorized User accounts must be approved by the applicable Data Owner;

2. Administrator access accounts are approved by the chief information officer (or a designee), who ensures the duties assigned to the user require administrator access to the system and accompanying College Data;
   a. ITS maintains a list(s) of employees approved for administrator account access;
      i. The list(s) is reviewed at least annually by the chief information officer or designee;
   b. Each individual granted administrator access receives appropriate security awareness training in accordance with the Information Technology Security Awareness and Training Policy;
   c. Each individual granted administrator access must use the account or access privilege most appropriate for the requirements of the work being performed (e.g., Authorized User account vs. administrator account);
   d. Each individual granted administrator access must refrain from abuse of privilege and only conduct investigations as directed by the chief information officer;
   e. Each individual granted administrator access must use a password escrow to enable ITS to gain access to the system in an emergency.

3. Use of shared administrator accounts are generally not allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares). Such exceptions require the approval of the chief information officer and documentation which justifies the need for a shared account:
   a. The password for a shared administrator access account must change under the following conditions:
      i. An individual knowing the password leaves the college or department;
      ii. Job duties change such that the individual no longer performs functions requiring administrator access; and
      iii. A vendor or third-party contractor with administrator account access leaves or completes its work.

4. Special access accounts (e.g., vendor or third-party contractor) are to be used in very limited situations and must provide individual accountability. Special access accounts must be:
   a. Requested in writing by a Data Owner (or his/her authorized designee) and authorized by the chief information officer or designee.
   b. Created with a specific expiration date:
c. Monitored when accessed remotely by the vendor or third-party contractor; and
d. Removed when the task or project is complete.

5. In those cases where law enforcement agencies request access in conjunction with a lawful investigation, the request must be made in writing (e.g., subpoena, court order). All such requests must be reported to the chief information officer, who will consult with the college’s legal counsel, before any action is taken.

V. Unsuccessful Login Attempts

ITS enforces, through the use of baseline configurations, a limit of login attempts by a user. If a user has unsuccessfully attempted more than three (3) attempts to login to an account within a 15-minute timeframe, the account will be locked for a minimum of thirty (30) minutes (or until an ITS enables the user ID) and the user may try again after that time. This control is in place, in part, to help prevent brute force attacks.

VI. System Use Notification

College information systems are configured by ITS, where feasible, to display a screen at login which clearly states that the system is the property of the college and is for authorized use only. The notification informs potential users that the system may be monitored, recorded, and audited, and that use of the system implies consent to monitoring and recording. The text displayed also states that the user acknowledges and agrees with the Acceptable Use of the College Computer and Network Systems Policy and that unauthorized use may be subject to disciplinary action, as well as criminal and civil penalties. The notification will remain on the screen until the user acts to log onto the system, acknowledging the notification.

VI. Session Lock

ITS, through the use of baseline configurations, enforces a session lock as a temporary action taken when an Authorized User stops work, and the resource is idle. The session lock, where feasible, will be set to initiate after a fifteen (15) minute period of idle time in order to conceal potentially Private College Data on the screen. The session lock, however, is not intended to take the place of logging out of a resource, as required in the Physical and Environmental Protection Policy.

VII. Permitted Actions without Identification or Authentication

To protect the integrity and availability of Public College Data, ITS generally requires identification and authentication on information systems containing only Public college Data. Some uses of these systems may be exempted to not require authentication, such as general form submission and anonymous reporting.

VII. Remote Access

Remote access is any access to a college information system by an Authorized User (or process acting on behalf of a user) communicating through an external network (e.g., the Internet or connection (e.g., dial-up, broadband, wireless).
ITS requires that all Authorized Users with a need to connect to a college information system while not physically located on the college network to use the encrypted virtual private network (VPN) to securely connect. This includes all connections using broadband, wireless, or dial-up methods. The use of the VPN protects the confidentiality and integrity of College Data. Once connected, the Authorized User’s normal access privileges are granted.

1. It is the responsibility of an Authorized User with VPN privileges to the college network to ensure that the remote access connection is given the same consideration as the Authorized User’s on-site connection to the college network;
   a. VPN access is to be controlled using the Authorized User’s NetID and LDAP password;
   b. When connected to the college VPN, all traffic from the user will be sent through the encrypted tunnel. All other traffic will be dropped;
   c. The VPN concentrator(s) will be set up and maintained by ITS;
   d. All computers connecting to the college VPN must have active, up-to-date antivirus software and operating system patches;
   e. VPN users will be automatically disconnected from the network after 60 minutes of inactivity;
   f. In the unusual circumstance that an employee connects to the VPN using non-college equipment, he or she must configure that equipment to comply with Canisius College VPN and network standards;
   g. Only VPN clients approved by Canisius College ITS may be used to connect to the college VPN;
   h. ITS will occasionally require the user of a VPN-connecting computer to bring it to campus to be audited and updated. Failure to do so will result in the suspension of the user’s VPN privileges;

2. At no time is a remote user connected to the college network permitted to connect to another network or device beyond the initial device making the connection. This includes, but is not limited to split tunneling, dual homing, or otherwise re-routing college traffic beyond the intended endpoint;

3. It is the responsibility of an Authorized User with VPN privileges to ensure that unauthorized users (e.g., family, friends, etc.) are not allowed access to the college network;

4. Authorized Users may not provide the user’s NetID and LDAP password to other individuals;

5. Authorized Users must take every reasonable effort to ensure the confidentiality, integrity, and availability of College Data and college information technology resources used remotely (e.g., not leaving Mobile Devices unattended or in public plain view);

6. Remote access users are not permitted to download or otherwise store Private College Data on their personal Mobile Devices (see the System and Communications Protection, Media Protection and Mobile Device Use and Support policies). This includes the transfer of such
data to a personal cloud service such as Dropbox or Google Drive (see the Cloud Computing Policy);

7. Authorized Users must understand their responsibilities for protecting Private College Data, and the consequences for mishandling such data.

Note: Two Factor Authentication (and then logon through the VPN) is mandatory for all remote access by administrator users to the Cardholder Data Environment

-Note: Logon through VPN is mandatory for all remote access by administrative users to the college information systems.

VIII. User of External Information Technology Resource Systems

Authorized Users must comply with the Cloud Computing Policy before using an externally-managed information system.

All connections between college information systems and external systems must be approved and documented in accordance with the Cloud Computing Policy.

All third-party connection requests must have approval from the chief information officer.

IX. Publicly Accessible Content

The Office of Marketing and Communication is responsible for ensuring that publicly-accessible information technology resources such as webpages and social media applications do not contain Private College Data. Additionally, the Office of Marketing and Communication must review the proposed content of publicly-accessible information and remove non-public information prior to posting onto college webpages, social media applications, or any other information technology resource. Individuals must be authorized to post content onto webpages, social media applications, or any other information technology resource that is publicly accessible. The Office of Marketing and Communication will periodically review publicly accessible web material for nonpublic or inappropriate information.

See also the System and Communications Protection Policy, which outlines security controls in place to safeguard the college’s public access servers.

IX. Responsibilities

Data Owners shall:

1. Approve and document all Authorized Users in their department in accordance with the procedures set forth in the Information Technology Personnel Security Policy.

   a. Data Owners must maintain all Authorized User account data, information, and documentation associated with an Authorized User’s logical access on file in accordance with the Record Retention Policy and Schedule;
2. Adhere to the procedures set forth in the Information Technology Personnel Security Policy for removing accounts of individuals who are no longer authorized to have access to the applicable information system;

3. Adhere to the procedures set forth in the Information Technology Security Personnel Policy to modify an Authorized User account to accommodate situations such as name changes, accounting changes, and permission changes;

4. Periodically review (on at least an annual basis) existing Authorized User accounts for validity; and

5. Ensure that Authorized Users in the department are not sharing accounts, unless the system resides on a guest network.

B. Information Technology Services (ITS) Access Control Responsibilities

1. Disables or removes all login IDs having access to Private College Data that have not been used/accessed within a period of 90 days. Exceptions may be made at the request of the Data Owner.

2. Ensures that access credentials for internal information systems are delivered to the Authorized User in a confidential manner;

3. Ensures that access credentials for Internet-facing only systems are securely delivered (e.g., by alternate channels such as U.S. Mail) to all external Authorized Users of systems that access Private College Data;

4. Configures applicable information system to automatically audit account creation, modification, disabling, and termination actions and notifies, as required, appropriate Data Owners and supervisors;

5. Investigates any unusual system access activities observed in logs or reported by employees. Investigation activities include the following:
   a. Monitoring applicable systems for atypical usage of information system accounts;
   a-b. Reporting atypical usage to the chief information officer; and
   c. Tracking and monitoring privileged role assignments (e.g., key management, network and system administration, database administration, and web administration).

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
Cloud Computing Policy
Data Classification Policy
Identification and Authentication Policy
Information Security Program
Information Technology Personnel Security Policy
Information Technology Security Awareness and Training Policy
Health Insurance Portability and Accountability Act Policy
Mobile Device Use and Support Policy
Password Policy
Revision Feedback for 2.4.2.: Access Control Policy

Submit Feedback
## CLOUD COMPUTING POLICY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>May 9, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number:</td>
<td>II – 2.4.3</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Issuing Authority:</td>
<td>President</td>
</tr>
<tr>
<td>Responsible Officer:</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Applicability:</td>
<td>All College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data (“applicable information systems”), as well as all Authorized Users who access, use, or handle those resources. All college students, staff, faculty, contractors, consultants, and other workers at Canisius College, including all personnel affiliated with third parties. This policy applies to all college-owned or college-leased equipment.</td>
</tr>
<tr>
<td>History:</td>
<td></td>
</tr>
</tbody>
</table>

### PURPOSE

The purpose of this policy is to ensure that Private College Data is not inappropriately stored or shared using public Cloud Computing and/or file sharing services to establish the college’s policies and procedures regarding the protection of college information placed into a cloud computing environment that is not directly controlled by Canisius College.

### POLICY

*College information Private College Data* as defined in this policy may not reside within any cloud computing environment unless Canisius College has entered into a legally binding agreement with the service provider to ensure that the data is protected and managed in accordance with standards and procedures required by law and acceptable to the Information Technology Services (“ITS”).

*College information Private College Data* placed into a college authorized cloud environment must be encrypted in transit and encrypted at rest. Moreover, the cloud service provider’s contract must indicate that they conform to all relevant federal, state, and local laws and regulations. Finally, any *college information Private College Data* residing within a cloud computing environment must be retrievable by the college and not solely by the individual who placed the data in the cloud environment, and must conform to the college’s Record Retention Policy and Schedule.

### DEFINITIONS

*Authorized User*—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.
Cloud Computing/Cloud Environment—encompasses utilizing any external computing, software services, or hosting environment that is not directly controlled by Canisius College.

College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

College Information System—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any Cardholder Data received in the course of business by the college, whether or not such Cardholder Data is covered by GLBA. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.

Data Custodians—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

Data Owners—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

Encrypted Data—refers to information that has been converted through software into a non-human readable form typically via a password or phrase (which is also used to decrypt the file when the information is to be accessed). All encryption referred to within this policy must conform to prevailing industry standards.

Encryption—the process of encoding (or scrambling) information so that it can only be converted back to its original form (decrypted) by someone who (or something which) possesses the correct decoding key.

Members of the College Community—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

Mobile Device—any handheld or portable computing device running an operating system optimized or designed for mobile computing that is capable of accessing, storing, and manipulating information in an untethered manner (usually, but not always, through a wireless connection). This includes, but is not limited to, laptops, tablets, smart phones/cell phones, PDAs, or other portable
devices. Any device running a full desktop version operating system is not included in this definition.

Non-Public Personal Information—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

Personally Identifiable Information or PII—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

Private College Data—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the College Data Classification Policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, Cardholder Data, and Sensitive Authentication Data. See the College Data Classification Policy for additional information.

Public College Data—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

Sensitive Authentication Data—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

Student Education Records—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.
**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

**College Information**—any data related to the business of the college including, but not limited to: financial, personnel, student, alumni, communication, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. Examples include: credit card information; tax identification numbers; payroll information; check requests and associated paperwork; student, parent, and employee tuition, financial aid, and loan accounts information; student educational records as defined by FERPA; photographic images (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); medical or financial information for any employee, temporary worker, or student; other personal information to include date of birth, address, phone numbers, maiden names, customer numbers, social security numbers; college contracts; college research data; alumni and donor records; personnel records; college financial data; passwords; college proprietary information/data; and any other information for which access, use, or disclosure is not authorized by: a) federal, state, or local law; or b) college policy or operations.

**Computer and Network Systems**—any college owned or leased computer, mobile device, or software, as well as any part of the college’s computer, data, voice or video networks physically located on any college owned, leased, or rented property or located on the property of any third party with the permission of that party. This includes devices on such networks assigned any routable and non-routable IP addresses and applies to the college’s wireless network and the network serving the college’s student residence housing and any other vendor supplied network made available to the college community.

**Users**—any individual granted access by Information Technology Services to a college computer and network system.

**PROCEDURES/GUIDELINES**

**I. Contract Approval Procedures**

All legally binding written agreements with a Cloud Computing service provider must be approved in writing by the vice president for business and finance.

The chief information officer or his/her designee will endorse the use of Cloud Computing services, including file storing and sharing, only if:

1. The Cloud Computing vendor meets established college data security requirements as set forth in applicable college information security-related policies and conforms to all relevant federal, state and local laws and regulations.
2. The Cloud Computing vendor provides appropriate levels of recovery for Private College Data by the college and not solely by the individual who placed the data in the Cloud Computing environment;

3. The Cloud Computing vendor accepts and is contractually bound to implement the college’s explicit restrictions on storage of Private College Data (i.e., Private College Data must be encrypted in transit and encrypted at rest);

The use of such service, in the judgement of the chief information officer (or his/her designee) does not place the college at an unreasonable risk of experiencing data breach, data loss/non-recovery, or degradation of applicable information systems and College Data.

II. Enforcement

ITS is responsible for the appropriate enforcement of this policy. During the course of any investigation of alleged inappropriate or unauthorized use of cloud computing environment, it may be necessary to temporarily suspend an Authorized User’s network or computing privileges, but only after determining there is at least a prima facie case against the individual, as well as a risk to applicable information college computer and network systems if privileges are not revoked. This is a necessary action taken to prevent further misuse and does not presume that the user initiated the misuse. Unsubstantiated reports will not result in the suspension of user account or network access unless sufficient evidence is provided to show that inappropriate activity occurred.

Students and employees who violate the provisions of the policy are subject to disciplinary action pursuant to the college’s applicable disciplinary policies, as well loss of access to applicable information the college’s computer and network systems.

Visitors and others third party users who violate the provisions of the policy are subject to loss of access to the college’s computer and network applicable information systems. In addition, the vice president for business and finance may administer other appropriate sanctions.

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
Data Classification Policy
Information Security Program
Health Insurance Portability and Accountability Act Policy
Mobile Device Use and Support Policy

Record Retention Policy and Schedule

Student Records (FERPA) Policy
Wireless Access Points Policy

Revision Feedback for 2.4.3.: Cloud Computing Policy
Submit Feedback
Purpose of this policy is to outline the rules for disposal of computer assets and other applicable information systems owned or leased by the college. Once a computer asset or applicable information system has reached the end of its active life on campus, it can be purchased by a member of the college community, donated, or disposed of as waste.

Policy
College personnel are responsible for the appropriate disposal of college computer assets and other applicable information systems in accordance with the procedures and guidelines set forth in this policy. Members of the college community may not directly give, lend, rent, donate, or dispose of college’s computer assets and other applicable information systems.

Definitions
Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

College Information System—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing asset platforms that can process, store, or transmit College Data.

Computer Assets—any device that contains electronic circuitry or any data storage media that keeps information. Devices with electronic circuitry include, but are not limited to, computers,
laptops, mobile devices, copy machines, fax machines, calculators, and telecommunication equipment. Computer assets also includes data storage media.

**Covered Data and Information**—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any Cardholder Data received in the course of business by the college, whether or not such Cardholder Data is covered by GLBA. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.

**Data Custodians**—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

**Data Owners**—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

**Disposal**—any computer asset leaving custody of the college, regardless of whether the equipment is being returned as part of a lease, being sold, donated, or being thrown away. It is the responsibility of the department and the employee in custody of the item to understand and manage the terms and conditions of its disposal.

**Members of the College Community**—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

**Mobile Device**—any handheld or portable computing device running an operating system optimized or designed for mobile computing that is capable of accessing, storing, and manipulating information in an untethered manner (usually, but not always, through a wireless connection). This includes, but is not limited to, laptops, tablets, smart phones/cell phones, PDAs, or other portable devices. Any device running a full desktop version operating system is not included in this definition.

**Non-Public Personal Information**—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit
histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the College Data Classification Policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, Cardholder Data, and Sensitive Authentication Data. See the Data Classification Policy for additional information.

**Public College Data**—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

**Sensitive Authentication Data**—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

**Student Education Records**—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

**College Information**—any data related to the business of the college including, but not limited to: financial, personnel, student, alumni, communication, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. Examples include: credit card information; tax identification numbers; payroll information; check requests and associated paperwork; student, parent, and employee tuition,
PROCEDURES/GUIDELINES

Any computer equipment asset and other applicable information system owned or leased by the college that is no longer useful on campus may either be purchased by a member of the campus community or outside vendor, donated, or disposed of as waste in accordance with the procedures set forth below:

I. Sales

Computer assets and other applicable information systems that have served their useful life at Canisius College may be made available for sale to a member of the Canisius College community. Such personal purchases must be approved by ITS before being offered for sale. The sale price will be based on the college’s depreciation schedule (20% straight line depreciation per year), but in no event will be less than $50. Computer assets with an original purchase price of $1,000 or more will require the completion of an Asset Disposal Form.

ITS will wipe and reformat the hard drive and re-install the operating system that came with the system. No college information will be transferred. The computer or other applicable information system will be sold on an “as is” basis and ITS will not support the computer, system, or the software after the purchase.

II. Disposal

If the equipment is to be discarded, ITS will use a professional computer salvage/recycling company to safely dispose of the equipment. ITS staff will ensure the asset is cleared of all software licensed to the college and any College Data. In the case of purchase or disposal, ITS will complete the required paperwork for the Controller’s Office and remove the equipment from the college’s inventory. The ITS Help Desk will coordinate this activity (x8340).

III. Donated

Any hardware considered no longer in service to the college may be donated by ITS. ITS staff will ensure the asset or other applicable information system is cleared of all software licensed to the college and any College information Data. Donation of a computer asset with an original purchase price of $1,000 or more will require the completion of an Asset Disposal Form.

IV. Data Disposition

It is imperative that College information Data is not contained on any machine that permanently leaves the campus. If a computer asset or other applicable information system is still operational, it will be booted with external media and the internal hard drive(s) will be wiped by ITS or an approved vendor with a tool such as DBAN or Disk Utility. If the computer asset or other applicable information system is not operational, the hard drive(s) will be removed and either
physically destroyed or installed in another computer and wiped with a software tool. Refer to the Media Protection Policy for additional information.

V. Enforcement

It is expected that ITS staff will enforce this policy whenever a piece of equipment is ready to leave campus. Responsibility for disposal and data disposition lies with the appointee of the director of user services.

RELATED POLICIES

- Capitalization and Depreciation Policy
- Computer Asset Replacement Policy
- Information Technology Change Control Policy
- Media Protection Policy
- Record Retention and Disposal Policy
PURPOSE

The purpose of this policy is to establish the procedure for the annual replacement of computer assets for faculty and staff using Canisius funds allocated for that purpose.

POLICY

Replacement of computer assets will proceed annually, as long as funds for this purpose are allocated, according to the procedures and guidelines set forth in this policy.

DEFINITIONS

*Computer Assets*—any device that contains electronic circuitry or any data storage media that keeps information. Devices with electronic circuitry include, but are not limited to, computers, laptops, mobile devices, copy machines, fax machines, calculators, and telecommunication equipment. Computer assets also includes data storage media.

PROCEDURES/GUIDELINES

I. **Inventory and Distribution**

The list for the annual replacement will include the oldest computer assets on campus, as well as new assets as needed for new full-time college employees. Job function, needs assessment, and special requests made by the deans and area vice presidents play a role in the development of the annual replacement list. At times, it may be necessary to add some computer assets that have been problematic, or to replace a department’s assets because of a software requirement. The goal is to use the allocated funds to replace as many as possible from the list.

II. **Standard Configuration of Macintosh and Windows Computers**

ITS will ensure that all computer assets are configured in accordance with the Configuration Management Policy. Typically, ITS will negotiate with vendors to provide the best standard configurations for both desktops and laptops on both platforms. These will be posted, along with cost information, for all recipients to see.

III. **Procedure for Notification**
Deans and department chairs will be notified of the full-time employees in their area who will receive new computer assets, as will each full-time employee receiving a new computer or device. Each person getting a new asset will have an “allotment” from the replacement budget, sufficient to fund their recommended asset. If a faculty or staff member needs or desires a model that is above the standard amount, the request will need to be justified to vice presidents, deans, and chairs.

IV. Useful Computer Life

Campus computers are replaced based on the useful life of the computer asset.

V. De-accessioning

Please consult the Computer Asset Disposal Policy.

VI. Accessibility

In accordance with the Electronic Accessibility Policy, the college makes every reasonable effort to purchase computer assets that are accessible to users with disabilities. Accessible, in this context, means compatible with assistive technology.

Prospective vendors will be requested to submit the Voluntary Product Accessibility Template (VPAT) published by the Information Technology Industry Council, describing the accessibility of their products and services, and such accessibility will be taken into consideration in making a purchasing decision. All college contracts for applicable resources will contain appropriate provisions concerning accessibility, as determined by ITS.

RELATED POLICIES

Capitalization and Depreciation Policy
Configuration Management Policy
Computer Asset Disposal Policy
Electronic Accessibility Policy
Information Technology Change Control Policy
Procurement Policy and Purchasing Procedures
### ELECTRONIC ACCESSIBILITY POLICY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>May 6, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number:</td>
<td>II – 2.4.6</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>Not Applicable.</td>
</tr>
<tr>
<td>Issuing Authority:</td>
<td>President</td>
</tr>
<tr>
<td>Responsible Officer:</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Applicability:</td>
<td>All members of the Canisius College Community.</td>
</tr>
<tr>
<td>History:</td>
<td></td>
</tr>
</tbody>
</table>

---

**PURPOSE**

The purpose of this policy is to set forth minimum guidelines for electronic accessibility at Canisius College.

**POLICY**

In accordance with applicable federal and state laws, including the Americans with Disabilities Act of 1990 (ADA), as amended, and Section 504 of the Rehabilitation Act of 1973, it is the policy of Canisius College to make Information and Communication Technology ("applicable technologies") at the college accessible to members of the college community and the general public to the greatest extent that is reasonably practicable.

Accordingly, all individuals with responsibility for creating, selecting, procuring, developing, implementing, and maintaining applicable technologies at the college must strive to ensure equal and effective access to these technologies. These responsibilities include the:

1. Use of Webpage design standards (see Section I.A below) that provide access for all, including those with disabilities;
2. Use of hardware and software products that promote accessibility (see Section I.C below); and
3. Provision of accessible technology-related work environments to employees and students that accommodate all users (see Sections 1.A-C below).

The following circumstances may qualify as exemptions from this policy:

1. When conformance fundamentally alters a program, service, or activity;
2. When conformance creates an undue administrative burden; or
3. When conformance is not technically feasible. In such circumstances, the individual, office or unit sponsoring the program, service, or activity must provide Equally Effective Alternative access that communicates the same information in as timely a fashion as does the original format or medium.
Non-compliant technologies must not be purchased or developed prior to receiving an exemption approval by the chief information officer or his/her designee.

The following sets forth minimum guidelines for electronic accessibility at Canisius College:

All information technology products (i.e., software applications, telecommunications, videos, multimedia, ATM’s, copiers, fax machines, and desktop and portable computers) purchased by the college must have the capability to use assistive software and hardware;

The college will provide accessible information technology products for employees and students with disabilities; and

The college provides reasonable access to web enhanced instruction, informational or instructional video media, and alternate media formats utilized as part of its academic offerings.

**DEFINITIONS**

*Information Technology Products*—software applications, telecommunications, videos, multimedia, ATM’s, copiers, fax machines, and desktop and portable computers.

*Accessible*—means that individuals with disabilities are able to independently acquire the same information, engage in the same interactions, and enjoy the same services within the same timeframe as individuals without disabilities, with substantially equivalent ease and effectiveness of use.

*Archived*—means a Web page or application that is no longer available online but is still subject to the applicable records retention requirement under college policy.

*Information and Communication Technology*—includes e-learning and information technology and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information, including but not limited to, the internet and intranet websites, content delivered in digital form, electronic books and electronic book reading systems, search engines and databases, learning management systems, classroom technology and multimedia, personal response systems (“clickers”), and office equipment such as classroom podiums, copiers and fax machines. It also includes any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, creation, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This term includes telecommunications products (such as telephones), information kiosks, Automated Teller Machines (ATMs) transaction machines, computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

*Equally Effective Alternative Access*—means an alternative format, medium or other aid that accurately and in a timely manner communicates the same content as does the original format or medium, and which is appropriate to an individual’s disability. To provide equally effective alternative access, the college need not ensure that qualified individuals with disabilities achieve the identical result or level of achievement as individuals without disabilities, but the college must provide appropriate auxiliary aids and services as necessary to afford individuals with disabilities an equal opportunity to obtain the same result, gain the same benefit or reach the same level of achievement, in the most integrated setting appropriate to their needs. In providing equally effective alternative access, the college may rely on any commonly accepted standard or
combination of standards provided the remainder of this definition is met. The college is not required to take any action that results in a fundamental alteration in the nature of a service, program or activity, or in undue financial and administrative burden, but must nevertheless ensure, to the maximum extent possible, that qualified individuals with disabilities receive the benefits or services provided by the college.

Member of the College Community—includes any person who is a student, faculty member, staff member, organization, club, group, team, alumni, volunteer, trustee, or any other person employed by the college.

Public Facing Content—means any content that is intended for access by the general public, without restrictions. Content that is not public-facing is termed “controlled” content, and encompasses content where authentication or authorization is required for access, and/or content is targeted to and delivered for those enrolled in specific programs, majors or classes.

Undue Administrative Burdens—are created when a proposed course of action causes significant difficulty. Because the college must consider all resources available when reviewing claims of undue administrative burdens, the decision to invoke undue administrative burdens will be carefully weighed, sufficiently documented and ultimately authorized by the chief information officer or his/her designee. In situations where undue administrative burdens can be documented, equally effective alternative access must still be provided.

PROCEDURES/GUIDELINES

I. Accessibility Standards

A. Web Pages and Applications Accessibility

To the fullest extent feasible, all college Web pages and applications should strive to comply with the following accessibility standards:

1. Public Facing Web Pages and Applications

   a. The college has adopted the Worldwide Web Consortium Web Content Accessibility Guidelines version 2.0, Level AA Conformance (WCAG 2.0 Level AA) and WAI-ARIA technical specifications as its goal for accessible college Web pages;

   b. All new and redesigned public facing Web pages and applications published for, hosted by, or otherwise provided by the college or any of the college’s departments, programs, or offices must be compliant when created or updated.

   b, All public facing Web pages and applications created for, hosted by, or otherwise provided by the college or any of the college’s departments, programs, or offices in existence prior to [INSERT DATE THIS POLICY IS APPROVED] must be compliant in accordance with the implementation timeline established by the department of Marketing & Communications.

   d. All archived public facing Web pages and applications published for, hosted by, or otherwise provided by the college or any of the college’s departments, programs, or offices must be clearly marked as archived and include accessible instructions on how users can request an Equally Effective Accessible format of its content.
e. Exceptions to the college Accessibility Standards referenced above based on technical impracticality or fundamental alteration of a program must be submitted to the ITS for a determination of the standards of accessibility that will be met. College departments and employees must be prepared to provide content and/or services in a suitable Equally Effective Accessible format.

2. Controlled Web Pages and Applications: Controlled content and functionality on controlled content Web pages and applications should be made available to users with disabilities on request in an Equally Effective Accessible format.

B. Instructional Materials Accessibility

Course instructors are responsible for assuring that all Electronic and Information Technology instructional materials are accessible. Instructional materials include, but are not limited to, syllabi, textbooks, presentations, handouts, electronic instructional materials delivered within the college’s learning management system, face-to-face classes, or an alternate method, and electronic instructional activities such as online collaborative writing, web conferencing, and other similar activities.

C. Technology Procurement

The college makes every reasonable effort to purchase and develop college Information and Communication Technologies that are accessible to users with disabilities. Accessible, in this context, means compatible with assistive technology.

Prospective vendors will be requested to submit the Voluntary Product Accessibility Template (VPAT) published by the Information Technology Industry Council, describing the accessibility of their products and services, and such accessibility will be taken into consideration in making a purchasing decision. All college contracts for college Information and Communication Technologies will contain appropriate provisions concerning accessibility, as prescribed by the ITS.

II. Training

ITS along with COLI and the department of Marketing & Communications offers training and educational resources to college community members, including faculty, web developers and personnel involved with course delivery to ensure accessibility of Electronic and Information Technology.

RELATED POLICIES

Anti-Discrimination and Harassment Policy
Employee Accessibility (ADAA) Policy
Student Accessibility Policy.
Purpose

The purpose of this policy is to define the college’s information security program (“program ISP”), which establishes a college-wide approach to information security and prescribes mechanisms that help identify and prevent the compromise and misuse of covered data and information; defines mechanisms that allow the college to satisfy its legal and ethical responsibilities with regard to its networks’ and computer systems’ connectivity to worldwide networks; and prescribes an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this program.

Policy

It is the policy of the college to maintain a comprehensive program ISP in compliance with the Gramm Leach Bliley Act (GLBA). The objective of the program ISP is to: ensure the security and confidentiality of covered data and information in compliance with applicable GLBA rules as published by the Federal Trade Commission; safeguard against anticipated threats to the security or integrity of covered data and information, including electronic data; and guard against unauthorized access to or use of covered data and information that could result in harm or inconvenience to college students, employees, and customers.

The college’s program ISP incorporates, by reference, college-wide and departmental policies and procedures that address the security and confidentiality of College Data encompassed by the definition of “covered data and information” below. These include, but are not limited to:

- Access Control Policy
- Acceptable Use of College Computer and Network Systems Policy
- Audit and Accountability Control Policy
- Computer Assets Disposal Policy
- Computer Asset Replacement Policy
- Confidential Information Policy
- Configuration Management Policy
- Data Classification Policy
- Health Insurance Portability and Accountability Act Policy
- Identification and Authentication Policy
Identity Theft Prevention Policy
Information Technology Personnel Security Policy
Information Technology Physical and Environmental Protection Policy
Information Technology Security Awareness and Training Policy
Media Protection Policy
Mobile Device Use and Support Policy
Student Records (FERPA) Policy

DEFINITIONS

**College Information**—is any data related to the business of the college including, but not limited to: student and employee financial information. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. Examples include: credit card information; tax identification numbers; payroll information; check requests and associated paperwork; student, parent, and employee tuition, financial aid and loan accounts information; student educational records as defined by FERPA; photographic images (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); medical or financial information for any employee, temporary worker, or student; other personal information to include date of birth, address, phone numbers, maiden names, customer numbers, social security numbers; college contracts; college research data; alumni and donor records; personnel records; college financial data; passwords; college proprietary information/data; and any other information for which access, use, or disclosure is not authorized by: a) federal, state, or local law; or b) college policy or operations.

**Covered Data and Information**—for the purpose of this policy, covered data and information includes student and employee financial information required to be protected under the Gramm Leach Bliley Act (GLB). In addition to this coverage which is required by federal law, Canisius College chooses as a matter of policy to also define covered data and information to include college information as that term is defined in this policy. Covered covered data and information includes both paper and electronic records.

**Employee Financial Information**—that information the college has obtained from an employee in the process of offering a benefit or service. Offering a benefit or service includes all college sponsored benefit plans and college financial services such as the Employer Assisted Housing Program, computer loans, flexible spending accounts, and personal payroll services. Examples of employee financial information include bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

**Student Financial Information**—that information the college has obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of student financial information include bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

**Authorized User**—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college
computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

Cardholder Data - full magnetic stripe or the Primary Account Number (PAN) plus any of the following: cardholder name; expiration date; service code; CVC2/CVV2/CID (a three- or four-digit number displayed on the signature panel of the card or, in the case of American Express, on the face of the card. Canisius College does not store cardholder data in any of its information systems. Cardholder data is stored by third-party vendors, which are contractually obligated to comply with the PCI DSS.

College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

College Information System—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any Cardholder Data received in the course of business by the college, whether or not such Cardholder Data is covered by GLBA. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

Data Custodians—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

Data Owners—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

Members of the College Community—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

Non-Public Personal Information—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of
customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to this policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, Cardholder Data, and Sensitive Authentication Data. See the College Data Classification Policy for additional information.

**Public College Data**—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

**Sensitive Authentication Data**—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

**Student Education Records**—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

**PROCEDURES/GUIDELINES**
In compliance with the GLBA, the college’s ISP includes the following elements:

The Gramm-Leach-Bliley (GLB) mandates that the college

1. Appoint an information security plan ISP coordinator;
2. Conduct a risk assessment of likely security and privacy risks;
3. Institute a training program for all employees who have access to covered data and information;
4. Oversee service providers and contracts, and
5. Evaluate and adjust the program ISP on an annual basis periodically.

I. Designation of the ISP Coordinator

In order to comply with GLBA, the college has designated the chair of the ITS Systems and Security Committee (SSC) to serve in the role of information security program ISP coordinator. The chair of the SSC, as well as the committee members, must work closely with college legal counsel and all relevant academic and administrative schools and departments throughout the college. The chair of SSC is appointed by the chief information officer.

The coordinator (or the coordinator’s designee) must help the relevant offices of the college identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program, and regularly monitor and test the program.

II. Risk Assessment and Safeguards

The coordinator (or the coordinator’s designee) must work with all relevant areas of the college to identify potential and actual risks to security and privacy of information. Each department head, or designee, will conduct an annual data security review, with guidance from the coordinator. Data Owners will be asked to identify any employees in their respective areas that work with covered data and information. In addition, the relevant departments of ITS will conduct an annual review of procedures, incidents, and responses, and will document all relevant materials. Selective publication of these materials is for the purpose of educating the college community on network security and privacy issues. ITS will assure that procedures and responses are appropriately reflective of those widely practiced at other institutions of higher education, as measured by four advisory groups: The Educause Security Institute, The Internet2 security working group, the SANS Top Twenty risks list, and the Federal NIST Computer Security Resource Center.

In order to protect the security and integrity of the college network and its data, ITS will develops and maintains a registry of all computers attached to the college network. This registry will include, where relevant, IP address or subnet, MAC address, physical location, operating system, intended use (server, personal computer, lab machine, dorm machine, etc.), the person, persons, or department primarily responsible for the machine, and whether the machine has special access to any confidential data covered by relevant external laws or regulations.

ITS assumes the responsibility of assuring that patches for operating systems or software environments are reasonably up to date for systems that it administers and will keep records of patching activity. Furthermore, ITS will seek to enforce: i) currency with respect to security level of all systems attached to the network; and ii) virus and worm protection of all systems attached
to the network. ITS will review its procedures for patches to operating systems and software, and will keep current on potential threats to the network and its data. Risk assessments will be updated annually in accordance with the Risk Assessment and Security Policy.

ITS bears primary responsibility for the identification of internal and external risk assessment, but all members of the college community are involved in risk assessment. ITS, working in conjunction with the relevant college offices, will conduct regular risk assessments, including but not limited to the categories listed by GLBA. Department heads will cooperate with the committee and play an active role in addressing security in their areas.

ITS is audited on a yearly basis by a third party, external auditing firm. At the conclusion of the audit process, the auditing firm presents a report to the Senior Leadership Team that includes suggested policy, control and procedural improvements and strategies for addressing the risk. The Senior Leadership Team then makes decisions on policy, procedures and associated controls, budget, and system operational and management changes. As new policies, procedures, and associated controls are implemented as a result of the risk assessment process, ITS, in collaboration with the SSC and applicable Data Owners, monitors the affected system(s) to verify that the implemented controls continue to meet expectations.

s, processes, and devices are limited to Authorized Users. Moreover, information system access is limited to the types of transactions and functions that authorized users are permitted to execute. The college’s administrative software systems schema and reports identify those users who have been granted such access. Moreover, the college annually conducts an audit that requires departmental supervisors to verify those individuals that may continue to have electronic access to Private College Data, including Covered Data and Information via the college’s administrative software systems.

In accordance with the Information Technology Physical and Environmental Protection Policy, ITS assures the physical security of ITS administered computers, including servers, which contain or have access to Private College Data, including Covered Data and Information. The SSC conducts a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures which may expose the college to risks.

While the college has discontinued usage of social security numbers as student identifiers, one of the largest security risks may be the possible non-standard practices concerning social security numbers, e.g. continued reliance by some college employees on the use of social security numbers. Social security numbers are considered protected information under both GLBA and the Family Educational Rights and Privacy Act (FERPA). By necessity, student social security numbers still remain in the college student information system. The college will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances students are inappropriately being asked to provide a social security number. This assessment will cover college employees as well as subcontractors such as the bookstore and food services.

ITS ensures that all electronic covered information Private College Data is encrypted in transit and that the central databases are strongly protected from security risks. See the Media Protection and Mobile Device Use and Support policies for additional information.
All Canisius College employees are expected to adhere to the Canisius College Standards of Ethical Conduct and other applicable policies. In addition, the college requires that all new college hires undergo background and reference checks prior to hire. See the college’s Background, Reference and Verification Screens Policy.

ITS has developed an Identity Theft Prevention Policy to detect and mitigate any actual or attempted attacks on covered systems. In addition, ITS has developed a contingency plan which includes incident response procedures for actual or attempted unauthorized access to Private College Data, including Covered Data and Information.

The information security coordinator will periodically review the college’s disaster recovery program and data-retention policies and propose necessary changes to the Senior Leadership Team.

III. Employee Management, Training, and Education

All Canisius College employees are expected to adhere to the Canisius College Standards of Ethical Conduct and other applicable policies. In addition, the college requires that all new college hires undergo background and reference checks prior to hire. See the college’s Background, Reference and Verification Screens and Information Technology Personnel Security policies.

While directors and supervisors are ultimately responsible for ensuring compliance with the college’s information security practices, controls and procedures, ITS and the SSC will work in cooperation with Human Resources to develop training and education programs for all employees who have access to Private College Data, including Covered Data and Information.

In addition to the above, ITS posts news of email scams, phishing attempts and other malicious actions to inform Authorized Users of possible threats.

Refer to the Information Technology Security Awareness and Training Policy for additional information.

IV. Oversight of Service Providers and Contracts

A. Covered Data and Information

The information security program requires the college to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. The Business and Finance Office will request assurances of GLBA compliance to all covered contractors.

At a minimum, contracts with service providers must include the following provisions:

1. An explicit acknowledgement that the contract allows the service provider access to Private College Data (including Covered Data and Information);
2. A specific definition or description of the Private College Data (including Covered Data and Information) permitted to be accessed by the service provider;
3. A stipulation that the Private College Data (including Covered Data and Information) will be held in strict confidence by the service provider and accessed only for the explicit business purpose of the contract;
4. An assurance in writing from the service provider that it will protect the Private College Data (including Covered Data and Information) it accesses according to commercially
acceptable standards (e.g., NIST 800-171 Standards) and no less rigorously than it protects its own confidential data. Service provider are required to acknowledge in writing that they are responsible for the security of Private College Data that the service provider possesses or otherwise stores, processes, or transmits on behalf of the college;

5. A provision providing that service provider personnel accessing Private College Data (including Covered Data and Information) possess the same level of security clearance as a college employee granted access to the same data;

6. A provision providing for the return or destruction of all Private College Data (including Covered Data and Information) received by the service provider upon completion or termination of the contract with the college;

7. An agreement that any violation of the contract’s confidentiality conditions may constitute a material breach of the contract and entitles the college to terminate the contract without penalty; and

8. A provision ensuring that the contract’s confidentiality requirements shall survive any termination agreement.

Refer also to the Payment Card Information Security Policy for vendor requirements applicable to the Cardholder Data Environment.

ITS, in collaboration with the applicable Data Owner, will monitor the vendor’s compliance with all contractually required information security-related policies and controls.

B. Cardholder Data

Canisius College does not store Cardholder Data in any of its information systems. Rather, Cardholder Data is stored by third-party vendors.

1. Third-party vendors that process, transmit or store Cardholder Data for the college must be PCI DSS compliant and approved by the vice president for business and finance and the chief information officer.

2. Third-party vendors will be required to conduct their own PCI DSS assessment, and must provide sufficient evidence to the chief information officer to verify that the scope of the service providers' PCI DSS assessment covered the services provided to the college and that the relevant PCI DSS requirements were examined and determined to be in place.

3. Third-party vendors are required to acknowledge in writing that they are responsible for the security of the Cardholder Data environment that the third-party possesses or otherwise stores, processes, or transmits on behalf of the college, or to the extent that they could impact the security of the Cardholder Data environment.

V. Evaluation and Revision of the Information Security Program

GLBA mandates that this program be subject to periodic review and adjustment. ITS will review its information security-related policies, controls, and procedures at least once each year. Processes in other relevant offices of the college such as data access procedures and the training program undergo regular review. The program itself as well as the related data retention policy are reevaluated annually in order to assure ongoing compliance with existing and future laws and regulations.

VII. Information Security Policy Exceptions Request
All departments are expected to comply with the ISP and college information security policies, which are designed to establish the controls necessary to protect College Data, including Covered Data and Information.

If a Data Owner determines that compliance with any information security policy and associated control or procedure adversely impacts a business process of the department, the Data Owner may request an exception as follows:

1. A Data Owner (or an appointed designee) seeking an exception must email the chief information officer for review. The written request must provide:
   a. Business or technical justification detailing the reasons for the exception, including the college policy and associated control for which the exception is being requested;
   b. Scope of the requested exception, including quantification (i.e., cost) and requested duration (not to exceed one (1) year);
   c. Analysis of all associated risks;
   d. Explanation of alternative controls to mitigate the risks;
   e. Explanation of any residual risks; and
   f. Approval of the area vice president that oversees the department requesting the exception;

2. The chief information officer will gather any necessary background information and make a recommendation to approve or deny the request;

3. The chief information officer will approve or deny the request for an exception;

4. The requestor will be notified of the decision to approve or deny;

5. All requests for exception will be retained by the chief information officer for the period of the exception; and

Exceptions are valid for a one-year period unless otherwise noted. If the exception is still required, the Data Owner may seek to renew the exception and provide any additional risks identified since the previous request. If the conditions have substantially changed, a new request for exception must be submitted to the chief information officer. Where little has changed, the review process may be shortened as recommended by the chief information officer.

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
Access Control Policy
Audit and Accountability Control Policy
Background, Reference and Verification Screens Policy
Cloud Computing Policy
Confidential Information Policy
Configuration Management Policy
Information Security Program
Health Insurance Portability and Accountability Act Policy
Identity Theft Prevention Policy
Identification and Authentication Policy
Information Security Program
Information Technology Personnel Security Policy
Information Technology Physical and Environmental Protection Policy
Information Technology Security Awareness and Training Policy
Media Protection Policy
Mobile Device Use and Support Policy
Password Policy
Record Retention and Disposal Policy
Standards of Ethical Conduct
Student Records (FERPA) Policy

Revision Feedback for 2.4.8.: Information Security Program Policy
Submit Feedback
INFORMATION TECHNOLOGY CHANGE CONTROL POLICY

Effective Date: May 6, 2019  
Policy Number: II – 2.4.9  
Supersedes: Not Applicable.  
Issuing Authority: President  
Responsible Officer: Chief Information Officer  
Applicability: All Canisius College departments.  
History:  

PURPOSE

The purpose of this policy is to manage changes to the college’s information systems, computer and network systems in a rational and predictable manner so that college employees can plan accordingly.

POLICY

All changes to the college’s computer and network information systems are subject to the formal change management processes set forth in this policy. Once approval is acquired, all related purchase requests (including hardware and software related purchases) must adhere to current college purchasing policies and procedures.

DEFINITIONS

Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

Change—anything that transforms, alters, or modifies the operating environment or standard operating procedures that have potential to affect the stability and reliability of ITS supported information technology resource system infrastructure and disrupt the business of the college. A change can be planned or unplanned.

College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

College Information System—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.
Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any Cardholder Data received in the course of business by the college, whether or not such Cardholder Data is covered by GLBA. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

Data Custodians—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

Data Owners—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

Encryption—the process of encoding (or scrambling) information so that it can only be converted back to its original form (decrypted) by someone who (or something which) possesses the correct decoding key.

Members of the College Community—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

Mobile Device—any handheld or portable computing device running an operating system optimized or designed for mobile computing that is capable of accessing, storing, and manipulating information in an untethered manner (usually, but not always, through a wireless connection). This includes, but is not limited to, laptops, tablets, smart phones/cell phones, PDAs, or other portable devices. Any device running a full desktop version operating system is not included in this definition.

Non-Public Personal Information—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

Personally Identifiable Information or PII—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s
maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

_Private College Data_—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the College Data Classification Policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, and Sensitive Authentication Data. See the Data Classification Policy for additional information.

_Public College Data_—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

_Sensitive Authentication Data_—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

_Student Education Records_—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

_Student Financial Information_—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

_Computer and Network Systems_—any college owned or leased computer, mobile device, or software, as well as any part of the college’s computer, data, voice or video networks physically located on any college owned, leased, or rented property or located on the property of any third party with the permission of that party. This includes devices on such networks assigned any routable and non routable IP addresses and applies to the college’s wireless network and the network serving the college’s student residence housing and any other vendor supplied network made available to the college community.

PROCEDURES/GUIDELINES

I. ___ Change Control Process
Information Technology Services (“ITS”) constantly assesses the college’s computer and network systems and considers changes as necessary. Steps leading up to and involving the change control process include the following:

1. Request for change (i.e., new version of software, bug fix, hardware purchases, etc.) triggers the need for the change control process;
2. Steps required to make the change are identified by Information Technology Services ITS in consultation with appropriate end user department staff;
3. Initial risk and impact on Canisius College is determined and documented;
4. A test plan is created;
5. A date of implementation is estimated based on who is affected and how long it will take to complete the change;
6. Appropriate approval is obtained (see below).

Requests for additional reviews of technology resources must be submitted to the chief information officer.

II. Approval and Schedule

Low Impact Changes: Low impact changes include installation of new information systems or reconfiguration of existing information systems where the procedure impacts only a minimal amount of Canisius College departments and can be reversed easily and quickly with minimum downtime. Low impact changes must be approved by the affected end user departments to ensure that the proposed change to Canisius College’s system, equipment and/or software will function properly with the college’s network configuration and that there is no duplication in equipment or services. Once approval is obtained, all system resource related purchase requests (including hardware and software related purchases) must adhere to current Canisius College purchasing procedures. Low impact changes can be made as soon as the change control request is approved.

Medium and High Impact Changes: Medium and High impact, strategic changes include installation of new information systems or reconfiguration of existing information systems that affect the entire college. The changes may also require significant down time. ITS must initially recommend to the Senior Leadership Team and president the change request to ensure that the proposed change to the system, equipment and/or software will function properly with Canisius College’s network configuration and that there is no duplication in equipment or services. Once final approval is obtained, all system resource related purchase requests (including hardware and software related purchases) must adhere to current Canisius College purchasing procedures. Changes can be made on the agreed upon date after approval as described above, proper notification, and testing.

Emergency Changes

There are situations where in order to support the continuity of Canisius College operations an emergency production change will be required. An “Emergency” includes any change, which if not implemented, would greatly impede college productivity or cause unacceptable additional costs. All emergency changes will be implemented pursuant to the ITS Management Escalation Procedures.

III. Notification Requirements
Upon approval, notification of changes is required as part of the change control process. The individuals notified will depend on several things including: department affected by the change, the level of risk involved, and the amount of downtime needed to make the change. Outside of emergency changes, the timing of notifications must be reasonable to allow for a response and any alternate plans that need to be made by those affected by the changes.

**IV. Accessibility**

In accordance with the Electronic Accessibility Policy, the college makes every reasonable effort to purchase information systems that are accessible to users with disabilities. Accessible, in this context, means compatible with assistive technology.

Prospective vendors will be requested to submit the Voluntary Product Accessibility Template (VPAT) published by the Information Technology Industry Council, describing the accessibility of their products and services, and such accessibility will be taken into consideration in making a purchasing decision. All college contracts for applicable resources will contain appropriate provisions concerning accessibility, as determined by ITS.

**V. Additional Acquisition Guidelines**

All information systems using any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the Data Classification Policy, as well as any associated services from a third-party vendor applicable to such systems (“applicable resources or services”) must be acquired and managed in accordance with the following information security guidelines:

**A. Requests for Proposals**

Requests for proposals to purchase applicable resources or services must include, either explicitly or by reference, information security requirements that describe:

1. Required security capabilities;
2. Required design and development processes;
3. Required test and evaluation procedures; and Required documentation as determined by ITS; and
4. The requirements in the request for proposal must also include text requiring the vendor to update security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

See also the Information Security Program for additional information regarding provisions that must be included in final contracts with service vendors.

**B. Information System Documentation**

All information system hardware must be tagged and inventoried in accordance with the college’s Procurement Policy and Purchasing Procedures. Moreover, ITS will ensure that administrator and user guides applicable to hardware are obtained from the vendor/manufacturer (or written in-house) and distributed to end users of the system. Such guides must include information on:

1. Configuring, installing, and operating the information system; and
2. Optimizing the system’s security features.
C. **Software Restrictions**

Authorized Users are prohibited from installing software on applicable college-owned and leased information system resources that are not approved by ITS. ITS identifies and publishes on its website the types of software installations that are permitted, including approved and tested updates and security patches to existing software. Only licensed and registered software approved by ITS may be used on college information systems.

Note that in accordance with the Peer-to-Peer File Sharing Policy, the use of peer-to-peer file sharing software is prohibited.

D. **Security Engineering Principles**

ITS is responsible for ensuring that applicable resources have security engineering principles applied to their specification, design, development, implementation, and modification of the resource system prior to the purchase being authorized.

E. **External Information System Services**

ITS ensures that third-party providers of applicable information system services employ adequate security controls in accordance with applicable laws, regulations, guidance, as well as established service level agreements. Final contracts with third-party vendors must include the following provisions:

9. An explicit acknowledgement that the contract allows the vendor to access to Private College Data (including Covered Data and Information);

10. A specific definition or description of the Private College Data (including Covered Data and Information) permitted to be accessed by the vendor;

11. A stipulation that the Private College Data (including Covered Data and Information) will be held in strict confidence by the vendor and accessed only for the explicit business purpose of the contract;

12. An assurance in writing from the vendor that it will protect the Private College Data (including Covered Data and Information) it accesses according to commercially acceptable standards (e.g., NIST 800-171 Standards) and no less rigorously than it protects its own confidential data. Vendors are required to acknowledge in writing that they are responsible for the security of Private College Data that the vendor possesses or otherwise stores, processes, or transmits on behalf of the college;

13. A provision providing that vendor personnel accessing Private College Data (including Covered Data and Information) possess the same level of security clearance as a college employee granted access to the same data;

14. A provision providing for the return or destruction of all Private College Data (including Covered Data and Information) received by the vendor upon completion or termination of the contract with the college;

15. An agreement that any violation of the contract’s confidentiality conditions may constitute a material breach of the contract and entitles the college to terminate the contract without penalty; and
16. A provision ensuring that the contract’s confidentiality requirements shall survive any termination agreement.

ITS, in collaboration with the applicable Data Owner, will monitor the vendor’s compliance with all contractually required security controls.

Refer also to the Payment Card Information Security Policy for vendor requirements applicable to the Cardholder Data Environment.

RELATED POLICIES

Configuration Management Policy
Computer Asset Replacement Policy
Data Classification Policy
Electronic Accessibility Policy
Information Security Program
Payment Card Information Security Policy
Peer-to-Peer File Sharing Policy
Procurement Policy and Purchasing Procedures
MOBILE DEVICE USE AND SUPPORT POLICY

Effective Date: May 6, 2019
Policy Number: II – 2.4.11
Supersedes: Not Applicable.
Issuing Authority: President
Responsible Officer: Chief Information Officer
Applicability: All Authorized Users accessing College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the college’s Data Classification Policy via a Mobile Device, as well as to all members of the college community using a Mobile Devices on campus or at a college activity. Both college-owned devices and personally-owned devices used to access college information.

History:

PURPOSE

The purpose for this policy is to outline the requirements and user expectations for reading and manipulating College Data on mobile devices. Mobile devices extend the security boundary of the campus, in that they allow for the transportation, storage, and manipulation of college information. This policy is intended to outline mechanisms for safeguarding that information. In addition, this policy outlines expectations with respect to the general use of mobile devices on the college campus or at college activities.

POLICY

The policies and procedures/guidelines relating to the use of mobile devices are below. The use of mobile devices is also subject to the college’s Acceptable Use Policy, the Standards of Ethical Conduct, Copyright and Intellectual Property Policy, and other applicable college policies.

The use of a mobile device to access College Data must be accomplished via secure and encrypted means if the mobile device is not directly connected to a college network. Unauthorized access to College Data utilizing a mobile device is prohibited.

In addition, users are prohibited from using mobile devices utilizing the college’s network(s) to violate copyrights including, but not limited to, copyrighted music, movies, software and publications. Moreover, photographing or digitally recording individuals with any mobile device that has photographic or video capturing capabilities in areas such as bathrooms, locker rooms, or other areas where there is a reasonable expectation of privacy, and/or taking photographs or video of an individual against their will is prohibited. Electronic transmission via the college’s network(s) of photographs or video of any person without the subject’s express permission is also prohibited. Finally, mobile devices may not be used on campus to record conversations unless all parties to the conversation give their consent, with the exception of recordings made for the purpose of law enforcement.
DEFINITIONS

**Authorized User**—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

**Cardholder Data**—full magnetic stripe or the Primary Account Number (PAN) plus any of the following: cardholder name; expiration date; service code; CVC2/CVV2/CID (a three- or four-digit number displayed on the signature panel of the card or, in the case of American Express, on the face of the card).

**College Data**—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

**College Employees**—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

**College Information System**—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

**College Network**—any part of the college’s data, voice, or video network physically located on any college owned, leased, or rented property or located on the property of any third party with the permission of that party. This includes devices on such network assigned any routable and non-routable IP addresses and applies to the college’s wireless network and the network serving the college’s student residence housing and any other vendor supplied network made available to the college community.

**Covered Data and Information**—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any Cardholder Data received in the course of business by the college, whether or not such Cardholder Data is covered by GLBA. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

**Data Custodians**—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

**Data Owners**—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.
**Encryption**—the process of encoding (or scrambling) information so that it can only be converted back to its original form (decrypted) by someone who (or something which) possesses the correct decoding key.

**Members of the College Community**—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

**Mobile Device**—any handheld or portable computing device running an operating system optimized or designed for mobile computing that is capable of accessing, storing, and manipulating information in an untethered manner (usually, but not always, through a wireless connection). This includes, but is not limited to, laptops, tablets, smart phones/cell phones, PDAs, or other portable devices. Any device running a full desktop version operating system is not included in this definition.

**Non-Public Personal Information**—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the Data Classification Policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, Cardholder Data, and Sensitive Authentication Data. See the Data Classification Policy for additional information.

**Public College Data**—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

**Remote Wipe**—the ability to erase all data on a device when the user and the device are physically separated. This is most often done through a service that the manufacturer provides via a website.
**Security Patch**—a fix to a program or application that eliminates a vulnerability exploited by malicious hackers. Most mobile devices will notify the user of updates to their installed applications that include the latest vulnerability fixes.

**Sensitive Authentication Data**—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

**Student Education Records**—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

**College Information**—any data related to the business of the college including, but not limited to: financial, personnel, student, alumni, communication, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. Examples include: credit card information; tax identification numbers; payroll information; check requests and associated paperwork; student, parent, and employee tuition, financial aid, and loan accounts information; student educational records as defined by FERPA; photographic images (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); medical or financial information for any employee, temporary worker, or student; other personal information to include date of birth, address, phone numbers, maiden names, student/customer numbers, social security numbers; college contracts; college research data; alumni and donor records; personnel records; college financial data; computer passwords; college proprietary information/data; and any other information for which access, use, or disclosure is not authorized by: a) federal, state, or local law; or b) college Policy or operations.

**Mobile Device**—any handheld or portable computing device including running an operating system optimized or designed for mobile computing. Any device running a full desktop version operating system is not included in this definition.

**User**—any individual granted access by ITS to the campus Exchange environment, or the college outlook web access portal.
PROCEDURES GUIDELINES

I. College-Issued Mobile Devices

Certain college employees are required to use Mobile Devices to facilitate college business. Budget directors and/or managers in consultation with the appropriate vice president will determine when college-funded Mobile Devices is appropriate for employees. There must be a clear business case for issuance of the Mobile Device.

Employees issued a college-owned or leased Mobile Device are subject to the college’s Acceptable Use Policy, the Standards of Ethical Conduct, Copyright and Intellectual Property Policy, and other applicable college policies, as well as the Mobile Device Security Control Requirements set forth in Section III below.

Mobile Devices acquired and issued by the college, including the data/voice records and College Data stored therein, remain the property of the college and must be surrendered to ITS upon discontinuation of service or employment.

II. Personally-Owned Mobile Devices

The college recognizes and allows Authorized Users to connect personally owned Mobile Devices to the college’s network(s). Authorized Users accessing the college’s network(s) via a personally-owned Mobile Device are subject to the Acceptable Use Policy, the Standards of Ethical Conduct, Copyright and Intellectual Property Policy, and other applicable college policies, as well as the Mobile Device Security Controls Requirements set forth in Section III below.

In accessing the college network(s) with a personal Mobile Device, the Authorized User understands and agrees that the college will not reimburse or otherwise compensate the user for any costs associated with accessing the college network(s). Such costs may include, but are not limited to, monthly call and data plans, long distance calling charges, additional data or roaming fees, charges for excess minutes or usage, equipment, surcharges and any applicable fees or taxes. The Authorized User also understands that he/she may be held liable for any criminal and/or civil penalties that may result from loss, theft or misuse of College Data accessed and/or stored on the personal Mobile Device.

Upon termination of affiliation with the college, Authorized Users who have used a personal Mobile Device to access College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the college’s Data Classification Policy agree to immediately delete all College Data classified as Private-Highly Restricted and Private-Restricted (“Private College Data”) stored on the device. Moreover, Authorized Users must remove all college email accounts from the device. Failure to complete the above may result in the device being remote wiped by ITS.

III. Mobile Device Security Control Requirements

Authorized Users who access College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the college’s Data Classification Policy via a Mobile Device must adhere to the following security control requirements governing the use of any Mobile Devices to access the
college’s network(s), regardless of whether or not the device was purchased or leased with college funds.

Device Precautions

The following security requirements govern the use of any mobile devices that are used on the college’s network(s), regardless of whether or not the device was purchased with college funds:

1. Remote access to the college’s nonpublic-facing information systems will be protected via secure or encrypted protocols. Only those employees and contractors whose job duties require this level of access will be granted remote access (see the Access Control and Identification and Authentication policies);

2. All mobile devices accessing the college’s network(s) must be updated to the latest device operating system with the latest security patches and anti-virus software.

3. All applications must be updated with the latest security patches;

4. Authorized Users may not allow someone who is not authorized access to the college network to use their devices if the device has been used to store, access and/or process Private College Data;

5. All devices that have been used to store, access and/or process Private College Data must delete the data stored on their devices immediately after the work with it is completed;

5-6. All devices with direct connectivity to the Internet and the ability to access and/or process Private College Data must have firewall software or equivalent functionality installed on the device
   a. Firewall software must be audited by ITS; and
   b. Configuration settings of the firewall software must not be alterable by the Authorized User of the Mobile Device;

6. All devices must be configured with a PIN, passcode, or password-enabled lock screen configured to activate at no more than 5 minutes of inactivity;

8. All devices with built-in encryption capability must have the device’s encryption enabled;
   a. Authorized Users may not transmit unencrypted Private College Data via texting messages, instant messages, emails, or voicemail.

7-9. All devices must have “remote wipe” enabled through a third-party application or the manufacturer’s website;

8-10. All devices that have been used to store, access and/or process college administrative information must be wiped to remove such data before they are transferred to someone else through sale or gifting;

9-11. In the event that a device which has been used to store, access and/or process administrative information becomes lost, stolen or compromised, the owner must contact ITS;

12. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the college’s network(s).
40-13. If a Mobile Device used to access Private College Data is lost or stolen, the Authorized User must contact ITS to report the missing device.

I. Consent

Users of personally owned handheld devices may access information through the Outlook web access portal. In accessing the portal with a personal mobile device, the user understands and agrees that the college will not reimburse or otherwise compensate the user for any costs associated with accessing the college network with a personal mobile device. Such costs may include, but are not limited to, monthly call and data plans, long-distance calling charges, additional data or roaming fees, charges for excess minutes or usage, equipment, surcharges and any applicable fees or taxes. The user also understands that he/she may be held liable for any criminal and/or civil penalties that may result from loss, theft or misuse of the administrative data accessed and/or stored on the personal device.

Upon termination of affiliation with the college, users agree: (a) to immediately delete all college information stored on the device; and (b) to remove the college email account and Wi-Fi settings from the device. Failure to complete the above may result in the device being wiped by ITS.

V. Initial Configuration

To ensure proper initial configuration of handheld Mobile Devices, users should consult with ITS before purchasing a new device to verify its suitability for the college’s network environment.

For allowed college-owned or leased devices, ITS will configure the device to access the campus email and calendar resources. A brief orientation session on proper use of the device can be scheduled with either ITS User Services or the Center for Online Learning and Innovation.

For allowed personal Mobile Devices, ITS will provide written procedures for configuring devices to access campus resources. It is the responsibility of the owner to configure the device properly, and should they need assistance, contact their service provider for further assistance.

V. Support

For allowed college-owned or leased Mobile Devices, Authorized Users should contact the Help Desk for assistance. ITS will handle all technical issues on behalf of the college.

For allowed personal Mobile Devices, users should contact their service provider for troubleshooting assistance.

VI. Student Use of Mobile Devices in the Classroom

Mobile Devices may not be used in a manner that causes disruption in the classroom or library. Moreover, Canisius College does not allow the use of such devices to photograph or video any classes without instructor permission. Abuse of devices with photographic or video capabilities for purposes of photographing test questions or materials is a violation of Canisius College policy.

VIII. Risks/Liabilities/Disclaimers

While the college will take every precaution to prevent the user’s personal data from being lost in the event it must remote wipe a device, it is the user’s responsibility to take additional precautions, such as backing up notes, documents, application data, etc. The college reserves the right to disconnect devices or disable services without notification.
The user is personally liable for all costs associated with a non-college issued device and assumes full liability for risks including, but not limited to, the partial or complete loss of college and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

**VIII. Enforcement**

Each [Authorized User](#) of college information systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data, as well as a member of the college community using a Mobile Device on campus or at a college activity, both college-owned devices and personally owned devices used to access college information is responsible for following this policy.

**IX. Sanctions**

Students and employees who violate the provisions of the policy may be subject to disciplinary action pursuant to the college’s applicable disciplinary policies, as well loss of access to the college’s ITS information systems and resources.

Visitors and others third-party users who violate the provisions of this policy are subject to loss of access to the college’s ITS resources. Moreover, the vice president for business and finance may administer other appropriate sanctions.

**RELATED POLICIES**

- [Acceptable Use of College Computer and Network Systems Policy](#)
- [Access Control Policy](#)
- [Cloud Computing Policy](#)
- [Data Classification Policy](#)
- [Identification and Authentication Policy](#)
- [Intellectual Property Rights and Ownership Policy](#)
- [Standards of Ethical Conduct](#)
- [Information Security Program](#)
## PASSWORD POLICY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>May 6, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number:</td>
<td>II – 2.4.12</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>Not Applicable.</td>
</tr>
<tr>
<td>Issuing Authority:</td>
<td>President</td>
</tr>
<tr>
<td>Responsible Officer:</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Applicability:</td>
<td>Anyone who has been issued authentication credentials for an account on any College Information System (“applicable information system”) that resides at any Canisius College facility, has access to the Canisius College network, or stores any non-public Canisius College Private College Data information. This includes both members of the Canisius community, such as faculty, staff, or students, as well as members of third-party organizations granted access to college resources.</td>
</tr>
</tbody>
</table>

### HISTORY:

**PURPOSE**

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the procedures and guidelines for resetting passwords.

**POLICY**

It is the policy of Canisius College that anyone who has been issued authentication credentials for an account on any information system that resides at any Canisius College facility, has access to the Canisius College network, or stores any non-public Canisius College information, including both members of the Canisius community, such as faculty, staff, or students, as well as members of third-party organizations granted access to college resources (“user”), adhere to the password procedures and policy guidelines set forth in this policy. At no time should a user grant access to his/her account by providing someone else the password.

**DEFINITIONS**

*Authorized User*—anyone who has been issued authentication credentials for an account on any system that resides at any Canisius College facility, has access to the Canisius College network, or stores any non-public Canisius College information, including both members of the Canisius community, such as faculty, staff, or students, as well as members of third-party organizations granted access to college resources

**PROCEDURES/GUIDELINES**

Passwords are an important aspect of information technology resource security. A poorly chosen password may result in the compromise of the college’s entire network. Accordingly, all newly generated or issued passwords will be strong passwords, as described below.

**I. Generating Passwords**
Default passwords must be changed by the Authorized User immediately upon receipt from ITS. In selecting a new password, Authorized Users must select strong passwords. Accordingly, all passwords must have the following characteristics:

1. Contain both upper and lower case characters (e.g., a-z, A-Z);
2. Have digits and punctuation characters as well as letters e.g., @/$&"(),<>`;=#; dash, underscore, pound and others as defined on the Canisius password change web form or in the wiki password creation tips;
3. Are at least eight characters in length;
4. Are not a word in any language, slang, dialect, jargon, etc.;
5. Cannot contain user’s name (last or first) and must not be based on personal information, names of family, etc.;
6. Passwords must never be stored on electronic media in unencrypted clear text form. Strong encryption must be used. When writing passwords down, keep them in a secure place that is not easily accessible to others;
7. Password history will be enforced for end users of the college’s administrative ERP system applicable information systems.

Weak passwords have the following characteristics:

1. The password contains less than eight characters
2. The password is a word found in a dictionary (English or foreign)
3. The password is a common usage word such as:
   a. Names of family, pets, friends, co-workers, fantasy characters, etc.
   b. Computer terms and names, commands, sites, companies, hardware, software.
   c. Birthdays and other personal information such as address and phone numbers.
   d. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
   e. Any of the above spelled backwards.
   f. Any of the above preceded or followed by a digit (e.g., secret!, 1secret).

Authorized Users are encouraged to try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "Tmb1w2R!" or "Tmb1W>r~" or some other variation. (NOTE: Do not use either of these examples as passwords!)

Password cracking or guessing may be performed on a periodic or random basis by ITS. If a password is guessed or cracked during these exercises, the Authorized User will be required to change it.

II. Protecting Passwords
All passwords are to be treated as sensitive, confidential Canisius College information. Here is a list of “don’ts”:

1. Do not use the same password for Canisius College accounts as for other non-Canisius College access (e.g., personal ISP account, option trading, benefits, etc.);
2. Do not share Canisius College passwords with anyone, including administrative assistants or secretaries;
3. Don't reveal a password over the phone to ANYONE;
4. Don't reveal a password in an email message;
5. Don't talk about a password in front of others;
6. Don't hint at the format of a password (e.g., "my family name");
7. Don't reveal a password on questionnaires or security forms;
8. Don't share a password with family members;
9. Don't use the "Remember Password" feature of applications (e.g., Firefox, Thunderbird.);
10. Don't store passwords in a file on ANY computer system without encryption;
11. Passwords routed over the college network must be encrypted;
12. Passwords must be masked upon entry (e.g., displaying asterisks or dots when a user types in a password) and not displayed in clear text.

If an account or password is suspected to have been compromised, report the incident to ITS and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by ITS or its delegates. If a password is guessed or cracked during one of these scans, the user will be notified and required to change it.

### III. Forgotten Passwords

In the event that a password is forgotten:

1. A self-service forgotten password reset program is available at [http://apps.canisius.edu/pwforgot](http://apps.canisius.edu/pwforgot). Only authorized, full time employees of the Canisius College may reset passwords by means other than the self-help program. A log of Authorized Users will be kept by the chief information officer.
2. A self-service password reset program is available for end users at: [http://www.canisius.edu/passwordreset](http://www.canisius.edu/passwordreset);
3. No passwords will be changed on behalf of a computer user without positive identification such as a Canisius College ID card;
4. If the user cannot come to the Help Desk, then resets may be performed over the phone after alternate verification of the user’s identity;
5. Reset passwords will follow the guidelines for strong passwords above; and
6. If technically possible, the new password that is reset on behalf of a computer user will be set to expire upon first use by the user, who will then be prompted to choose a new password.

IV. Privileged Account Passwords

There are additional rules that apply to ITS personnel and vendors in the use of privileged accounts and in the initial configuration of network equipment.

1. All production system-level passwords must be part of the Information Technology Services (ITS) administered global password management database;

2. User accounts that have system-level privileges granted through group memberships or programs such as “sudo” must have a unique password from all other accounts held by that user;

3. Where SNMP is used, the community strings must be defined as something other than the standard defaults of “public,” “private” and “system” and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2);

4. Under no circumstances will the ITS person who changes a user password attempt to access any data and/or applications of that user beyond simple verification of the password reset. Violation of this provision will result in the most serious disciplinary consequences, up to termination of employment.

V. Application Development Standards

Application developers must ensure their programs contain the following security precautions.

1. Applications should support authentication of individual users, not groups;

2. Applications should not store passwords in clear text or in any easily reversible form;

3. Applications should provide for some sort of role management; such that one user can take over the functions of another without having to know the other’s password;

4. Applications should support CAS, TACACS+, RADIUS, and/or X.509 with LDAP security retrieval, wherever possible.

5. Applications must enforce the changing of passwords and the minimum length;

VI. Password Expiration

All faculty and staff passwords will be scheduled to expire 180 days from the date they were last set.

Advance warnings of upcoming password expiration will be sent to the account holder via campus email beginning 30 days prior to expiration, with repeated reminders thereafter until the expiration date or until your password is changed. An account holder may change his or her password at any time -- it is not necessary to wait for expiration.

Please note that no data will be lost between the time a password expires and the time it is reset. Email accounts will continue to receive messages during this period but existing mail will not be accessible and new mail will not be able to be sent out.

VII. Enforcement
Any employee or student found to have violated this policy may be subject to disciplinary action in accordance with applicable college policy.

**RELATED POLICIES**

- Acceptable Use of College Computer and Network Systems Policy
- Access Control Policy
- Acquisition and Disposal Policy
- Audit and Accountability Control Policy
- Configuration Management Policy
- Data Classification Policy
- Electronic Mail Policy
- Information Security Program
- Information Technology Personnel Security Policy
- Information Technology Security Awareness and Training Policy
- Media Protection Policy
- Mobile Device Policy
- Passwords Policy
SUPPORTED COMPUTER, EQUIPMENT, AND SOFTWARE INFORMATION TECHNOLOGY MAINTENANCE POLICY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>May 6, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number:</td>
<td>II – 2.4.15</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>Not Applicable.</td>
</tr>
<tr>
<td>Issuing Authority:</td>
<td>President</td>
</tr>
<tr>
<td>Responsible Officer:</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Applicability:</td>
<td>All Authorized Users of college information systems and resources that collect, process, maintain, use, share, disseminate or dispose of College Data. All Users of Canisius College supported equipment and software.</td>
</tr>
<tr>
<td>History:</td>
<td></td>
</tr>
</tbody>
</table>

PURPOSE

The purpose of this policy is to protect the college’s information systems and resources. Maintenance provides continued security, functionality, and stability within the college’s information system by implementing the necessary controls that dictate the required procedures for auditing, configuring, and disposal of information system resources. Describe those services that are available for college supported computers, equipment, and software. This policy also sets forth the college’s procedural guidelines regarding laptop repairs.

POLICY

It is the policy of Canisius College to provide sufficient technical support to correct hardware failures in order to reduce the risk of impact to College Data and administrative operations. The Office of Information Technology Services (“ITS”) is charged with the responsibility to service college supported computers, equipment, and software. For a listing of supported equipment, please see the Procedures/Guidelines section of this policy.

DEFINITIONS

**Authorized User**—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

**College Data**—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

**College Employees**—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

**College Information System**—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term...
system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

*Covered Data and Information*—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any Cardholder Data received in the course of business by the college, whether or not such Cardholder Data is covered by GLBA. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

*Data Custodians*—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

*Data Owners*—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

*Encryption*—the process of encoding (or scrambling) information so that it can only be converted back to its original form (decrypted) by someone who (or something which) possesses the correct decoding key.

*Members of the College Community*—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

*Mobile Device*—any handheld or portable computing device running an operating system optimized or designed for mobile computing that is capable of accessing, storing, and manipulating information in an untethered manner (usually, but not always, through a wireless connection). This includes, but is not limited to, laptops, tablets, smart phones/cell phones, PDAs, or other portable devices. Any device running a full desktop version operating system is not included in this definition.

*Non-Public Personal Information*—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.
**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the College Data Classification Policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, Cardholder Data, and Sensitive Authentication Data. See the Data Classification Policy for additional information.

**Public College Data**—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

**Sensitive Authentication Data**—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

**Student Education Records**—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format. Not applicable.

**PROCEDURES/GUIDELINES**

**I. Controlled Maintenance**

**ITS:**

1. Schedules, performs, documents, and reviews records of maintenance and repairs on applicable college information systems and resources in accordance with manufacturer or vendor specifications;
2. ITS includes the following information in maintenance and repair records:
   a. Date and time of maintenance;
   b. Name of individuals performing the maintenance;
   c. Name of the college employee escorting third-party vendors performing maintenance activities, as necessary;
   d. A written description of the maintenance performed; and
   e. System components/equipment removed or replaced, including the identification number, if applicable.

3. Controls all maintenance activities, whether performed at a college facility or remotely and whether the equipment is serviced on site or removed to another location;

4. Requires that the director of user services or director of infrastructure (or his/her designee) explicitly approve the removal of the resource or resource components from college facilities for off-site maintenance or repairs;

5. Sanitizes equipment to remove all Private College Data from associated media prior to removal from college facilities for off-site maintenance or repairs; and

6. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

II. Maintenance Personnel

A. College Maintenance Personnel

The chief information officer (or his/her designee) ensures that college employees performing maintenance on a college information system or resource have required access authorizations or designates college personnel with required access authorizations and technical competence deemed necessary to supervise maintenance when maintenance personnel do not possess the required access authorizations.

B. Remote Maintenance

ITS, with the approval of the chief information officer (or his/her designee):

1. Approves and monitors remote maintenance and diagnostic activities;

2. Approve special access credentials to third-party personnel and consultants who legitimately require privileged access to a college information system or resource to conduct maintenance or diagnostic activities;

   a. In contracting with an outside third-party vendor or consultant, ITS must ensure the vendor or consultant has the ability to safeguard Private College Data prior to issuing the special access credential;

   b. Contract must meet the requirements outlined in the Selection of Appropriate Third-Party Vendors Providers section of the college’s Information Security Program;

4-3. Audits remote maintenance and diagnostic sessions; and
4. Reviews the records of the remote maintenance and diagnostic sessions.

**III. Supported Software**

For supported software packages (see [wiki.canisius.edu](http://wiki.canisius.edu) for a current listing), ITS provides consulting services, training, documentation, and acts as a technical liaison between Authorized Users and the vendor’s software consultants. Software that is not listed as supported will receive “limited support.” ITS will provide consulting for such software on a time available basis. Please note that ITS does not have the expertise to recommend the statistical methods appropriate for particular data analysis.

**IV. Supported Equipment and Computer Repair**

ITS will repair college-owned computers and computer peripherals (except for printers) provided that:

1. The equipment was purchased based on ITS recommendations and/or standards;
2. The equipment is logged in the Canisius College inventory system and was originally installed by ITS or its agents;
3. Parts can be located and are reasonably priced;
4. The equipment is still functional, fills a business/educational need, and is sufficiently current that reasonable support can be provided. Reasonable support precludes items where support personnel require additional specialized training, where documentation fails to exist or is difficult to locate, or where the cost to repair at ITS expense exceeds the cost to upgrade equipment; and
5. Failures are not caused by abuse, misuse, neglect or vandalism. Failures caused by departments who attempt to move equipment on their own, or by agents other than ITS, will be charged for repairs.

Currently ITS will move (“trickle down”) computers to a new location if they are still usable ([see the Computer Asset Replacement Policy](#)). Older computers may be able to be supported as long as they are used in their present location.

Equipment problems should be reported to the Help Desk at (716) 888-8340. ITS will attempt to respond to trouble calls within one business day. When spares of like equipment are available, ITS will loan this to the user while theirs is replaced or repaired. Some laptop repairs can be performed only by the manufacturer, in which case ITS will facilitate the repair.

Authorized Users should consider [consult with ITS if](#) maintenance contracts for critical equipment is needed.

**V. Repair of Damaged Laptops**

ITS repairs college-owned desktop and laptop computers when problems result from normal wear and tear. Damage to computers, especially laptop computers, which results from neglect, abuse, or improper handling, is not covered by User Services. In the latter case, the individual employee assigned the computer or the department of that employee is responsible for the cost of the repair. User Services will perform or facilitate the repair or replacement as appropriate.

Laptop computer users are advised to take special care of their computers when traveling. College laptop computers are at risk of becoming severely damaged when they are placed in the overhead
bins on airplanes. ITS recommends that all college-owned laptop computers be placed under the seat in front of the passenger when traveling by air.

RELATED POLICIES

Computer Asset Replacement Policy
Data Classification Policy
Information Security Program
Information Technology Personnel Security Policy

Identification and Authentication Policy
Media Protection Policy

Mobile Device Use and Support Policy
Payment Card Security Policy
System and Communication Protection Policy
System and Information Integrity Policy

Repair of Laptop Computers Policy TBA
WIRELESS ACCESS POINTS POLICY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>May 6, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number:</td>
<td>II – 2.4.16</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>Not Applicable.</td>
</tr>
<tr>
<td>Issuing Authority:</td>
<td>President</td>
</tr>
<tr>
<td>Responsible Officer:</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Applicability:</td>
<td>All users of the Canisius College’s wireless access points.</td>
</tr>
<tr>
<td>History:</td>
<td></td>
</tr>
</tbody>
</table>

PURPOSE
The purpose of this policy is to provide guidelines regarding the installation and use of wireless access points on the college campus.

POLICY
In order to provide wireless access to authorized users, the Office of Information Technology Services (“ITS”) installs “access points” in and around the campus. These access points are generally small, antenna-equipped boxes that connect directly to the local area network (LAN), converting the LAN’s digital signals into radio signals. The radio signals are sent to the network interface card (NIC) of the mobile device (e.g. smartphone, IPad, laptop, etc.), which then converts the radio signal back to a digital format the mobile device can use. All Authorized Users employing wireless methods of accessing the college’s network systems must use Canisius College approved access points.

Personally-owned and unauthorized wireless access points that are installed without the knowledge or permission of ITS and used by individuals to gain unauthorized access to the college network are strictly prohibited. Any unapproved personal access point discovered in operation and connected to the college network is subject to being disabled and/or removed immediately and indefinitely.

Use of the Canisius College wireless network is subject to the college’s Acceptable Use of College Computer and Network Systems Policy and Information Security Program.

DEFINITIONS
Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.
College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

College Information System—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any Cardholder Data received in the course of business by the college, whether or not such Cardholder Data is covered by GLBA. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.

Data Custodians—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

Data Owners—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

Encryption—the process of encoding (or scrambling) information so that it can only be converted back to its original form (decrypted) by someone who (or something which) possesses the correct decoding key.

Members of the College Community—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

Mobile Device—any handheld or portable computing device running an operating system optimized or designed for mobile computing that is capable of accessing, storing, and manipulating information in an untethered manner (usually, but not always, through a wireless connection). This includes, but is not limited to, laptops, tablets, smart phones/cell phones, PDAs, or other portable devices. Any device running a full desktop version operating system is not included in this definition.

Non-Public Personal Information—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection
with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the College Data Classification Policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, Cardholder Data, and Sensitive Authentication Data. See the College Data Classification Policy for additional information.

**Public College Data**—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

**Sensitive Authentication Data**—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

**Student Education Records**—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.
**Wireless Access Point**—a network device that serves as a common connection point for devices in a wireless network. Access points use radio frequency spectrum instead of wired ports for access by multiple users of the wireless network. Access points are shared bandwidth devices connected to the college wired network.

**Wireless Network**—network technology that uses radio frequency spectrum to connect computing devices to a wired port on the college’s network.

**College Information**—is any data related to the business of the college including, but not limited to: financial, personnel, student, alumni, communication, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. Examples include: credit card information; tax identification numbers; payroll information; check requests and associated paperwork; student, parent, and employee tuition, financial aid, and loan accounts information; student educational records as defined by FERPA; photographic images (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); medical or financial information for any employee, temporary worker, or student; other personal information to include date of birth, address, phone numbers, maiden names, customer numbers, social security numbers; college contracts; college research data; alumni and donor records; personnel records; college financial data; passwords; college proprietary information/data; and any other information for which access, use, or disclosure is not authorized by: a) federal, state, or local law; or b) college policy or operations.

**Computer and Network Systems**—any college owned or leased computer, mobile device, or software, as well as any part of the college’s computer, data, voice or video networks physically located on any college owned, leased, or rented property or located on the property of any third party with the permission of that party. This includes devices on such networks assigned any routable and non-routable IP addresses and applies to the college’s wireless network and the network serving the college’s student residence housing and any other vendor supplied network made available to the college community.

**Mobile Device**—any handheld or portable computing device including running an operating system optimized or designed for mobile computing, such as Android, Blackberry OS (RIM), Apple’s iOS, or Windows Mobile. Any device running a full desktop version operating system is not included in this definition.

**Users**—any individual granted access by the Information Technology Services to a college computer and network system.

**PROCEDURES/GUIDELINES**

I. **Wireless Access Point Approval**

All wireless access points within the college’s firewall must be approved and centrally managed by ITS. The addition of new wireless access points within campus facilities will be managed at the sole discretion of ITS staff.

ITS will periodically conduct sweeps of the wireless network to ensure there are no unauthorized access points present.
ITS reserves the right to turn off without notice any access point connected to the network that it feels puts the college’s network, information systems, College Data, or Authorized Users at risk. Access point broadcast frequencies and channels are set and maintained by ITS. Any device or equipment found to be interfering with access point signals may be subject to relocation or removal, including cordless phones, microwave ovens, cameras, light ballasts, etc.

Wireless access users agree to immediately report to ITS any incident or suspected incidents of unauthorized access point installation.

II. Enforcement

ITS is responsible for the appropriate enforcement of this policy. During the course of any investigation of alleged inappropriate or unauthorized use, it may be necessary to temporarily suspend a user’s network or computing privileges, but only after determining there is at least a prima facie case against the individual, as well as a risk to the college network if privileges are not revoked. This is a necessary action taken to prevent further misuse and does not presume that the user initiated the misuse. Unsubstantiated reports will not result in the suspension of user account or network access unless sufficient evidence is provided to show that inappropriate activity occurred.

III. Sanctions

Students and employees who violate the provisions of this policy are subject to disciplinary action pursuant to the college’s applicable disciplinary policies, as well as loss of access to the college’s network. They may also be subject to criminal and/or civil proceedings.

Visitors and others third party users who violate the provisions of the policy are subject to loss of access to the college’s network. They may also be subject to criminal and/or civil proceedings. In addition, the vice president for business and finance may administer other appropriate sanctions.

IV. Disclaimer and Limitation of Liability

Canisius College makes no representations as to the performance, accuracy, or reliability of the college’s information technology resources. The college disclaims all warranties of any kind, expressed or implied, to the fullest extent permissible pursuant to applicable law, including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

By using the college’s wireless access network, users agree that Canisius College, its trustees, or employees have no liability whatsoever for damages in any form under any theory of liability or indemnity in connection with a user’s use of the college’s network, even if the college has been advised of the possibility of such damages. Authorized Users further recognize that the college has no control over the content of information servers on external electronic systems or the Internet accessed via the college’s wireless network. The college, therefore, disclaims any responsibility and/or warranties for information and materials residing on non-college information servers on external electronic systems or the Internet. Such materials do not necessarily reflect the attitudes, opinions, or values of Canisius College.

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
PURPOSE

The purpose of this policy is to establish policy guidelines and procedures governing official college interactions with state and federal legislators and governmental agencies by members of the college community.

POLICY

Subject to specific control by the Board of Trustees, all official interactions on behalf of Canisius College (including the college’s schools, departments, divisions, offices, centers, programs, etc.) with government offices, boards, agencies or legislators are subject to the direction of the college president or an authorized designee. Individuals seeking to officially interact on behalf of the college with such offices, boards, agencies or legislators must be authorized to do so by the president.

Personal Contacts

Contacts with government officials and staff of a personal nature, whether in writing or in person, must be made in the name of the individual making the contact and may in no way imply that the contact is being made on behalf of the college. College letterhead and email may not be used in presenting a personal view in such cases.

Professional Contacts

Professional contacts with government officials and staff, whether by letter, email, telephone, social media, or in person, must be done in the name of the individual making the contact or on behalf of the applicable professional society, and not on behalf of the college. Reference to affiliation with the college may be made as an aid to identification.

DEFINITIONS

Not applicable.

PROCEDURES/GUIDELINES

1. Invitations to Government Officials
The college president is to be informed in advance of invitations to government officials and/or their staff to visit any campus or facility of the college in their official capacity to ensure coordination with key college offices and awareness of political sensitivities.

II. Official Requests from Government and Accreditation Officials

When requests for information, expertise, resources, or visits are received from governmental officials and/or staff for the purposes of gathering information and/or making assessments of college activities, college offices must notify the college president for assistance with the request, including coordination with relevant college offices, as appropriate.

III. Other Activities Requiring Advance Approval

Members of the college community must also contact the college president prior to any interactions with government officials under the following circumstances:

1. Would like to make a gift to a government official, including the purchase of a meal;

2. Are considering directly contacting a government official with respect to legislation or executive actions or decisions on government policies, programs or regulations; or with respect to government funding, including contracts and grants (note exclusions below);

3. Are considering indirectly contacting a government official, through avenues such as the media or other “grassroots lobbying”, in attempt to influence actions or decisions regarding legislation or executive actions or decisions on government policies, programs or regulations; or with respect to government funding, including contracts and grants (note exclusions below).

The president or a designee will review the proposed interaction, which may be reportable on city, state, or federal levels, and will provide guidance on the interaction.

IV. Exclusions

Faculty and non-faculty researchers as well as staff in Institutional Advancement who are assisting government officials do not need to seek authorization from the college president prior to engaging in the following interactions: (a) the provision of policy expertise or testimony in the researcher’s field of expertise; (b) contact with program and grant/program officers to discuss prospective or ongoing governmental funding projects that have been, or will be, awarded through a competitive review process.

Members of the college’s faculty should be in contact with Institutional Advancement when approaching government officials regarding funding.

RELATED POLICIES

Political Activities and Speakers Policy
Standards of Ethical Conduct
PURPOSE
The purpose of this policy is to clarify under what circumstances photography, digital recording, and filming on the Canisius College campus is permitted.

POLICY
Photography and Filming by Outside Businesses and Hobbyist
Outside businesses (e.g., media professional photographers or videographers, organizations, and companies) and hobbyists occasionally seek authorization to film or photograph a particular site or building at Canisius College’s campus. Any requests for filming and/or photography by outside businesses and hobbyists on college property must be submitted in writing to the Office of College Communications, Office of Marketing and Brand Engagement, which reviews them in consultation with the college president, to determine whether they are compatible with the college’s mission and goals. The Office of College Communications reserves the right to deny requests that reflect negatively on the College or will interfere with its routine operations. The Office of College Communications, Office of Marketing and Brand Engagement in consultation with the appropriate member of the Senior Leadership Team then makes the final determination on whether requests will be accommodated.

Individuals receiving a request for filming or still photography on campus must direct the individual to the Office of College Communications, Office of Marketing and Brand Engagement.

Amateur Photography and Filming by College Community Members and Guests
Amateur photography, recording, and filming by members of the college community and their guests at college sanctioned events considered open to the public (i.e., commencement) is generally permitted provided the consent of the subject(s) has been obtained. Consent is not required when the individual is photographing, recording, or filming general crowd shots of an event. Otherwise, such activities must be conducted in a non-disruptive manner and in compliance with applicable college policies.

Photography and Video (i.e., Digital Images) Consent
Current students, faculty, staff, and alumni of the College: Canisius students, faculty and staff are advised that the Office of College Communications, Office of Marketing and Brand Engagement
takes photographs and video recordings throughout the year in various locations on and off campus. These photographs and video recordings often include the names, images, voices and likenesses of Canisius students, faculty and staff. Canisius reserves the right to use these photographs and videotapes as part of its publicity and marketing efforts without the expressly-written consent of the above-mentioned individuals. Additionally, students who enroll at Canisius do so with the understanding that these photographs and videotapes might include their names, images, voices and likenesses, and such photographs or videotapes might be included, published, or used in Canisius publications including print, broadcast, or electronic media, for publicity, commercial, or marketing purposes. Enrollment at Canisius constitutes students’ consent to the inclusion, publication, or use of their names, images, voices, and likenesses, taken while enrolled at Canisius, for publicity, commercial, promotional or marketing purposes, with unlimited use and for an unspecified time period.

**Individuals who are not Canisius students, faculty or staff:** Photographs and video recordings taken by Canisius staff that include the names, images, voices and likenesses of individuals who are not Canisius students, faculty or staff may only be used for publicity, commercial, promotional or marketing purposes after a signed consent form from those individuals is obtained.

**Use of photos and video recordings Supplied by students and/or faculty:** Any photographs or video recordings supplied to the Office of College Communications, Office of Marketing and Brand Engagement by students, faculty, staff, alumni, friends of the college or contractors become the property of Canisius College and may be used freely for publicity, commercial, promotional or marketing purposes, provided the subject’s consent (if required) has been obtained.

**DEFINITIONS**

*Filming and Digital Recording*—the capturing of moving or still images of college property by any means on any media now known or that may be invented in the future including, but not limited to, film, videotape, digital memory, or any electronic transmission to another medium or to the Internet.

*Photography*—the capturing of still images onto any compatible medium, or posting to the Internet, by any means or devices now known or that may be invented in the future including, but not limited to, film cameras, digital cameras, electronic devices such as personal computers, mobile phones, iPads, etc.

**PROCEDURES/GUIDELINES**

**Conditions of Approval**

Regardless of the type of photography, recording, or filming requested by an outside business or hobbyist, if the request is granted approval, the approved entity may only photograph, record, or film in those areas and during the time frames authorized by the Office of College Communications, Office of Marketing and Brand Engagement. In addition, individuals must obtain the permission of the subjects of their photography, recording, or filming.

Prior to the date of the shoot, the Office of College Communications, Office of Marketing and Brand Engagement will be responsible for: (a) assuring an individual employed by the college is in attendance when the individual, group, or organization makes use of the college facility or grounds; and (b) notifying Public Safety and other college departments of the upcoming shoot.

**RELATED POLICIES**
Not Applicable

Social Media Policy.

Revision Feedback for 2.6.5.: Photography, Digital Recording, and Filming Policy
Submit Feedback
SOCIAL MEDIA POLICY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>May 6, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number:</td>
<td>II – 2.6.6</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>Not Applicable.</td>
</tr>
<tr>
<td>Issuing Authority:</td>
<td>President</td>
</tr>
<tr>
<td>Responsible Officer:</td>
<td>AVP for Marketing and Communication</td>
</tr>
<tr>
<td>Applicability:</td>
<td>All members of the Canisius College community.</td>
</tr>
<tr>
<td>History:</td>
<td></td>
</tr>
</tbody>
</table>

PURPOSE

The purpose of this Policy is to establish clear guidance for creating and approving content pertaining to Canisius College (including the college’s departments, divisions, offices, centers, programs, etc.) on any publicly available social media site. The purpose of this policy is to establish the college’s policy, guidelines, and procedures for creating and approving content pertaining to Canisius College (including the college’s schools, departments, divisions, offices, centers, programs, series, etc.) on any publicly available website or social media platforms. In addition, guidelines are provided to the general campus community regarding personal use of social media.

POLICY

Canisius College’s official presence on social media platforms is overseen by the Office of College Communications. Websites and/or accounts that purport to represent information as Canisius college (including the schools, departments, divisions, offices, centers, programs, series, etc.) on any publicly available Website or social media platforms must be approved by and coordinated with the Office of College Communications.

Websites/providers or social media platforms that host unauthorized accounts using identification as Canisius College or its subdivisions—in name or image, including the college seal or its logos—will be contacted for immediate removal of accounts.

All official college social media sites and official college communications, including but not limited to the account itself, content, followers, subscribers, and contacts are the property of Canisius College. Members of the college community have no ownership rights whatsoever to an official college social media site.

The college does not govern or regulate content on personal social media sites by members of the college community. However, to the extent the use of personal social media sites may reasonably be construed as implying the support, endorsement, or opposition of the college, members of the college community must distinguish their personal views from those that they are authorized to express on behalf of the college. Members of the college community are also reminded that violations of law or college policy conducted through social media sites, or evidence of violations posted on social media sites of which the college is made aware, may be subject to disciplinary...
and/or legal action, regardless of whether a personal account or official college social media site is used.

**DEFINITIONS**

*College Data*—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

*College Work Product*—includes any and all log-in information, data, passwords, trademarks, and content related to an official college social media site, including all followers, subscribers, and contacts. College work product, however, does not include social media sites or accounts that are created or used by a member of the college community exclusively for personal use.

*Copyrightable Works*—an original work of authorship that has been fixed in any tangible medium of expression from which it can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. Copyright includes a bundle of rights: the right to make reproductions of the work, the right to distribute copies of it, the right to make derivative works that borrow substantially from a copyrighted work, and the right to make public performances or displays of most works.

*Covered Data and Information*—means all information required to be protected under the GLBA, including Student Financial Information. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any credit card information received in the course of business by the college, whether or not such credit card information is covered by GLB. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

*Intellectual Property*—means certain creations of the human mind that are granted legal aspects of a property right. These property rights include patents, copyrights, trademarks, trade secrets, and any other such rights that may be created by law in the future.

*Members of the college Community*—includes any person who is a student, faculty member, staff member, organization, club, group, team, alumni, volunteer, trustee, or any other person employed by the college.

*Official College Communications*—communications done in the name of the college on a social media site.

*Official College Social Media Site*—a social media site or account that is created or used by a member of the college community in the name of the college or a college department, program, team, or officially recognized college club, group, or organization (collectively “college”) or to promote and/or market the college, including accounts featuring or displaying the college’s name and trademarks (collectively “College Work Product”).

*Private College Data*—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the Data Classification Policy.
**Private-Highly Restricted:** College Data that are not public and are available within the college only to those with a legitimate need to know and are so highly sensitive that the loss of confidentiality of the data could either (a) cause significant personal, college, or other harm or (b) a law, regulation or contract require a high degree of security. **Examples of Private-Highly Restricted College Data include, but is not limited to:**

- **Personally Identifiable Information or PII:** any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

- **Covered Data and Information within the meaning of Title V of the Gramm Leach Bliley Act of 1999 (Public Law 106-102, 11 Statute 1338) (as amended) and its implementing regulations.**

- **Human subjects research data or other sensitive research data.**

- **Protected Health Information or PHI:** Individually Identifiable Health Information that is transmitted or maintained by the college in electronic or any other form or medium as defined by Health Insurance Portability and Accountability Act (HIPAA).

- **Payment card information regulated by the Payment Card Industry Data Security Standard (PCI DSS).**

- **Legal investigations conducted by the college.**

**Private-Restricted:** College Data that by law are not public and are available within the college only to those with a legitimate need to know but are not so highly sensitive that the loss of confidentiality of the data would cause significant personal, institutional, or other harm, and no law, regulation, or contract require a higher degree of security. **Examples of Private-Restricted College Data include, but is not limited to:**

- **Student Directory Information** (if student has requested non-disclosure (suppressed): name, address, email address, telephone/mobile device number, dates of enrollment/registration, enrollment/registration status, major, adviser, college/school, class, academic awards and honors received, and degree received.

- **Student Non-Directory Data:** grades, courses taken, class schedule, test scores, advising records, educational services received, disciplinary actions, student ID number, immunization records, career services records.

- **Linking a library patron’s personal identity with materials requested or borrowed by the person or with a specific subject about which the person has requested information or materials.**

- **Donor and gift data.**

- **Location of assets (e.g., specific information on where the college physically or electronically stores data, or technology that must be protected).**
- Passwords, PIN numbers, or other types of authentication (e.g., multi-factor/two-factor, biometrics).
- Trade secrets or intellectual property.
- Sealed bids.
- Unpublished research data that have not been made public, such as de-identified data or proprietary research materials.

*Social Media*—includes the various online technology tools that enable people to communicate easily via the Internet to share information and resources. Social media can include blogs and social networking sites like Facebook, Twitter, Instagram, YouTube, Snapchat, and LinkedIn. In addition, any web application, site, or account maintained by Canisius College that facilitates an environment for employees, students, and alumni to share information and opinions in an interactive way is included in this definition.

*Trade Secrets*—includes all information including, any formula, drawing, pattern, compilation lists, program, device, method, technique or process that derives independent economic value, actual or potential, from not being generally known to and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use.

**PROCEDURES/GUIDELINES**

**College Use of Social Media**

*Notification*

Individuals are requested to report violations of this Policy to the Office of College Communications.

*Enforcement*

The Office of College Communications is responsible for the appropriate enforcement of this policy.

*Sanctions*

Office of College Communications staff may remove any textual or multimedia content, webpages, or external links from college websites or other social media formats that violate college policies and standards, or local, state, federal, or international laws. In addition, ITS staff may refer violators to the appropriate administrators for disciplinary action.

**I. Official College Social Media Sites**

All official college social media sites must be authorized in accordance with the Approval Procedures set forth below in Paragraph I.A. Any official college social media site which does not receive prior authorization will be subject to review when discovered and may be amended or removed at the discretion of an account administrator designated pursuant to Paragraph I.A or the Office of College Communications or the Athletics Communications Office, as applicable.

**A. Approval Procedures**

A request for an official college social media site must first have the written approval of the applicable department head, then final written approval by the Office of College Communications.
If the presence or participation on social media sites involves a college athletic program, the request must be approved by the Athletics Communications Office.

Once the social media site has been approved, the approving department head must assign at least two staff or faculty members and one member of the Office of College Communications or Athletics Communications Office as account administrators. These individuals must be faculty or staff. Account administrators may delegate social media responsibilities to enrolled students, but a student may not have full administrative access to any official college social media site.

B. Responsibilities

1. Account Administrator Responsibilities

Account administrators for an approved official college social media site are responsible for:

1. Regularly monitoring content and postings for correctness and accuracy;

2. Monitoring communications and comments for acceptability in the college workplace and campus community. All posts, comments and actions on the site have the ability to affect the reputation of the college as well as other individuals affiliated with Canisius;

3. Protecting Private College Data and intellectual property rights of others and the college. This includes, but is not limited to, intellectual property, operating plans, student financial data, protected health information (PHI), FERPA protected student records, donor information, employee information, home addresses, phone numbers, and social security numbers. Such data may not be posted on an approved official college social media site;

4. Monitoring and removing content that is illegal, obscene, defamatory, harassing, discriminatory, threatening, or an invasion of privacy;

5. When required by college policy or law, obtaining the expressed consent of involved parties prior to distribution or publication of recordings, digital images, videos, text, slideshow presentations, artwork and advertisements whether those rights are purchased or obtained without compensation;

6. Monitoring content for compliance with the college’s Brand Guide and removing content that does not comply;

7. Monitoring content for compliance with all federal and state laws, regulations, and college policies, removing content that does not comply, and reporting violations to the applicable campus authorities and/or law enforcement;

8. Monitoring content for compliance with the social media site’s terms and conditions for use and removing content that does not comply;

9. Minimizing security risks by:
   a. Utilizing strong passwords in accordance with the college’s Password Policy;
   b. Activating multi-factor authentication for all accounts where it is available;
   c. Registering the account using only official college email address;
   d. Regularly monitoring the site; and
   e. Changing passwords and updating/adjusting account administrator roles.
immediately when an account administrator or editor, especially students, has left the college and no longer is authorized to access to the official college social media site; and

10. Deactivating a dormant account.

2. Office of College Communications and Athletics Communications Office Responsibilities

The Office of College Communications or Athletics Communications Office as applicable oversees the college’s institutional presence on official college social media sites and determines whether to approve official college social media sites as they become available. In addition, these offices routinely review in collaboration with account administrators’ official college social media sites for compliance with this policy, instruct account administrators to correct, modify, suspend, or terminate official college social media sites that are not in compliance with this policy, and suspend or terminate official college social media sites, where appropriate.

It is the policy of the college to address a policy violation by working with account administrator in a fair and equitable manner to prevent a recurrence prior to terminating an account. The college, however, reserves the right to immediately terminate an account even if the policy violation constitutes a first offense. In such cases, written notice of the account termination action will be provided to the account administrator by the applicable office.

3. Members of the College Community Responsibilities

Members of the college community are responsible for refraining from creating, using, or posting to official college social media sites in violation of this policy. Moreover, they are expected to surrender access to official college social media sites, as appropriate, when college status changes.

C. User Agreements for Official College Social Media Sites

Whenever an Official College Social Media Site is approved and created, the Social Media outlet requires the account creator to agree to certain terms and conditions for use of the site by clicking “Yes” or “I accept” as part of the account creation process. These are legal contracts, and they often contain terms and conditions that create risks for the account creator and the College (for an official college social media sites). Account administrators are delegated authority to create an official college social media site through completion of the application process and approval by the Office of College Communications or Athletics Communications Office, as applicable.

College account administrators are not authorized to enter into advertising agreements with social media sites without prior authorization and approval obtained by contacting the Office of College Communications or Athletics Communications Office, as applicable. Any member of the College community desiring to purchase advertising services from a social media site must follow all applicable policies governing both the public relations considerations and the procurement and contracting considerations related to such services.

D. Ownership of Social Media Work Product

All official college social media sites, accounts, developments, and intellectual property created or used by a member of the college community for the college as a result of the performance of assigned college duties or with the significant use of college facilities, resources and/or personnel
or to promote and/or market the college, including accounts featuring or displaying the college’s name and trademarks (collectively “College Work Product”), belong solely to the college. The college owns and has the right to control all College Work Product whether the member of the college community opens the account or uses, manages, or access it. The college does not require or request members of the college community to provide personal social media account information or passwords in accordance with applicable laws.

Upon the college’s request by the college or immediately after separation from the college, members of the college community are not authorized to access, use, update, or modify the College Work Product unless written authorization is granted by the Office of College Communications or Athletics Communications Office, as applicable.

Upon separation from the college, the college will retain ownership and control of all College Work Product created or used during the individual’s affiliation with the college, including all related data and information.

Any member of the college community with account access to an official college social media site agrees to provide to the area vice president the login information, including the usernames and passwords, for College Work Product created, modified, or used upon creation of the account. When passwords are updated, the area vice president must be provided the new password.

Note: Whether a College Work Product has been developed by a member of the college community as a result of the performance of assigned college duties or with the significant use of college facilities, resources, and/or personnel shall be determined in accordance with the college’s Intellectual Property Rights and Ownership Policy.

E. User Generated Content on Official College Social Media Sites

The college is not responsible for comments or posts made by followers of or visitors to official college social media sites. Comments posted by these individuals may not reflect the official views or policies of the college. Accordingly, official college social media sites that permit followers or visitors to share comments and other user-generated content must contain a disclaimer stating that any such user-generated content does not reflect the opinions or views of the college, its trustees, officers, or employees. Such disclaimer must be published in the account’s “about” section.

The college reserves the right to block, remove, or delete from an official college social media site any and all posts, comments, links, images, video, music, or other content for any reason. Examples of posts, comments, links, images, video, music, or other content that may be blocked, removed, or deleted, include, but are not limited to, those that:

1. Incite unlawful discrimination, violence, or harassment or are defamatory, obscene, or threatening;
2. Are irrelevant to the topic of the posting;
3. Incorrectly creates an appearance of an endorsement by the college;
4. Targets or disparages an individual’s race, color, national or ethnic origin, sex, disability, age, religion, genetic information, veteran or military status, or any other basis prohibited from discrimination under local, state, or federal law;
5. Advocates illegal activity;
6. Infringes copyrights, trademarks, or other intellectual property rights;
7. Contains spam, junk mail, or unauthorized solicitations; or
8. Violates any applicable local, state, federal law or regulation or college policy or procedure.

F. Multi-Media Usage on Official College Social Media Sites

All multimedia usage on an official college social media site must adhere to copyright, trademark, intellectual property, and privacy laws and regulations, as well as applicable college policies addressing these matters.

1. Digital Images: Usage of digital images (i.e., photographs, video or digital records) taken on campus or at college-sponsored events on an official college social media site must comply with the college’s Photography, Digital Recording, and Filming Policy.

2. Music:
   a. Usage of music protected by copyright is strictly prohibited unless written permission from copyright owner is received.
   b. Written permission for usage of copyright music must specifically include online distribution allowances. Additionally, broadcast and royalty requirements must be satisfied.
   c. Consumer ownership of music does not constitute a right to distribute, or usage on behalf of the college.
   d. Royalty-free music is recommended for usage online.

3. Video:
   a. Events streamed on the Canisius College official YouTube, Facebook, or any other social media account require the explicit authorization of the college president;
   b. Video taken at private events used to advertise products or services of the college may not require releases when the focus of the photograph is a location or event, not a person (i.e., the social media post is used for news or documentary uses).
      i. News is a factual account about an individual, initiative, event, body or work, etc. that would be “new” to the reader (“news”) for the purpose of relaying information for advancement of knowledge.
      ii. Documentary use is the factual “documenting” of a person, initiative, program or event, purely for the purpose of relaying information or advancing knowledge.
   c. When an individual's face in a video taken at a private event is identifiable and “featured” for purposes of college programs or administrative programs; promotes events in advance; fundraising; recruiting; or encouraging attendance or participation, the best practice is to obtain a signed release.
      i. Promotional or marketing uses are generally considered those that use Social Media to seek to motivate action — attendance, donation, participation, enrollment, etc.
ii. Private events or invitation only-events when a registration or RSVP is required should include the following opt-out language on the registration or RSVP form if video will be taken for purposes of marketing or promotion: “The college will be taking photos/video at this event for use in advertising and other promotional materials, whether in print, electronic, or social media. Please check this box if you do not authorize that you [or your child] be photographed at this event [or camp].”

d. Public events do not require a signed release by subjects. Furthermore, events that occur outdoors or in public space on or off campus are typically considered to be public events.

i. Examples: a group of students at a college football game; a group of alumni at a homecoming event; students walking on campus, etc.

e. Written permission should be obtained from speakers, guest lecturers, performers, and other campus visitors who are present at college-sponsored events, unless otherwise guaranteed in performance contracts.

f. For use of images and music in videos, please review image and music guidelines above, as well the college’s streaming web video guidelines.

g. Written permission for usage of copyright video must specifically include online distribution allowances. Additionally, broadcast and royalty requirements must be satisfied.

h. Consumer ownership of video does not constitute a right to distribute, or usage on behalf of the college.

i. College video footage may be published with permission from the Office of College Communications.

Refer to the college’s streaming web video guidelines on the college wiki for additional information.

G. Additional Guidelines for Use of Official College Social Media Sites and Postings of Official College Communications

Members of the college community who post to an official college social media site or post an official college communication must be mindful that they are personally responsible for what they post and are expected to observe the following guidelines:

1. Post accurate, concise, and useful information;
2. Uphold the college’s mission and Jesuit values;
3. Be clear about their role and/or position with the college;
4. Read, obey, and comply with the Terms of Service for all social media tools before posting anything;
5. Be respectful of fans, followers, and those posting on the site. Use discretion regarding use of public forums versus direct messages;
6. Protect confidential and proprietary information:
a. Posting or sharing confidential or proprietary information about the college, its students, employees, alumni or affiliates is strictly prohibited;

b. All members of the college community must follow applicable federal requirements, including but not limited to Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Family Educational Rights and Privacy Act of 1974 (FERPA);

7. Do not consider any information posted to social media sites and blogs as private, even if the strongest privacy settings are used;

8. Adhere to all applicable college policies and procedures;

9. Adhere to trademark, logo, and licensing guidelines as published in college’s Brand Guide;

10. The College Communications or Athletics Communications Office, as applicable will provide members of the media and the public with college and departmental news:

   a. Members of the college community should not speak or post information to the media without contacting the College Communications or Athletics Communications Office, as applicable;

   b. All media inquiries should be directed to College Communications or Athletics Communications Office, as applicable;

11. Respect copyright and intellectual property rights of other entities, artists, and organizations in accordance with federal laws and regulations;

12. Know the facts before posting;

13. Cite sources whenever possible. Give credit where credit is due;

14. If an error is made, correct it quickly;

15. Respect the ideas of others;

16. Do not represent personal opinions as being endorsed by the college or any of its organizations.

H. Right to Terminate Official College Social Media Sites

In the event that this policy is violated, or an official college social media site appears to be stagnant (no posts or activity for more than six months), an account administrator or the Office of College Communications or Athletics Communications Office, as applicable reserves the right to terminate the account.

II. Personal Use of Social Media

A. College Employees

The college respects the rights of its employees to use social media as a medium of self-expression. However, the college requires that the following guidelines be observed:

Employees are personally responsible for what they post on social media sites. For non-business participation on social media sites, employees must use a personal e-mail address. Use of personal e-mail accounts serves to prevent confusion and works to eliminate any misperception of speaking on behalf of the college.
The personal use of social media sites during business hours to access social media must be limited to incidental use. Incidental use should not interfere with the employee’s performance of assigned job responsibilities or someone else’s job performance or compromise the functionality of the campus network.

In using social media as part of the employee’s personal life, employees should refrain from presenting personal opinions in ways that imply endorsement by the college. If posted material may reasonably be construed as implying the support, endorsement, or opposition of the college with regard to any personal statements, including opinions or views on any issue, the employee should make clear that he or she is speaking for oneself and not as a representative of the college.

In addition, an employee’s personal use of social media or electronic postings should be consistent with college policies. Examples of postings that are contrary to college policy include, but are not limited to the following:

1. Unlawfully discriminatory or harassing behavior, including but not limited to sexual or gender-based misconduct, against a member of the college community;
2. Posting of materials or information in violation of the college’s confidentiality or student record policies or provisions protecting trade secrets contained in any college confidentiality agreement, contract, and/or grant;
3. Postings that unlawfully or maliciously defame or disparage the college, its employees, students, or work product or make grossly reckless or maliciously false statements about the college;
4. Non-approved use of the college’s name or the posting of the college’s seal, logo, trade and service marks, monograms, or images;
5. Any violation of the Standards of Ethical Conduct;
6. Only individuals authorized by the Athletic Department may recruit potential student-athletes via social media. All governing athletic regulations must be followed when using official and/or personal social media accounts in the recruitment of student athletes.

In response to concerns or complaints or information provided by individuals, college administrators may look up profiles on social networking sites and may use the information in informal or formal disciplinary proceedings.

**B. Students**

Canisius College students must be concerned with any behavior that might reflect badly on themselves, their families, and the college. Such behavior includes any activities conducted online.

Students users must understand that any content they make public via online social networks or digital platforms (i.e., cell phones, mobile devices, laptops, tablets, etc.) is expected to follow acceptable social behaviors and also to comply with federal and state government laws and college policies, procedures, rules, and regulations, including the Community Standards. Because social networking sites are part of the public domain, students should make use of any available privacy settings, and as a general rule should avoid posting sensitive personal information such as a home address, phone number or birth date. Students should also be aware that inappropriate conduct online could negatively impact their personal, academic and professional lives if viewed by college personnel, employers or potential employers, internship supervisors, scholarship committees or
admissions committees. If inappropriate conduct is deemed a violation of any law or regulation, disciplinary and/or law enforcement action may be taken. Examples of misconduct include, but are not limited to, derogatory language about any member of the college community; demeaning statements about or threats to any third party; and incriminating photos or statements depicting hazing, unlawfully discriminatory or harassing behavior, sexual or gender-based misconduct, vandalism, stalking, underage drinking, and illegal drug use.

C. **Student Athletes**

Participation in intercollegiate athletics at Canisius College is a privilege, not a right. While the Athletic Department does not prohibit student-athlete use of online social network sites and/or digital platforms, it must be understood that the high standard of integrity expected of student-athletes on the field also extends to areas off the field, such as comments and postings made to Internet sites. The Athletic Department reserves the right to take action against currently enrolled student-athletes engaged in online behavior that violates National Collegiate Athletic Association (NCAA), Athletic Conference, or College, Athletic Department, or team policies, rules, and regulations. This action may include education, counseling, team suspension, termination from the team, reduction or non-renewal of any athletic scholarships, disciplinary sanctions or involvement of law enforcement agencies.

**RELATED POLICIES**

- Acceptable Use of College Computer and Network Systems Policy
- Brand Guide
- College Web Presence Policy
- Intellectual Property Rights and Ownership Policy
- Password Policy
- Photography, Digital Recording, and Filming Policy
- Standards of Ethical Conduct
PURPOSE
The purpose of this policy is to define the college’s policy, procedures, and guidelines for administering family and medical leave in compliance with the Family and Medical Leave Act (“FMLA”).

POLICY
It is the policy of Canisius College to provide eligible employees with unpaid family/medical leave (FMLA) for up to 12 weeks within any 12-month period for specified family and medical reasons; or up to 26 workweeks of unpaid leave in a 12-month period to care for a covered service member with a serious injury or illness.

To be eligible, employees must have worked for the college for at least 12 months, and for at least 1,250 hours during the last 12 months. The college maintains current health benefits during an approved family/medical leave, with the employees continuing to pay their portion of the premium. Accrued vacation may be used for any portion of the 12 weeks. Additional vacation and sick leave will not accrue during any unpaid portion of FMLA. Absences due to Workers’ Compensation, NYS Disability, paid medical leave or unpaid personal leave for family care will count toward one’s annual 12-week FMLA allotment.

The administration of leave under this policy shall be done in accordance with the procedure and guidelines set forth below, as well as FMLA and related regulations. Detailed information and application forms are available in Human Resources.

DEFINITIONS
Eligible Employee - one who has worked for Canisius College for at least twelve (12) months and has worked at least 1,250 hours during the twelve (12) months immediately preceding the requested leave.

Serious Health Condition - an illness, injury, impairment, physical or mental condition that results in (a) any period of incapacity or treatment related to inpatient care in a hospital, hospice, or
residential care facility, (b) any period of incapacity requiring absence from work, school, or other
regular activity for more than three (3) calendar days that also involves continuing care [treatment
two or more times by a health care provider or pursuant to a regimen of supervised care], or (c)
that requires continuing care by a health care provider for a chronic, serious health condition or
which results in a period of incapacity, or (d) prenatal care.

Medical Necessity - certification by a health care provider that a medical need can best be
accommodated by an intermittent or reduced leave and outlining the expected duration and
schedule of the intermittent or reduced leave.

Key Employee - an FMLA-eligible employee who is among the highest paid ten (10) percent of
the employees employed within seventy-five (75) miles of the employee’s worksite.

Qualifying Exigency - qualifying exigencies are situations arising from the military deployment of
an employee’s spouse, son, daughter, or parent to a foreign country. Qualifying exigencies include
the following: Short-notice deployment; Military events and related activities; Childcare and
school activities of the service member’s child; Financial and legal arrangements for the service
member; Counseling; Rest and recuperation of the service member; Attending to certain post-
deployment activities, including attending arrival ceremonies, reintegration briefings and events,
and other official ceremonies or programs sponsored by the military for a period of 90 days
following the termination of the covered military member’s active duty status, and addressing
issues arising from the death of a covered military member; or Additional activities that the
employer and employee shall agree qualify as an exigency and agree to both the timing and
duration of such leave.

Covered Service Member - a member of the armed forces, including a member of the national
guard or reserves, who is undergoing medical treatment, recuperation, or therapy, is otherwise in
outpatient status, or is otherwise on the temporary disability retired list, for a serious injury or
illness. A "covered service member” also includes a veteran who is undergoing medical treatment,
recuperation, or therapy for a serious injury or illness if the veteran was a member of the Armed
Forces at any time during the period of 5 years preceding the date on which the veteran undergoes
that medical treatment, recuperation, or therapy.

Where a term is defined in the FMLA and/or accompanying regulations, that definition will be
incorporated into policy.

PROCEDURES/GUIDELINES

Family and medical leave will be provided to eligible employees in conformity with the Family
and Medical Leave Act (FMLA). Eligible employees are entitled to:

1. A maximum of twelve (12) weeks of leave during a twelve-month period for any of the
   following reasons:
   a. The birth of a child and to care for the newborn child within one year of birth;
   b. The placement with the employee of a child for adoption or foster care and to care
      for the newly placed child within one year of placement;
   c. Care of a child, spouse, or parent with a serious health condition;
   d. A serious health condition that results in the employee’s inability to perform the
      essential functions of the employee’s job;
e. Any qualifying exigency arising out of the fact that the employee’s spouse, son, daughter, or parent is a covered military member on “covered active duty;” or

2. A maximum of twenty-six workweeks of leave during a single twelve-month period to care for a covered service member with a serious injury or illness if the eligible employee is the service member’s spouse, son, daughter, parent, or next of kin (military caregiver leave).

Leave Entitlement

An eligible employee may take up to twelve (12) weeks unpaid leave for the reasons set forth in paragraph 1 (a-e) above in a twelve (12) month period. The twelve (12) month period is a rolling twelve (12) month period measured backward starting on the date an employee first uses any FMLA leave (i.e., no more than twelve (12) weeks FMLA may be taken in any twelve (12) month period). Any FMLA leave taken by an employee during the preceding twelve (12) month period will be used to determine the amount of available leave pursuant to the FMLA. Once the employee’s leave exceeds the requirements of the FMLA, the college may have to fill the employee’s position, as business circumstances may not allow the college to keep the position open.

Leave shall normally be continuous, except that leave for the care of a child, spouse or parent with a serious health condition or due to the employee’s own serious health condition may be taken intermittently or on a reduced basis when medically necessary. See the Reduced or Intermittent Leave paragraph 7 clause of the Administrative Requirements section below for additional information.

Leave for a newborn child or adoption or foster care placement of a child must be completed within twelve (12) months of the birth, adoption, or placement, and the leave must be taken all at one time. Spouses employed by Canisius College are jointly entitled to a combined total of twelve (12) weeks of family leave for the birth or placement of a child, or to care for a parent who has a serious health condition. However, for other qualifying reasons under FMLA (other than military caregiver leave), each eligible spouse is entitled to twelve (12) workweeks. If the employee and his or her spouse are employed by the college, they are limited to a combined total of twenty-six (26) workweeks of FMLA leave during a single twelve (12) month period for the care of a service member or veteran with a serious injury or illness (military caregiver leave).

Substance Abuse

FMLA leave is available for treatment for substance abuse or for the care of an immediate family member who is undergoing treatment for substance abuse. The patient must be undergoing treatment by a health care provider, and must not be using the substance in issue.

Military Caregiver Leave

Eligible employees are entitled to up to twenty-six (26) work weeks of unpaid FMLA leave in a single twelve (12) month period to care for a current member of the armed forces, the national guard or reserves who has a serious injury or illness incurred or aggravated in the line of duty on active duty for which he/she is undergoing medical treatment, recuperation, or therapy; is otherwise in outpatient status; or is otherwise on the temporary disability retired list, or to care for a veteran who is undergoing medical treatment, recuperation, or therapy for a serious injury or illness (as that term is defined by the Secretary of Labor) incurred or aggravated in the line of duty on active duty, provided the veteran was a member of the U.S. armed forces (including the national
guard or reserves) during the five-year period preceding that medical treatment, recuperation, or therapy.

**Administrative Requirements**

**Use of Paid Leave:** Employees will be required to utilize their paid leave prior to receipt of unpaid FMLA leave.

While on FMLA leave related to an employee's own medical condition, the employee must use concurrently and will be paid accumulated sick leave benefits and then any accumulated vacation and personal leave day pay (if applicable) for the duration of the leave (or until the benefits are exhausted, whichever comes first), if applicable. Any remaining time on FMLA leave will be unpaid.

For leaves not related to an employee's medical condition, an employee must use concurrently and will be paid accumulated personal leave, and New York paid family leave, and vacation pay for the duration of the leave (or until the benefits are exhausted, whichever comes first), and any remaining time on leave will be unpaid. Employees must comply with the college’s normal paid leave policies.

Example: paid vacation and/or paid personal leave for leave taken pursuant to (1) and (2) above, and paid sick, vacation and personal leave for leave taken pursuant to (2) and (3) above. The period of this paid leave will be counted against the employee’s total FMLA leave entitlement, as will any workers’ compensation leave.

**Application for Leave:** Employees must give thirty (30) days advance notice of the need to take FMLA leave to Human Resources. When it is not possible to give thirty (30) days advance notice, notice must be given as soon as practicable, ordinarily within one or two days of when the need for the leave becomes known to the employee.

- Failure to give adequate notice as outlined above may result in a delay of up to thirty (30) days before FMLA leave will be granted.
- When requesting intermittent leave for medical treatments, employees must make reasonable efforts to schedule the leave so as not to unduly disrupt college operations.
- After receiving a request for FMLA leave, the associate vice president for human resources and compliance or a designee will inform the employee whether he or she is eligible under the FMLA. If eligible, the associate vice president for human resources and compliance or designee will inform the employee about any additional information the employee must provide to qualify for FMLA leave as well as detail the employee’s rights and responsibilities concerning FMLA leave. If the employee is not eligible for FMLA leave, the associate vice president for human resources and compliance will inform the employee why he or she is not eligible.

**Medical Certification:** Employees must provide medical certification from an appropriate health care provider to support a FMLA request related to a serious health condition on a form which will be provided to the employee. This certification must be returned within fifteen (15) days under normal circumstances.

- If an employee provides medical certification that is questionable or inadequate, (s)he will be referred to a second provider at Canisius College’s expense.
If the first and second opinions differ, a third opinion will be obtained, again at Canisius College’s expense. The third health care provider will be selected by mutual agreement of the employee and Canisius College, and that opinion will be final and binding.

Note: The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits employers and other entities covered by GINA Title II from requesting or requiring genetic information of employees or their family members. In order to comply with this law, the college requests that employees do not provide any genetic information when replying to this request for medical information. ‘Genetic information,’ as defined by GINA, includes an individual’s family medical history, the results of an individual’s or family members genetic tests, the fact that an individual or an individual’s family member sought or received genetic services, and genetic information of a fetus carried by an individual of an individual’s family member or an embryo lawfully held by an individual or family member receiving reproductive services.

Medical Re-Certification: Employees on FMLA leave for pregnancy, chronic or long-term conditions under the continuing supervision of a health care provider will be required to submit monthly re-certifications or updated reports regarding the family member or employee’s current medical status. Employees must give advance notice of their intent to return to work, either as part of a monthly re-certification, or, when less leave is required than was anticipated, at least two days. Failure to meet the certification requirements may result in counting the employee’s days off against his or her attendance record; disciplinary action, up to and including termination; or denial of reinstatement following the leave.

Prohibition on Working During FMLA Leave: Except where express authorization is given, employees on FMLA leave are prohibited from performing any work, paid or unpaid, for any other person or entity, including the employee’s own business. Violations of this prohibition may result in FMLA leave being revoked and the employee’s prior days off being counted against his or her attendance record; disciplinary action, up to and including termination; or denial of reinstatement following the leave.

Returning from FMLA Leave: An employee taking a FMLA leave due to a serious health condition must present certification that (s)he is fit for duty prior to reinstatement. Failure to provide the requisite certification will result in denial of restoration to employment. In most cases, an employee returning from FMLA leave will be restored to the position previously held prior to FMLA leave, provided that position remains available. If that position is unavailable, the employee will be reinstated to an equivalent position with equivalent pay, benefits and other terms and conditions of employment. An employee taking FMLA leave is not entitled to any greater right to reinstatement or other benefits than if continuously employed during the leave period. Key employees may be denied job restoration if such denial is necessary to prevent substantial and grievous economic harm to the operation of the college.

Reduced or Intermittent Leave: If FMLA leave is taken on a reduced or intermittent basis, the employee may be transferred temporarily to an available alternative position for which the employee is qualified and which better accommodates the recurring periods of leave.

Request for an Extension of a FMLA Leave: In order for a FMLA leave of absence to be extended for longer than what was originally approved, the request must be accompanied by an appropriate health care provider certification indicating the condition or disability and circumstances for the extension before the request will be considered.
Failure to Return from a FMLA Leave: Any employee who fails to return to work as scheduled after FMLA leave may be subject to dismissal from employment. Employees who exceed their FMLA entitlement without extension(s) of their leave approved under other appropriate leave provisions, may be subject to dismissal from employment.

Benefits During Family or Medical Leave of Absence

- Health insurance coverage will continue throughout the duration of a FMLA leave. The conditions under which such coverage is provided will be the same as if the employee were actively working. Moreover, employees will not lose any employment benefits earned and accumulated before their FMLA leave begins. Employees on FMLA leave, however, are not eligible for jury duty, funeral leave, or sabbatical leave during such leave.

- The employee share of any health plan premiums must continue to be paid by the employee while on FMLA leave, and payments are due at the same time as if made by payroll deduction. Similarly, employees contributing to their family’s health care coverage are required to make the appropriate contributions during the approved family or medical leave of absence. Monthly payment by cash or check must be received by Human Resources by the fifteenth of each month. Failure to make any required payment will cause such health care coverage to lapse.

- If an employee’s share of any health insurance premium is delinquent for more than thirty (30) days, the employee’s health coverage may be terminated. If coverage is not terminated and Canisius College elects to pay the entire premium, the amount of the employee’s delinquency will be recovered from the employee after (s)he returns to work.

- If an employee fails to return to work after FMLA leave has expired, Canisius College may recover the cost of any premiums it paid during the employee’s unpaid FMLA leave unless the employee’s failure to return to work is the result of: (a) The continuation, recurrence or onset of a serious health condition that would entitle the employee to FMLA leave; or (b) Other circumstances beyond the control of the employee.

- A key employee is a salaried employee whose salary is among the highest paid 10 percent (10%) of all employees of the college. Key employees may not be entitled to return to their position should the college determine that substantial and grievous economic injury will result from his or her absence. If a key employee is notified of Canisius College’s intent to deny restoration of employment, the key employee will continue to be entitled to maintenance of health benefits until such time as the key employee gives notice that (s)he no longer wishes to return to work, FMLA leave entitlement is exhausted, or restoration is actually denied at the end of the leave period. Premium costs paid on behalf of key employees in such circumstances are not recoverable.

Factual Misrepresentations

Factual misrepresentations made by employees in order to obtain FMLA leave shall result in disciplinary action, up to and including termination. Additionally, disciplinary action may also be taken against employees who are engaged in employment activities unrelated to the college while on an approved FMLA leave.

RELATED POLICIES
Family Care Days Policy

Part-time Paid Days Policy

Sick Leave (Staff) Policy

Revision Feedback for 3.4.2: FMLA Policy

Submit Feedback
PURPOSE
The purpose of this policy is to define the college’s moving expenses benefit program.

POLICY
It is the policy of Canisius College to pay for the following costs for new full-time exempt hires requiring moving assistance and meeting the distance limitation requirement (see Section III below), up to a maximum of $2,000, for the following expenses:

- Transporting household goods;
- Cartons necessary for packing;
- Insurance (not to exceed $1.25 per pound*), and
- Packing and unpacking of mattresses and box springs.

The college will not contribute to the payment of any other packing and unpacking costs, extra stops, storage, appliance service, etc.

Invoices for using the college’s moving agent will be sent directly to the college for payment. Any unauthorized overage will be billed to the new hire by the Business Office.

*Individuals may obtain as much insurance coverage as they wish; the college will simply bill the employee for the difference.

DEFINITIONS

*Moving/Relocation Expenses*: Expenses associated with packing, loading, hauling, insuring or temporarily storing property (no more than 30 days), unpacking, transportation and lodging during the move.

PROCEDURES/GUIDELINES
The name (including spouse’s), address, and telephone number (home and business) of all full-time exempt new hires (faculty, librarian & administrative) who will require moving assistance should be sent to Human Resources, which will then notify the college’s moving agent to arrange an estimate and scheduling of the move.
New hires that choose to move themselves (that is, via U-Haul or other self-drive moving service) will have the same dollar limitation and restrictions. Those who move themselves will submit an itemization of expenses (attaching the corroborating receipts) to the Human Resources for reimbursement.

I. **Eligible Moving Expenses**

Expenses for travel from the former residence to the new residence are typically eligible for reimbursement from the college (subject to associated dollar limitations) as moving expenses. Such reimbursements are treated as compensation and subject to tax withholding (see Section IV below). Travel expenses are limited to one trip, one way, per dependent family member. The actual costs of transportation and lodging incurred en-route are considered eligible moving expenses. Mileage reimbursement will be made based on IRS guidelines.

II. **Ineligible Expenses**

The following cannot be made as non-taxable payments or reimbursements of moving expenses under IRS guidelines. Payments for the following types of expenses will be treated as taxable compensation to the employee and will be included in the employee’s W-2 wages. These expenses fall outside the scope of the Moving Expense Policy and associated dollar limitations and will not be reimbursed by the college:

- Storage and related expenses outside the allowable 30 days mentioned above;
- Meals consumed during the time of travel;
- **Meals and travel costs incurred by laborers**;
- Pre-move house hunting expenses;
- Temporary living expenses;
- Return trips to former residence;
- Travel expenses related to side-trips or vacation stops on the way from the former residence to the new residence;
- Other expenses per IRS guidelines such as, security deposits, lease-breaking fees, expense of selling existing residence, mortgage penalties, and other home improvements; and
- Cost of unpacking personal items;
- **Payments to non-professional movers (e.g. friends or family members) who assist the employee with the move**;
- Expenses incurred by persons not considered to be dependents for tax purposes;
- Costs of cleaning a new or former residence;
- **Costs related to immigration**;
- Utility, internet, cable/satellite, and telephone installation charges;
- **Personal telephone calls, tips, movies or other entertainment**;
- **Extraordinary items requiring special handling (e.g., boats, non-household animals, non-household items)**;
• Any other expenses not explicitly permitted by this policy or prohibited by the college Procurement Policy and Purchasing Procedures.

Expenses that are not covered by this policy are the responsibility of the employee.

III. Distance Limitation

The move of the residence must meet the minimum IRS distance requirements; the distance from the prior residence to the new job location must be 50 miles more than the distance from the prior residence to the former job location.

IV. Tax Reporting

All employee moving expenses paid by the college are subject to withholding of federal income, Social Security (or FICA Alternative), and Medicare taxes, and will be reported on the employee’s annual Form W-2. This applies whether the college is reimbursing the employee or paying the moving company directly on the employee’s behalf. For further clarification/information contact the Human Resources at (716) 888-2240.

Employees receiving a payment and/or reimbursement of relocation and moving expenses by the university should consult with their tax advisor or the Internal Revenue Service for information about moving-related expenses. The amount of eligible moving expenses reimbursed to employees by the college will be reported on the individual’s W-2 form during the year(s) in which the reimbursements occurred.

IRS Publication 521 details the federal income tax rules and regulations for individuals, in regard to moving expenses.

RELATED POLICIES

Procurement Policy and Purchasing Procedures Not Applicable.
PURPOSE
The purpose of this policy is to set forth the college’s policies, procedures, and guidelines that safeguard the rights and welfare of human subjects in any research related activity conducted at Canisius College.

POLICY
Canisius College is committed to a policy of safeguarding the rights and welfare of all human subjects in research. As standards for the ethical treatment of human subjects, the college accepts the principles set forth by the national Commission for the Protection of Human Subjects of Biomedical and Behavioral Research in its report Ethical Principles and Guidelines for the Protection of Human Subjects of Research (commonly known as the Belmont Report) and Title 45, section 46 of the U.S. Code. Anyone (faculty, students, or staff) doing any research on human subjects either outside of the classroom or within the classroom should consult with the IRB chair to determine whether their study requires IRB approval.

DEFINITIONS
Assent—an affirmative agreement by an individual not competent to give legally valid informed consent (e.g., a child or person who is cognitively impaired) to participate in research.

Human Subject—means a living individual about whom an investigator (whether professional or student) conducting research obtains: (a) information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens data through intervention or interaction with the individual; and/or (b) identifiable private information or identifiable biospecimens (45 CFR 46.102 f).

Informed Consent—a person’s voluntary agreement, based upon adequate knowledge and understanding of relevant information (purpose of study, methods used, risks and benefits involved from participation, etc.), to participate in research.
Interaction—includes communication or interpersonal contact between investigator and subject.

Intervention—includes both physical procedures by which data, information, or biospecimens are gathered (for example, venipuncture) and manipulations of the subject or the subject’s environment that are performed for research purposes. (45 CFR 46.102 f.2)

Begin Behavioral Interventions—are interactions that are brief, harmless, painless, not physically invasive, not likely to have significant adverse lasting impact, and the investigator has no reason to think the subjects will find the interventions offensive or embarrassing.

Minimal risk—means that the risks of harm anticipated in the proposed research are not greater, considering probability and magnitude, than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests. (45 CFR 46.102 i)

Principal Investigator (PI)—means a person who has ultimate administrative and fiscal authority in conducting and coordinating a research project.

Private Information—includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record). Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects. (45 CFR 46.102 f.2)

Identifiable Private Information—is private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.

Identifiable Biospecimen—is a biospecimen for which the identity of the subject is or may be ascertained by the investigator or associated with the biospecimen.

Legally Authorized Representative—means an individual, judicial or other body authorized under applicable law to consent on behalf of a prospective subject to the subject’s participation in the procedure(s) involved in the research.

Limited Review—is a review carried out by the IRB Chair or by one or more experienced reviewers designated by the chair from among members of the IRB, and is confined to approving the storage and maintenance plan for the privacy and confidentiality of identifiable data under Exempt Category (2) and (3).

Minor—generally means a person who is under the age of 18 who is not an emancipated minor except for certain purposes as specified by law.

Research—means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute research for purposes of these regulations, whether or not they are supported or funded under a program, which is considered research for other purposes. For example, some demonstration and service programs may include research activities. (45 CFR 46.102 d). Research includes questionnaires, interviews, tests, observations, surveys, and other experiments under the auspices of the college.

The following activities do not meet the definition of research and do not require IRB review:
(i) Scholarly and journalistic activities (e.g., oral history, journalism, biography, literary criticism, legal research and historical scholarship) that focus directly on the specific individuals about whom the information is collected;

(ii) Public health surveillance activities authorized by a public health authority to assess onsets of disease outbreaks or conditions of public health importance;

(iii) Certain criminal justice and intelligence activities; and

(iv) Authorized Operational Activities in support of intelligence, homeland security, defense or national security missions.

Refer to 45 CFR 46.102(l) of the revised Common Rule for the full description of the categories of activities excluded from the definition of Research.

Unanticipated or Unexpected Result—refers to an adverse event or other problem arising during the research the specificity or severity of which is not consistent with information already provided to the IRB. Adverse events are categorized as follows:

Adverse Events—undesirable and unintended, though not necessarily unanticipated, injuries or physical or emotional consequences for the subject.

Serious Adverse Events—adverse events which are fatal or life-threatening; that result in significant or persistent disability; that require hospitalization, or represent a significant hazard or potentially serious harm to research subjects or the researchers and their staff.

Unanticipated Problems—specific events experienced by subjects or developments that occur during implementation of research protocols that suggest the potential for increased risk to research subjects or the researchers and their staff.

Vulnerable Populations—human research subjects who are likely to be vulnerable to coercion or undue influence, such as children, prisoners, pregnant women, mentally disabled persons, or economically or educationally disadvantaged persons. Vulnerable subjects must be afforded special safeguards in a study to protect their rights and welfare. See 45 CFR 46.111(b) 21 CFR 56.111(b)

PROCEDURES/GUIDELINES

I. Purpose and Responsibilities of the IRB

The Canisius College Institutional Review Board (IRB) is empowered by federal agencies, including the FDA and DHHS, and bears primary authority to review, approve, monitor, and protect the rights and welfare of human subjects participating in research conducted by the college community.

In addition, the IRB:

1. Formulates human research guidelines and policies that meet federal regulations, incorporates the ethical concerns for the entire college community, and reflects the particular needs of the college’s researchers. These guidelines and policies are to be approved by the president of in consultation with the vice president for academic affairs;

2. Provides information to researchers as to the appropriate means for protecting the rights and welfare of subjects, securing the effective, free, informed consent of human subjects,
and fulfilling federal, local, and the standards of the college regarding human research; and

3. Maintains adequate records and confidentiality and prepares a yearly report for the President on the research approved.

II. Human Subject Research Procedures and Guidelines

A. Statement of Principles

The following are the principles governing Canisius College in the discharge of its responsibilities for protecting the rights and welfare of human subjects of research:

1. Research must be justifiable for its scientific or other meaningful purpose or value;
2. Even if an inquiry has scientific or other value, it must not be pursued if benefit is outweighed by risk to the subject;
3. The research must be conducted by sufficiently competent and knowledgeable people;
4. The research must be conducted under a sound design, suited to the nature of the study;
5. Informed consent is a process ensuring ethical conduct of research. No person should serve as the subject of research unless the person, or an authorized or legal representative, has given voluntary consent after being fully informed of the nature, risks, and benefits of the study and their rights as participants. Additional safeguards must be included in the study to protect the rights and welfare of subjects;
6. Participation as a subject in a research study should be voluntary, and care should be exercised to ensure that subtle pressures are not used to obtain participation;
7. Care must be taken throughout the duration of the research study (and sometimes beyond) to ensure against the risk of harm to subjects, either physical or emotional;
8. Research must be terminated if there arises a serious risk of harm to subjects, either physical or emotional;
9. The subject should be entitled to withdraw from participation in a research study at any time.

B. Criteria for IRB Approval of Research

In order to approve human subject research covered by this policy, the IRB will determine that all of the following requirements are satisfied:

1. Risks to Subjects Are Minimized

Risks to subjects are minimized: (i) by using procedures which are consistent with sound research design and which do not unnecessarily expose subjects to risk, and (ii) whenever appropriate, by using procedures already being performed on the subjects for diagnostic or treatment purposes. Minimal risk implies that the likelihood and degree of harm or discomfort expected as a result of the research are not greater than the risks encountered during the course of daily activity or during the course of routine physical or psychological examinations. Such risk considerations should not be limited to physical risk alone, but should also consider emotional and psychological risk, personal risk, and possible insurability risk.
Risks to subjects are reasonable in relation to anticipated benefits, if any, to subjects, and the importance of the knowledge that may reasonably be expected to result. In evaluating risks and benefits, the IRB should consider only those risks and benefits that may result from the research (as distinguished from risks and benefits of therapies subjects would receive even if not participating in the research). The IRB should not consider possible long-range effects of applying knowledge gained in the research (for example, the possible effects of the research on public policy) as among those research risks that fall within the purview of its responsibility.

2. **Selection of Subject is Equitable**

In making this assessment, the IRB will take into account the purposes of the research and the setting in which the research will be conducted and should be particularly cognizant of the special problems of research involving vulnerable populations, such as minors, prisoners, pregnant women, mentally disabled persons, or economically or educationally disadvantaged persons. Investigators should detail any extra precautions taken to safeguard the rights and welfare of subject populations.

3. **Informed Consent and Assent**

Informed consent has been obtained and appropriately documented from each prospective subject or the subject’s legally authorized representative, in accordance with, and to the extent required set forth in the General Requirements for Informed Consent section of this policy.

4. **Subject Safety**

Where applicable, the research plan makes adequate provision for monitoring the data collected to ensure the safety of subjects. The IRB will review who has been identified as having the primary responsibility for analyzing individual events to determine whether the study should be modified to minimize risk to current or future research subjects.

5. **Privacy of Subject & HIPAA Compliance**

When appropriate, the research plan makes adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

For research activities involving Protected Health Information (PHI), which is defined as individually identifiable information maintained in any medium, the IRB acts as the institution’s Privacy Board (required by HIPAA) to review and approve the proposed access, use, and disclosure of the PHI. The IRB is responsible for determining whether research subjects are required to sign an authorization for the use and disclosure of their PHI, or if one of the exceptions to the authorization requirements applies. Examples of these exceptions include waivers of authorization and the use of de-identified data or limited data sets.

6. **Vulnerable Subjects**

When some or all of the subjects are likely to be vulnerable to coercion or undue influence, such as minors, prisoners, pregnant women, mentally disabled persons, or economically or educationally disadvantaged persons, additional safeguards have been included in the study to protect the rights and welfare of these subjects. A full description of safeguards to ensure the fair and equitable treatment of these subjects and protect their rights and welfare can be found in the Department of Health and Human Services Office for Human Research Protections Code of Federal Regulations (see [http://www.hhs.gov/ohrp/policy/populations/index.html](http://www.hhs.gov/ohrp/policy/populations/index.html)).
7. **Required IRB Training**

The college offers an IRB training course through the [https://phrp.nihtraining.com/users/login.php](https://phrp.nihtraining.com/users/login.php). This training is up-to-date and meets the federal requirements for training in human subjects protections. Completion of this training is required for individuals participating in the IRB process, including investigators.

**C. Submission of Applications for Research Involving Human Subjects**

The Canisius College IRB will review and have authority to approve, require modifications in, or disapprove all research activities covered by this document. Any person wishing to conduct research involving human subjects must submit a proposal to the chair of the IRB. This includes faculty and staff research, graduate student projects, and undergraduate projects, including class projects. No involvement of human subjects may take place prior to formal, written notification from the IRB.

**D. Levels of IRB Review**

There are five types of IRB reviews: (1) a full board review; (2) an expedited review; (3) a limited review and (4) a continuing review. In addition, some research with human subjects is (5) exempt from review.

1. **Projects Exempt from Review**

Federal guidelines and college IRB policy permit certain types of research to proceed without IRB oversight. Exempt research activities involve no more than minimal risk and may include classroom studies, surveys, observation of public behavior, the non-invasive collection of physiological data, and the analysis of existing data that involves human subjects. Research that includes both exempt and non-exempt categories is not exempt. More detailed information regarding exempt research activities may be found at [45 CFR §46.101(b)](http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html#46.101).

Irrespective of whether a study is exempt from full review, it must meet accepted standards of protection of privacy and a subject’s right to refuse participation without penalty. The determination as to whether any particular research project qualifies as "exempt" must be made by at least one IRB member in accordance with the exemption review procedures set forth below. Investigators do not have the discretion to make this determination.

**Research Activities Exempt from IRB Full Review**

The following research activities shall normally be exempt from full IRB review:

- **Exemption #1** [45 CFR 46.104 (1)]: Research, conducted in established or commonly accepted educational settings, that specifically involves normal educational practices that are not likely to adversely impact students’ opportunity to learn required educational content or the assessment of educators who provide instruction. This includes most research on regular and special educational strategies, and research on the effectiveness of or the comparison among instructional techniques, curricula, or classroom management methods.

- **Exemption #2** [45 CFR 46.104 (2) i, ii, iii]: Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview
procedures or observation of public behavior (including visual or auditory recording) if at least one of the following criteria is met:

(i) The information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects;

(ii) Any disclosure of the human subjects’ responses outside the research would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects’ financial standing, employability, educational advancement or reputation; or

(iii) The information obtained is recorded by the investigator in such a manner that the identity of the human subjects can readily be ascertained, directly or through identifiers linked to the subjects, and an IRB conducts a limited IRB review (see Section C above) to make the determination that there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

Exemption #3 [45 CFR 46.104 (3) i, ii, iii]:

(i) Research involving benign behavioral interventions in conjunction with the collection of information from an adult subject through verbal or written responses (including data entry) or audiovisual recording if the subject prospectively agrees to the intervention and information collection and at least one of the following criteria is met:

a. The information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects;

b. Any disclosure of the human subjects’ responses outside the research would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects’ financial standing, employability, educational advancement or reputation, or

c. The information obtained is recorded by the investigator in such a manner that the identity of the human subjects can readily be ascertained, directly or through identifiers linked to the subjects, and an IRB conducts a limited IRB review (see Section C above) to make the determination that there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

(ii) For the purpose of this provision, benign behavioral interventions are brief in duration, harmless, painless, not physically invasive, not likely to have a significant adverse lasting impact on the subjects, and the investigator has no reason to think the subjects will find the interventions offensive or embarrassing. Provided all such criteria are met, examples of such benign behavioral interventions would include having the subjects play an online game, having them solve puzzles under various noise conditions, or having them decide how to allocate a nominal amount of received cash between themselves and someone else.

(iii) If the research involves deceiving the subjects regarding the nature or purposes of the research, this exemption is not applicable unless the subject authorizes the deception through a prospective agreement to participate in research in circumstances in which
the subject is informed that he or she will be unaware of or misled regarding the nature or purposes of the research.

Exemption #4 [45 CFR 46.104 (4)]: Secondary research for which consent is not required: Secondary research uses of identifiable private information or identifiable biospecimens, if at least one of the following criteria is met:

(i) The identifiable private information or identifiable biospecimens are publicly available;

(ii) Information, which may include information about biospecimens, is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained directly or through identifiers linked to the subjects, the investigator does not contact the subjects, and the investigator will not re-identify subjects.

(iii) The research involves only information collection and analysis involving the investigator's use of identifiable health information when that use is regulated under 45 CFR parts 160 and 164, subparts A and E, for the purposes of “health care operations” or “research” as those terms are defined at 45 CFR 164.501 or for “public health activities and purposes” as described under 45 CFR 164.512(b); or

(iv) The research is conducted by, or on behalf of, a Federal department or agency using government-generated or government-collected information obtained for non-research activities, if the research generates identifiable private information that is or will be maintained on information technology that is subject to and in compliance with section 208(b) of the E-Government Act of 2002, 44 U.S.C. 3501 note, if all of the identifiable private information collected, used, or generated as part of the activity will be maintained in systems of records subject to the Privacy Act of 1974, 5 U.S.C. 552a, and, if applicable, the information used in the research was collected subject to the Paperwork Reduction Act of 1995, 44 U.S.C. 3501 et seq.

Exemption #5 [45 CFR 46.104 (5) i, ii] Research and demonstration projects that are conducted or supported by a Federal department or agency, or otherwise subject to the approval of department or agency heads (or the approval of the heads of bureaus or other subordinate agencies that have been delegated authority to conduct the research and demonstration projects), and that are designed to study, evaluate, improve, or otherwise examine public benefit or service programs, including procedures for obtaining benefits or services under those programs, possible changes in or alternatives to those programs or procedures, or possible changes in methods or levels of payment for benefits or services under those programs. Such projects include, but are not limited to, internal studies by Federal employees, and studies under contracts or consulting arrangements, cooperative agreements, or grants. Exempt projects also include waivers of otherwise mandatory requirements using authorities such as sections 1115 and 1115A of the Social Security Act, as amended.

(i) Each Federal department or agency conducting or supporting the research and demonstration projects must establish, on a publicly accessible Federal Web site or in such other manner as the department or agency head may determine, a list of the research and demonstration projects that the Federal department or agency conducts or supports under this provision. The research or demonstration project
must be published on this list prior to commencing the research involving human subjects.

(ii) [Reserved]

Exemption #6 [45 CFR 46.104 (6)] Taste and food quality evaluation and consumer acceptance studies:

(i) If wholesome foods without additives are consumed, or

(ii) If a food is consumed that contains a food ingredient at or below the level and for a use found to be safe, or agricultural chemical or environmental contaminant at or below the level found to be safe, by the Food and Drug Administration or approved by the Environmental Protection Agency or the Food Safety and Inspection Service of the U.S. Department of Agriculture.

Exemption #7 [45 CFR 46.104 (7)] Storage or maintenance for secondary research for which broad consent is required: Storage or maintenance of identifiable private information or identifiable biospecimens for potential secondary research use if an IRB conducts a limited IRB review and makes the determinations required by § 46.111(a)(8).

Exemption #8 [45 CFR 46.104 (8)] Secondary research for which broad consent is required: Research involving the use of identifiable private information or identifiable biospecimens for secondary research use, if the following criteria are met:

(i) Broad consent for the storage, maintenance, and secondary research use of the identifiable private information or identifiable biospecimens was obtained in accordance with § 46.116(a)(1) through (4), (a)(6), and (d);

(ii) Documentation of informed consent or waiver of documentation of consent was obtained in accordance with § 46.117;

(iii) An IRB conducts a limited IRB review and makes the determination required by § 46.111(a)(7) and makes the determination that the research to be conducted is within the scope of the broad consent referenced in paragraph (d)(8)(i) of this section; and (iv) The investigator does not include returning individual research results to subjects as part of the study plan. This provision does not prevent an investigator from abiding by any legal requirements to return individual research results.

More detailed information regarding exempt research activities may be found at 45 CFR §46.101(d)(1-8).

Exempt Review Procedures

IRB exemption reviews may be carried out by the IRB chair, or at the discretion of the chair, by one or more experienced reviewers designated by the chair from among members of the IRB. In reviewing the research, the reviewers may exercise all of the authorities of the IRB except that the reviewers may not disapprove the research. A research activity may be disapproved only after review in accordance with the non-expedited procedure set forth in CFR 45§46.108(b).

In determining whether an IRB application and research is exempt from full IRB review, the IRB chair or other IRB member will utilize the Office for Human Research Protections decision
charts (see http://www.hhs.gov/ohrp/policy/checklists/decisioncharts.html). If the activity does not qualify for exemption, the IRB chair or a designee notifies the investigator in writing or via email. If the IRB chair, or designee, determines that an application does not qualify for exemption, the application will be processed either through Expedited Review or by Full IRB review.

The IRB reserves the right to request the investigator to provide additional information concerning applications or reports.

Note: Surveys conducted as a part of student life or student success assessment activities, as well as student life areas conducting surveys to measure academic student progress are exempt from IRB review.

2. Expedited Review

Expedited review is a procedure through which certain kinds of research may be reviewed and approved without convening a meeting of the IRB. Federal regulations make provisions for certain categories of research to be reviewed through an expedited procedure if the research involves no more than minimal risk. Expedited review is intended to enable the college to conserve administrative resources, provide timely reviews and focus the convened meetings of the IRB on those research activities involving greater risks or ethical complexities. In addition, the IRB may also use the expedited review procedure to review minor changes in previously approved research during the period covered by the original approval.

Research Categories that Meet Criteria for Expedited Review

The following categories of research may be reviewed by the IRB through an expedited review procedure:

1. Clinical studies of drugs and medical devices only when certain conditions are met;
2. Collection of blood samples by finger stick, heel stick, ear stick, or venipuncture in certain populations and within certain amounts;
3. Prospective collection of biological specimens for research purposes by noninvasive means;
4. Collection of data through noninvasive procedures (not involving general anesthesia or sedation) routinely employed in clinical practice, excluding procedures involving x-rays or microwaves;
5. Research involving materials (data, documents, records, or specimens) that have been collected, or will be collected solely for non-research purposes. (NOTE: Some research in this category may be exempt from the HHS regulations for the protection of human subjects (45 CFR 46.104). This listing refers only to research that is non-exempt);
6. Collection of data from voice, video, digital, or image recordings made for research purposes; and
7. Research on individual or group characteristics or behavior (including, but not limited to, research on perception, cognition, motivation, identity, language, communication, cultural beliefs or practices, and social behavior) or research employing survey, interview, oral history, focus group, program evaluation, human factors evaluation, or quality assurance methodologies.
(NOTE: Categories 1, 2, 3 and 4 are specific to clinical studies and/or medical procedures, which are generally not applicable at Canisius College. Also, some research in the exempt category may be exempt from the HHS regulations for the protection of human subjects (45 CFR 46.104). This listing refers only to research that is non-exempt.)

Applicability for Expedited Review

Research protocols that qualify for expedited review must meet two conditions:

1. The research must be determined to be minimal risk; and
2. All proposed research activities must be included in the list of eligible categories of expedited research as established by the DHHS for this purpose (see http://www.hhs.gov/ohrp/policy/checklists/decisioncharts.html).

Expedited review procedure may not be used where identification of the subjects and/or their responses would reasonably place them at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, insurability, reputation, or be stigmatizing, unless reasonable and appropriate protections will be implemented so that risks related to invasion of privacy and breach of confidentiality are no greater than minimal. In addition, expedited review procedures may not be used for classified research involving human subjects.

Standard requirements for informed consent (or its waiver, alteration, or exception) apply regardless of the type of review--expedited or Full Board--utilized by the IRB.

See also the Office for Human Research Protections expedited review decision chart.

Procedures for Expedited Review

Under expedited review procedures, reviews may be carried out by the IRB chair, or at the discretion of the chair, by one or more experienced reviewers designated by the chair from among members of the IRB. The expedited reviewer possesses all the same authorities as the full IRB to approve, modify, or conditionally approve the proposed research activities, except the authority to disapprove a research activity. A research activity may be disapproved only after review in accordance with the ordinary, non-expedited procedure set forth in 45 CFR 46.108(b).

Under normal circumstances, the chair or other assigned reviewer(s) is able to review protocols in this category within 30 business days after receipt of a substantively complete protocol.

3. Limited Review

Limited IRB Review is a new concept added by the Revised Common Rule and is utilized for the review of research that will record, store, maintain or, make secondary use identifiable private information (see the Research Categories that Meet Criteria for Limited Review clause below). It is an alternative to the IRB approval criteria otherwise used for review of research. In a limited IRB review, an IRB must conduct a review and make certain determinations as a condition of exemption.

Limited IRB review is designed to:

1. Ensure that there are adequate privacy safeguards for identifiable private information and identifiable biospecimens;
2. Reduce the chances that the disclosure of identifiable private information will occur and lead to harm; and

3. Respond to commenters who believe that IRB oversight should be retained for the secondary research use of identifiable private information and identifiable biospecimens.

Research Categories that Meet Criteria for Limited Review

1. Research Exempt under Category #2(iii)6 [45 CFR 46.104 (2), iii]: Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording) if the information obtained is recorded by the investigator in such a manner that the identity of the human subjects can readily be ascertained, directly or through identifiers linked to the subjects and an IRB conducts a limited IRB review to make the determination required by §__.111(a)(7).7

2. Research Exempt under Category #3(i)(C) [45 CFR 46.104 (3), i, C]: Research involving benign behavioral interventions in conjunction with the collection of information from an adult subject through verbal or written responses (including data entry) or audiovisual recording if the subject prospectively agrees to the intervention and information collection and the information obtained is recorded by the investigator in such a manner that the identity of the human subjects can readily be ascertained, directly or through identifiers linked to the subjects, and an IRB conducts a limited IRB review to make the determination required by §__.111(a)(7).

3. Research Exempt under Category # 7 [45 CFR 46.104 (7)] - Storage or maintenance for secondary research for which broad consent is required: Storage or maintenance of identifiable private information or identifiable biospecimens for potential secondary research use if an IRB conducts a limited IRB review and makes the determinations required by §__.111(a)(7).

4. Research Exempt under Category # 8 [45 CFR 46.104 (8)] -
   a. Secondary research for which broad consent is required: Research involving the use of identifiable private information or identifiable biospecimens for secondary research use, if the following criteria are met:
      i. Broad consent for the storage, maintenance, and secondary research use of the identifiable private information or identifiable biospecimens was obtained in accordance with the required elements of informed consent;
      ii. Documentation of informed consent or waiver of documentation of consent was obtained in accordance with the requirements for documentation of consent;
      iii. An IRB conducts a limited IRB review and makes the determination required by §__.111(a)(7) and makes the determination that the research to be conducted is within the scope of the broad consent; and
      iv. The investigator does not include returning individual research results to subjects as part of the study plan. This provision does not prevent an investigator from abiding by any legal requirements to return individual research results.
Procedures for Limited Review

For purposes of conducting the limited IRB review, the IRB need not apply the IRB approval criteria otherwise used for review of research, and shall make the following determinations:

1. Broad consent for storage, maintenance, and secondary research use of identifiable private information or identifiable biospecimens is obtained in accordance with the required elements of broad consent;
2. Broad consent is appropriately documented or waiver of documentation is appropriate, in accordance with the requirements for documentation of consent; and
3. If there is a change made for research purposes in the way the identifiable private information or identifiable biospecimens are stored or maintained, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

Continuing review of research is not required for research reviewed in accordance with the limited IRB review.

As an alternative to limited IRB review, the IRB may use the expedited review procedure to review research for which limited IRB review is a condition of exemption.


4. Full IRB Committee Review

A Full-board review occurs when a proposal and research protocols involve more than minimal risk to research participants or vulnerable populations of research participants (other than minors when the protocol qualifies for expedited review) and are reviewed by the IRB at a convened meeting. Full board review is required for studies that involve greater than minimal risk or vulnerable populations that require special protection by the IRB. These populations include, but are not limited to: pregnant women, human fetuses and neonates, prisoners, and minors.

The IRB will attempt to review any full-IRB research proposal and respond with a decision within thirty (30) days of receipt of the proposal. When a proposal is submitted, it is checked for completeness. The IRB will evaluate the proposal for the extent to which it provides for the protection of human subjects, demonstrates scientific merit and meets the criteria set forth in the Criteria for IRB Approval of Research section above. In order for the application to be approved, it must receive the approval of a majority of those members present at the meeting, including at least one member whose primary concerns are in nonscientific areas. The IRB chair will notify the investigator of the outcome of the full review.

a. Research Reviewed Elsewhere

In certain instances, an investigator from Canisius College may be involved in a collaborative research project involving human subjects which is to be conducted at another institution. If this project has already been approved by the IRB at the collaborating institution, Canisius College's IRB Chair may waive review requirements by the Canisius College IRB if the collaborating institution's IRB is willing to enter into an Institutional Review Board Authorization Agreement, which would allow Canisius College's investigator to rely on the IRB oversight and OHRP Federalwide Assurance (FWA) at the collaborating institution. Likewise, Canisius College may
provide IRB oversight to a collaborating institution by entering into an IAA as the institution providing IRB review.

5. Continuing Review

The IRB is required by the Revised Common Rule (Section II.109(e)) to conduct continuing review of research requiring review by the full IRB (i.e., full review) at intervals appropriate to the degree of risk, not less than once per year. Each year, the IRB will send PIs an Annual Progress Report to complete. Continuing reviews are required until the research involves only data analysis, or “accessing follow-up clinical data from procedures that subjects would undergo as part of clinical care” – unless the IRB reviewer provides a justification that continuing review beyond this point would enhance protection of research subjects.

Under the revised Common Rule, continuing review is not required for:

1. Research that is eligible for expedited review;
2. Exempt research conditioned on limited IRB review; and
3. Research that has completed all interventions and now only includes analyzing data, even if the information or biospecimens are identifiable.

The IRB may override this default and still choose to require continuing review, as long as the IRB documents the decision and the rationale for this decision. Refer to 45 CFR 46.109(f), 46.110, and 46.115(a)(8) of the revised Common Rule.

Investigators still have the obligation to report various developments (such as unanticipated problems, adverse events or proposed changes to the study) to the IRB.

Pre-2019 Research

Any study approved prior to January 21, 2019 will be subject to the college’s prior Human Subject Research Policy.

Annual Reporting

The discontinuing of continuing review for most research means that the IRB will no longer send Annual Progress Reports to PIs. However, Investigators should report to the IRB, on at least an annual basis, the withdrawal of subjects after informed consent for reasons related to the research study, or complaints from subjects or their legally authorized representatives (for example, parents or guardians). If there are not such events, investigators do not need to provide an annual report to the IRB.

E. Conflicts of Interest

If a member of the IRB wishes to conduct a study, that committee member may submit the study for expedited review to any other IRB member, or for committee review through any other IRB member; however, that member cannot participate in the evaluation.

F. IRB Action & Length of Approval

The investigator will be notified in writing (print or electronic) of the IRB’s action on the research proposal. These actions include:
Full Approval: The IRB approves the proposed purpose and design as described in the application for a period of one (1) year to conduct the approved research study. The investigator is responsible for informing the IRB in writing of any change or modification made to the study after approval is secured and/or continuing progress reports may be required.

Contingent Approval: An application receiving contingent approval requires additional information or minor revision. When the requested changes have been made, the IRB chair has the authority to provide full approval.

Denial: This is a rare action and is taken only when, in the judgment of IRB members, the risks of the research outweigh the benefits to study participants, or other, significant problems exist specific to the proposed study.

Suspension or Termination: The IRB has the authority to suspend or terminate any research project, including projects with full approval, that is not being conducted in accordance with the IRB’s decisions, conditions, and requirements, or when unexpected serious harm to human subjects has been discovered. The investigator will receive a written explanation of the decision for suspension or termination. Any suspension or termination of approval will be determined by the committee as a whole, shall include a statement of the reasons for the IRB’s action and shall be reported promptly to the investigator and appropriate college officials.

G. Periodic Review of the Approved Research

An approved IRB protocol is valid for one year. The investigator must apply for renewal of the protocol prior to expiration of the previously approved protocol. See the Continuing Review section above for additional information.

H. Revisions and Resubmission of Rejected Research Proposals

If an application has been rejected, the applicant may revise the proposal and resubmit it to the IRB. If the IRB deems that all the objections have been answered, the IRB may approve the study.

I. Unanticipated or Unexpected Results

In the event of an unanticipated or unexpected result, the investigator is required to submit a written report to the IRB. It should contain sufficient information for the IRB to judge whether or not the event raises new questions about either the risk/benefit ratio or the design of the research. Typically, the written report serves as IRB notification; however, in the instance of a serious adverse event, the investigator must notify the IRB immediately then file the report within the time frame noted below. The time frame for the submission of the report is determined by the type of unanticipated or unexpected event that has occurred.

- When an adverse event is serious and unanticipated, the investigator must notify the IRB in writing within 24 hours or by the end of the next working day.
- When an adverse event is serious but not unanticipated, the investigator must notify the IRB within five (5) working days.
- When an adverse event occurs which is not serious but is unanticipated, the investigator must notify the IRB within 10 working days.
- When an unanticipated problem (UP) occurs which does not meet the definition of an adverse event, the investigator must notify the IRB within 10 working days.
The written report must contain the following information: IRB study number; Title of Protocol; Name of Principal Investigator; Date of Event; Description of Event including nature of injury or other adverse occurrence, assessment of severity, and assessment of the relationship to the study; Handling/response of the investigator to the event; Proposed changes in either research protocol or consent form in response to the event; and Signature of the investigator.

J. Proposed Changes to Research Protocol

The investigator is responsible for obtaining prior approval for proposed changes to an approved research protocol.

The Revised Common Rule allows the IRB to use expedited review procedures for minor changes in previously approved research during the period for which approval is authorized. Expedited review procedures may be used for certain kinds of research involving no more than minimal risk, and for minor changes in approved research (see CFR 45 §46.110). Examples of minor changes that do not require IRB review include, but are not limited to:

1. Minor changes to wording of the recruitment materials that do not alter the risks or benefits to study participants (e.g., addition of a sentence to provide more information about timing or scheduling);
2. Minor procedural changes that do not alter the risks or benefits to study participants or that would reduce risk to participants (e.g., changes in the order of task administration);
3. Minor adjustment of the number of trials used; discontinuing the use of an approved self-report measure; omitting a portion of an approved experimental task);
4. Editorial changes that clarify but do not alter the existing meaning of an approved document (including the consent form) or instrument;
5. Correction of typographical errors on the consent form; and
6. Inclusion of new student research assistants with appropriate human subjects training and under the supervision of a faculty mentor.

Under an expedited review procedure, the review may be carried out by the IRB chair or by one or more experienced reviewers designated by the chair from among members of the IRB. In reviewing the research, the reviewers may exercise all of the authorities of the IRB except that the reviewers may not disapprove the research. A research activity may be disapproved only after review in accordance with the non-expedited procedure set forth in CFR 45 §46.108(b).

Changes that must be submitted to the full IRB for review include:

1. Significant changes in subject recruitment or selection/exclusion procedures, or in your research protocol (including in questionnaires, interviews or other data collection procedures, or in research sites/locations);
2. Changes in the informed consent procedures or the informed consent form(s) that alter the information given to participants with respect to procedures, risks and/or benefits, or that might affect their willingness to participate;
3. Changes in data monitoring procedures to protect the safety of participants, such as monitoring for suicidal ideation, or other risks of harm to self or others;
4. Changes in procedures that were designed to reduce any risks to participants, such as procedures to protect confidentiality;

5. Other changes that may affect the risks to subjects, or the balance of risks and benefits;

6. Changes in the PI or other key personnel.

The IRB office must have copies of the most up-to-date protocols and consent documents, even if they did not require an IRB amendment.

If the procedural change is judged to involve more than minimal risk, intentional deception, or questions pertaining to a protected population and does not meet the categories for exempt or expedited review it must be presented to a convened full review board for discussion and consideration of approval or non-approval.

The IRB reserves the right to request the investigator to provide additional information concerning the application for a procedural change. After review, the IRB will send the applicant formal notification of IRB actions.

K. Informed Consent

1. General Requirements for Informed Consent

Informed consent must be obtained from all research participants, regardless of the level of IRB review. In these instances, the investigator must ensure that the informed consent of each subject is documented.

The following are matters that must be communicated to a subject before informed consent is given:

- A statement of the purpose of the human subjects research, the expected duration of the subject’s participation, a description of any procedures to be followed, and an identification of any procedures that are experimental;
- A description of any treatment included in the research, and the probability of random assignment to each treatment;
- A description of any foreseeable risks and benefits to the subject;
- If the research involves a risk of harm to the subject, an explanation of whether any compensation or medical treatment is available if injury occurs to the subject and if so, what that compensation or treatment will be;
- A statement of the subject’s responsibilities with respect to the research;
- A statement describing how confidentiality will be maintained or private information identifying the subject will be dealt with;
- A statement concerning the access to the subject’s records that the IRB and any auditors will have for the verification of the procedures and data associated with the research;
- The name and contact details of a person the subject may contact for further information regarding the research, a statement of the subject’s rights, and the name and contact details of a person the subject should contact in the event of injury arising in conjunction with the research; and
A statement that the subject’s participation is voluntary, that refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and that the subject may stop participating at any time without penalty or loss of benefits to which the participant is entitled; and

One of the following statements is required about any research that involves the collection of identifiable private information or identifiable biospecimens:

- A statement that identifiers might be removed from the identifiable private information or identifiable biospecimens and that, after such removal, the information or biospecimens could be used for future research studies or distributed to another investigator for future research studies without additional informed consent from the subject or the legally authorized representative, if this might be a possibility; or

- A statement that the subject’s information or biospecimens collected as part of the research, even if identifiers are removed, will not be used or distributed for future research studies.

**Additional Elements of Informed Consent**

To the extent that is relevant, the informed consent must also include:

- A statement addressing any cultural or religious concerns of the subject;
- A description of any foreseeable risks to an unborn fetus carried by the subject or to an infant being nursed by the subject;
- A statement that the research may involve risks to the subject (or an embryo or fetus carried by the subject, if the subject is or may become pregnant) that are currently unforeseeable; a statement of any anticipated circumstances under which the subject’s participation in the research may be terminated by the Investigator without the subject’s consent;
- A statement of any costs to the subject that may result from participation in the research;
- A statement of the consequences of a subject’s decision to withdraw from the research and a description of the procedures for an orderly termination of participation by the subject; and

- A statement that any significant new findings developed during the course of the research, if they may relate to the subject’s willingness to continue participation, will be provided to the subject;

- The approximate number of subjects involved in the study;
- A statement that the subject’s biospecimens (even if identifiers are removed) may be used for commercial profit and whether the subject will or will not share in this commercial profit;
- A statement regarding whether clinically relevant research results, including individual research results, will be disclosed to subjects, and if so, under what conditions; and
For research involving biospecimens, whether the research will (if known) or might include whole genome sequencing (i.e., sequencing of a human germline or somatic specimen with the intent to generate the genome or exome sequence of that specimen).

Vulnerable Subjects: A principal investigator who seeks to obtain informed consent from vulnerable individuals must provide additional elements of protection, both with regard to obtaining and documenting informed consent, where that is necessary, and for the welfare of the subject. In the case of vulnerable subjects, consent is typically obtained from parent(s) or legal guardian(s). However, an understandable explanation of the research procedures should also be given to the minors or other vulnerable participants (populations such as prisoners, those who lack the capacity to consent, non-english speaking individuals, etc.) for whom consent has been obtained, and they should be given the chance to volunteer to participate in the proposed activity. Their wishes determine their participation.

2. Documentation of Informed Consent

Informed consent shall be documented by the use of a written consent form and signed by the subject or the subject’s legally authorized representative. A copy shall be given to the person signing the form.

The consent form must embody the elements of informed consent. This form may be read to the subject or the subject’s legally authorized representative, but in any event, the investigator shall give either the subject or the representative adequate opportunity to read it before it is signed.

The Revised Common Rule (45 CFR 46.116(a)(5)(i)) requires that informed consent form begin with a concise and focused presentation of the key information that is most likely to assist a prospective subject or legally authorized representative in understanding the reasons why one might or might not want to participate in the research. This part of the informed consent must be organized and presented in a way that facilitates comprehension.

Moreover, the consent form must indicate either that information or biospecimens collected for the research might be stripped of identifiers and used in other research in the future, or that this will not happen. Note that this is only about future research use of information and biospecimens that will be stripped of identifiers. Consent for the future use of identifiable private information and identifiable biospecimens for future unspecified research is covered under the section for “broad consent,” or could also occur under conditions where an IRB determines that a waiver of informed consent is appropriate.

a. Waiver of Informed Consent Documentation

The IRB may waive the requirement for the investigator to obtain a signed consent form for some or all subjects if it finds either:

- That the only record linking the subject and the research would be the consent document and the principal risk would be potential harm resulting from a breach of confidentiality. Each subject will be asked whether the subject wants documentation linking the subject with the research, and the subject’s wishes will govern; or

- That the research presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required outside of the research context.
In cases in which the documentation requirement is waived, the IRB may require the investigator to provide subjects with a written statement regarding the research.

Oral consent, however, is still required and the investigator must provide all of the above information.

3. **Parental Consent/Child Assent**

For individuals with “diminished autonomy” (for example, children), informed consent procedures typically involve obtaining consent from an individual who has the legal authority to make decisions about the individual’s participation in research. In the case of children, The Ethical Standards for Research with Children of the Society for Research in Child Development suggest that informed consent should be obtained from parents, legal guardians or those who act in loco parentis (e.g., teachers, school superintendents). Where feasible, children should also be given the opportunity to assent to participate, even if they do not fully comprehend the full significance of such assent, as well as the opportunity to refuse to participate.

34. **Internet-Based Human Subject Research**

All internet-based research studies must incorporate the principles of voluntary participation and informed consent; maintain the confidentiality of information obtained from or about human subjects; and appropriately address possible risks to participants, including psychosocial stress and related risks.

Internet-based research may not be suitable for studies involving greater than minimal risk, particularly where the research involves vulnerable populations or data that:

- Places subjects at risk of criminal or civil liability;
- Could damage subjects’ financial standing, employability, insurability, or reputation; or
- Places subjects at risk for identity theft.

Exceptions to the minimal-risk standard may be made at the discretion of the IRB, but may involve additional consent requirements as defined below.

**Recruitment:** Internet-based procedures for advertising a study and recruiting potential participants must follow the IRB guidelines for recruitment that apply to any traditional media, such as newspapers and bulletin boards. Additionally, advertising and recruitment efforts must comply with the college’s information technology policies.

**Informed Consent Process for Internet-Based Research:** Typically, internet-based research involving minimal risk to participants does not necessitate hard-copy documentation of consent. Instead, a variation of the following statement must be visible on the screen prior to entering the survey: “Confidentiality will be maintained to the degree permitted by the technology used. Your participation in this online survey involves risks similar to a person’s everyday use of the internet. By clicking “submit” upon completion of the survey, you are granting consent for your responses to be included in the research study.”

**Internet-Based Research Involving Minors:** Investigators are not permitted to collect personal information from a child without posting notices about how the information will be used and without obtaining parental permission. Written permission must be obtained via postal mail or
A face-to-face interview must be conducted to obtain parental consent for studies with minors that involve more than minimal risk.

45. Students as Research Subjects

It is the college’s general position that teachers should not use their own students as subjects in their research if it can be avoided. The college recognizes, however, that in some research situations, use of one’s own students is integral to the research. This is particularly true of research into teaching methods, curricula and other areas related to the scholarship of teaching and learning. The following are two models of research design that may be permissible to the IRB:

- Collection of Data by Third Party: In situations where the activities to be undertaken by the students are not part of required class activities, and thus students may or may not choose to participate, the instructor/researcher should arrange to have the data collected by an independent third party, so that the instructor does not know who participated, and does not have access to the identifiable data or identity of participants for any purpose until grades have been assigned and entered.

- Collection of Data by Instructor/Researcher: In situations where the collection of data by a third party is not feasible, the IRB may approve the research if the student provides written consent to use the data, e.g., test results, papers written, homework, etc., after grades are entered.

Note: The giving of course credit or extra credit to students who participate in research as part of a course requirement will be approved by the IRB only when alternative means of obtaining credit is made available to students who do not wish to volunteer as research subjects. The IRB will carefully review these alternatives to make sure that students are not being coerced into becoming subjects. The informed consent statement must make clear the consequences of withdrawing from a project prior to completion.

56. Payment to Research Participants

It is not uncommon for subjects to be paid for their participation in research. Payment to research subjects for participation in studies must not be considered a benefit. Financial incentives are often used when health benefits to a subject are remote or non-existent. The amount and schedule of payment must be presented to the IRB at the time of the initial review. The IRB will review both the amount of the payment and the proposed method and timing of disbursement to assure that neither are coercive nor present undue influence.

7. General Waiver or Alteration of Informed Consent

Informed consent may be waived or altered under the following conditions:

a. Waiver

The IRB may waive the requirement to obtain informed consent provided the IRB finds and documents that:

1. The research involves no more than minimal risk to the subjects;

2. The research could not practicably be carried out without the requested waiver or alteration;
3. If the research involves using identifiable private information or identifiable biospecimens, the research could not practicably be carried out without using such information or biospecimens in an identifiable format;

4. The waiver or alteration will not adversely affect the rights and welfare of the subjects; and

5. Whenever appropriate, the subjects or legally authorized representatives will be provided with additional pertinent information after participation.

b. Alteration

If a total waiver is not approved, an IRB may approve a consent procedure that omits or alters some of the elements of informed consent. However, there are complicated restrictions on alterations, and the Revised Common Rule does not allow the IRB to approve alterations of the general requirements, including requirements that:

1. Informed consent is obtained prior to beginning the research;

2. Without coercion and under circumstances that allow opportunity to discuss and consider whether or not to participate;

3. With information presented in language that is understandable to the participant or legally authorized representative;

4. The participant is provided with the information a “reasonable person” would want to have;

5. The informed consent begins with a concise and focused presentation of the key information; and

6. Does not include any exculpatory language that waives or appears to waive “any of the subject’s legal rights, or releases or appears to release the investigator, the sponsor, the institution, or its agents from liability for negligence.”

Alterations must also meet the same conditions as those for a waiver of informed consent.

If a broad consent procedure is used, the IRB may not omit or alter any of the elements required for broad consent.

c. Requirements for Waiver and Alteration:

In order for an IRB to waive or alter consent as described in this subsection, the IRB must find and document that:

1. The research involves no more than minimal risk to the subjects;

2. The research could not practicably be carried out without the requested waiver or alteration;

3. If the research involves using identifiable private information or identifiable biospecimens, the research could not practicably be carried out without using such information or biospecimens in an identifiable format;

4. The waiver or alteration will not adversely affect the rights and welfare of the subjects.

Whenever appropriate, the subjects or legally authorized representatives will be provided with additional pertinent information after participation.

8. Broad Consent
The Final Common Rule allows the use of “broad consent” (i.e., seeking prospective consent to unspecified future research) from a research participant for storage, maintenance, and secondary research use of identifiable private information and identifiable biospecimens.

Broad consent is an optional alternative that an investigator may choose instead of, for example, conducting the research on nonidentified information and nonidentified biospecimens, requesting an institutional review board (IRB) waive the requirement for informed consent, or obtaining consent for a specific study.

a. Required Elements of Broad Consent
b. The following information:
   a. A description of any reasonably foreseeable risks or discomforts to the subject;
   b. A description of any benefits to the subject or to others that may reasonably be expected from the research;
   c. A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained;
   d. A statement that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled; and
   e. When appropriate:
      i. A statement that the subject’s biospecimens (even if identifiers are removed) may be used for commercial profit and whether the subject will or will not share in this commercial profit;
      ii. For research involving biospecimens, whether the research will (if known) or might include whole genome sequencing (i.e., sequencing of a human germline or somatic specimen with the intent to generate the genome or exome sequence of that specimen).
   c. A general description of the types of research that may be conducted with the identifiable private information or identifiable biospecimens. This description must include sufficient information such that a reasonable person would expect that the broad consent would permit the types of research conducted;
   d. A description of the identifiable private information or identifiable biospecimens that might be used in research, whether sharing of identifiable private information or identifiable biospecimens might occur, and the types of institutions or researchers that might conduct research with the identifiable private information or identifiable biospecimens;
   e. A description of the period of time that the identifiable private information or identifiable biospecimens may be stored and maintained (which period of time could be indefinite), and a description of the period of time that the identifiable private information or identifiable biospecimens may be used for research purposes (which period of time could be indefinite);
f. Unless the subject or legally authorized representative will be provided details about specific research studies, a statement that they will not be informed of the details of any specific research studies that might be conducted using the subject’s identifiable private;

g. Unless it is known that clinically relevant research results, including individual research results, will be disclosed to the subject in all circumstances, a statement that such results may not be disclosed to the subject; and

h. An explanation of whom to contact for answers to questions about the subject’s rights and about storage and use of the subject’s identifiable private information or identifiable biospecimens, and whom to contact in the event of a research-related harm.

Note: If an individual was asked to provide broad consent for the storage, maintenance, and secondary research use of identifiable private information or identifiable biospecimens and refused to consent, the IRB cannot waive consent for the storage, maintenance, or secondary research use of the identifiable private information or identifiable biospecimens.

L. Completion

Unless the IRB is informed otherwise, research studies are deemed completed on calendar year from the date of approval.

M. Non-Compliance

The IRB is responsible for determining the validity of all allegations of noncompliance with respect to human subjects research activities conducted under the auspices of the College and, if found to be non-compliant, determining whether it constitutes non-compliance that is serious or continuing in nature. If it is determined that a research protocol is not in compliance with regulations, regardless of whether it received prior review and approval by the IRB, it may direct corrective action to be taken.

There are two levels of noncompliance:

- **Serious**: non-compliance that may affect the rights and welfare of participants including: (i) conducting non-exempt human research without submitting an IRB protocol; (ii) actions that compromise confidentiality of the participants or the integrity or validity of the research; (iii) actions that harm the participants either physically, psychologically or emotionally; (iv) the use of subjects from federally identified protected groups, which were not identified on the IRB protocol; (v) failure to report serious events, unanticipated problems, or substantive changes to the proposed protocol to IRB.

- **Continuing**: a pattern or multiple instances of non-compliance that: (i) indicates a lack of understanding or disregard for the regulations or institutional requirements that protect the rights and welfare of participants and others; (ii) compromises the scientific integrity of a study such that important conclusions can no longer be reached; (iii) suggests a likelihood that noncompliance will continue without intervention; or (iv) involves frequent instances of noncompliance or a failure to respond to a request from the IRB to resolve an episode of noncompliance or a pattern of minor noncompliance.

All cases of alleged non-compliance are to be reported to the IRB chair on an immediate basis. Reports can be made by research subjects, members of the research team or anyone else familiar with the research project.
The IRB chair will inform the principle investigator (and sponsoring agency if applicable) that a non-compliance report has been made. The IRB chair will also determine whether the report is serious enough to merit suspension of the research.

- The IRB chair will investigate and determine whether the alleged non-compliance is serious or continuing. In the case of alleged serious or continuing non-compliance, the IRB chair will call a meeting of the full IRB. The researcher will be given the opportunity to attend the meeting to present information, but may not be present while the IRB makes its decisions. The IRB will determine whether action needs to be taken, and if so what form it will take. This can include requiring changes be made to the protocol, assigning a person to monitor the remainder of the research, requiring the researcher to undergo training, or suspension/termination of the research.

For cases of serious or continuing noncompliance, the IRB chair will report to the vice president for academic affairs the non-compliance and the IRB’s decisions on remedial action. In cases of continuing non-compliance, the matter may be referred to the dean for appropriate disciplinary action pursuant to the *Faculty Handbook*.

For cases that are determined not to be serious or continuing, the review will end. However, corrective action may be instituted. Examples include the imposition of improvement plans, additional training, and/or the requiring the prompt submission of evidence of compliance with IRB requirements.

**N. Confidentiality**

An investigator must not disclose any personal information obtained for the purposes of human subjects research without the express consent of the subjects or donor to whom it relates (or legally authorized representative), except where: disclosure is necessary to eliminate any apparent immediate risk of harm to the subject, donor, or to any other person; and the disclosure is the minimum necessary for the purpose of eliminating such harm.

If personal information relating to a subject or donor is, or is likely to be, disclosed without consent, the investigator must immediately inform that subject or donor (or legally authorized representative): of the disclosure and of its purpose and extent; and that any person given access to the information will be required by the researcher to be subject to a duty of confidentiality, and must ensure that any 3rd parties to whom the information is disclosed will be subject to a legally binding duty of confidentiality.

**III. Monitoring Authorized Research Proposals**

A principle investigator must at all times:

1. Act in accordance with the terms of the authorized research proposal (including any revisions or conditions specified by the IRB when approving the proposal);
2. Comply with federal, state and local laws and regulations, as well as college policies and procedures;
3. Permit the IRB to observe, or have a third party observe on its behalf, the conduct of the research; and
4. Permit the IRB to audit, or have a third party audit on its behalf, the research facilities, files, and progress reports.
A principal investigator must promptly notify the IRB of any: material change in circumstances occurring after the approval of a research proposal; or inaccuracy, of which it has since become aware, in any information provided to the IRB in support of the authorized research proposal. Additionally, a principal investigator must promptly notify the IRB of any suspension or premature termination of its research, and of the reasons for that suspension or termination. Finally, a principal investigator must immediately restrict, suspend, or terminate research where it is directed by the IRB to do so.

In carrying out an approved research project, a principal investigator must submit to the IRB a safety report immediate upon the occurrence of any serious adverse event.

**Investigator Responsibilities**

(Adapted from OHRP) Investigators play a crucial role in protecting the rights and welfare of human subjects and are responsible for carrying out sound ethical research consistent with research plans approved by an IRB. Along with meeting the specific requirements of a particular research study, investigators are responsible for ongoing requirements in the conduct of approved research that include, in summary:

1. Obtaining and documenting informed consent of subjects or subjects’ legally authorized representatives prior to the subjects’ participation in the research, unless these requirements have been waived by the IRB;

2. Obtaining prior approval from the IRB for any modifications of the previously approved research, including modifications to the informed consent process and document, except those necessary to eliminate apparent immediate hazards to subjects;

3. Ensuring that amendments, requests for continuing review and approval, and notification of completion of the research study are submitted to the IRB in accordance with IRB policy and procedures.

4. Providing to the IRB prompt reports of any unanticipated problems involving risks to subjects or others;

5. Providing to the IRB prompt reports of serious or continuing noncompliance with the regulations or the requirements or determinations of the IRB; and

6. Keeping certain records, including informed consent forms, as required by the HHS regulations for at least three years after completion of the study.

**III. Record-Keeping by the Institutional Research Review Board**

The college, or when appropriate an IRB, shall prepare and maintain adequate documentation of IRB activities, including the following:

- Copies of all research proposals reviewed, scientific evaluations, if any, that accompany the proposals, approved sample consent documents, and reports of adverse events.

---

1 If all research-related interventions or interactions with human subjects have been completed, and all data collection and analysis of identifiable private information described in the IRB-approved research plan have been finished, then the human subjects research study has been completed.
- Actions taken by the IRB and separate deliberations for each action.
- Minutes of all convened IRB meetings which shall be in sufficient detail to show attendance at the meetings; actions taken by the IRB; the vote on these actions including the number of members voting for, against, and abstaining; the basis for requiring changes in or disapproving research; and a written summary of the discussion of controverted issues and their resolution. The recusal of any IRB members because of a conflicting interest shall also be documented when recording votes on IRB actions.
- Copies of all correspondence between the IRB and the investigators.
- A list of IRB members in the same detail as described in §46.103(b)(3).
- Written procedures for the IRB in the same detail as described in §46.103(b)(4) and §46.103(b)(5).
- Statements of significant new findings provided to subjects, as required by §46.116(b)(5). CFR 45§46.116(b)(5) (informed consent). This is: A statement that significant new findings developed during the course of the research which may relate to the subject's willingness to continue participation will be provided to the subject;
- Required determinations and protocol-specific findings justifying those determinations for:
  - Waiver or alteration of the consent process. [45 CFR 46.116(c) and (d)]
  - Justification for the waiver of the requirement for written documentation of consent [45 CFR 46.117]
  - Research involving pregnant women, fetuses, and neonates. [45 CFR 46.204]
  - Research involving prisoners. [45 CFR 46.306]
  - Research involving children. [46 CFR 46.404-407]
  - The rationale for determining that risk associated with using a medical device in a study is significant or non-significant (referred to as significant risk/non-significant risk device determinations).
  - When the expedited procedure for review is used, documentation of discussions, decisions, and findings will be included in the protocol file.

The records required by this policy shall be retained for at least 3 years, and records relating to research, which is conducted, shall be retained for at least 3 years after completion of the research. All records shall be accessible for inspection and copying by authorized representatives of the federal department or agency at reasonable times and in a reasonable manner when applicable.

IV. Duration of Approvals

Approvals shall be in force for a period of one calendar year from the date of approval. If the project is not completed in that period, the researcher may simply submit a letter indicating that the project is continuing. So long as there have been no changes in the study or in the ethical standards of Canisius College or of the relevant discipline, the IRB member may approve the study. At this point, the approval is extended for a period of one calendar year from the date of
the new approval. If the study or the relevant research standards have changed, the study may be submitted for expedited or committee review.

RELATED POLICIES

Classification as a Gift or Grant Policy

Grant Accounting Policy

Principal Investigators Policy

Research Ethics and Conduct Policy
PROPOSED POLICIES

COLLEGE INTERN POLICY

Effective Date: 

Policy Number: III - 

Supersedes: Not Applicable. 

Issuing Authority: President 

Responsible Officer: Associate Vice President, Human Resources & Compliance 

Applicability: All Canisius College departments that engage Interns. 

History: 

PURPOSE

The purpose of this policy is to provide guidance for college departments seeking to provide a structured learning environment to unpaid Interns. Note that this policy does not apply to the approval of a student internships for academic credit as part of an academic degree earned at Canisius College or a course offered at Canisius College. 

POLICY

College departments may provide a structured learning environment to unpaid Interns. Internships must be properly authorized by the host department and Human Resources in accordance with the procedures set forth in this policy. Authorized Interns are agents of the college; therefore, qualifications, background, and suitability of the individual must be considered before offering an Intern opportunity. Moreover, any individual listed on a sex offender registry or who has been convicted of an offense for which he or she must register as a sex or violent offender may not serve as an Intern. No department may discriminate in selecting Interns based on any status protected by state or federal law.

The college shall have no liability for personal injury or property damage which may be suffered by the Intern, unless such injury or damage directly results from the negligent acts or omissions of the college or its employees. 

Department heads providing internship opportunities are accountable and responsible for compliance with this policy and may be subject to disciplinary action for the department’s failure to comply. 

DEFINITIONS
Intern(s)—a student or trainee who accepts a short-term unpaid, supervised work experience at Canisius College for the purposes of educational or professional interest. In determining whether an individual is an Intern, the college will consider the following criteria:

1. The extent to which the intern and the college clearly understand that there is no expectation of compensation. Any promise of compensation, express or implied, suggests that the intern is an employee—and vice versa;

2. The extent to which the internship provides training that would be similar to that which would be given in an educational environment, including the clinical and other hands-on training provided by educational institutions;

3. The extent to which the internship is tied to the intern’s formal education program by integrated coursework or the receipt of academic credit;

4. The extent to which the internship accommodates the intern’s academic commitments by corresponding to the academic calendar;

5. The extent to which the internship’s duration is limited to the period in which the internship provides the intern with beneficial learning;

6. The extent to which the Intern’s work complements, rather than displaces, the work of paid employees while providing significant educational benefits to the intern; and

7. The extent to which the Intern and the college understand that the internship is conducted without entitlement to a paid job at the conclusion of the internship.

PROCEDURES/GUIDELINES

I. Eligibility

Any Intern may serve at Canisius College with the following restrictions:

1. An Intern cannot replace or be substituted for current employees or perform work that would otherwise require another individual to be employed;

2. Individuals under the age of 14 may not serve as an Intern. Individuals who are at least 14 years old but under the age of 18 must have parental consent;

3. Interns who do not hold U.S. Citizenship or permanent residency should consult IDENTIFY OFFICE for any information related to visa status. An individual with a pending H-1B visa application to work at the college may not serve as an Intern; and

4. Any individual listed on a registry that is part of the college’s criminal record check or who has been convicted of an offense for which he or she must register as a sex or violent offender may not serve as an Intern.

II. Selection and Assignment

The following procedures are required to engage an Intern:

1. A department that desires to accommodate an Intern must complete a description of the duties to be performed by the Intern and obtain written approval from the appropriate vice president and Human Resources. The description of duties must include the following:

   a. Title and name of supervisor;
b. Dates of the internship;
c. Schedule / hours of work;
d. Where duties will be performed;
e. Activities to be performed;
f. Training provided by supervisor or others in the department;
g. Personal, educational, or professional benefits the Intern should derive from the internship;
h. How the internship relates to the Intern’s course of study, including whether the Intern will receive course credit from Canisius College or another college or university;
i. Benefits, if any, to the college;
j. Safety or risk issues; and
k. How the Intern’s services will be measured or evaluated.

2. After receiving approval from the appropriate vice president, each Intern (or their parent/guardian) must complete applicable Human Resources paperwork and, if determined necessary by Human Resources, satisfactorily complete a background check (see the Background, Reference, and Verification Screens Policy);

3. Each Intern must complete a Release and Waiver of Liability Form. The completed form is then forwarded to Human Resources for filing; and

4. The department head must ensure that the Intern receives appropriate training prior to their beginning the internship at the college.

**IV. Intern Responsibilities**

An Intern must complete and sign a Release and Waiver of Liability Form and any other forms required by Human Resources.

An Intern must comply with all applicable college and department policies and procedures, as well as legal requirements that govern their actions. These include but are not limited to those relating to employee conduct, safety, confidentiality, sensitive information, protected health information, college computer and network system use, financial responsibility, and drug or alcohol use. Department heads are responsible for making certain Interns comply with all applicable college and department policies and procedures, as well as applicable laws and regulations.

**V. Dismissal**

The department sponsoring the internship or Human Resources may decline and/or discontinue the Internship at any time and without advance notice. Similarly, the Intern may end service at any time.

**RELATED POLICIES**

Background, Reference, and Verification Screens Policy
INTERN REGISTRATION FORM

This portion of the form to be filled out by the Volunteer:

Social Security No: __________________________

Last Name: ___________________________ First Name: ___________________________
Middle Initial: __________

Preferred First Name: ______________________ Date of Birth: ______________________

Gender: ___________________________

Permanent Address:
_____________________________________________________________________________

City: ___________________________ State: ____________ Zip Code: ______________________

Telephone #: ___________________________

Do you have health insurance? Yes ___ No ___

If yes, please provide Medical Insurance Carrier:
(Optional)________________________________________________________

EMERGENCY CONTACT INFORMATION:

Last Name: ___________________________ First Name: ___________________________Middle Initial: __________

Relationship__________________________

Street Address: __________________________ City: __________________________

State: __________ Zip: __________

Phone:( ____ ) - __________ Ext: __________

I have carefully read the Canisius College Volunteer Policy and information above and understand their contents. The above information provided by me is accurate.

_____________________________________________________________________________
Volunteer’s Signature Date

This portion of the form is to be filled out by the department supervisor:

Department Head Name: ____________________________________________________________

Department Head Title: ____________________________________________________________

Internship Dates: _____/_____/_____ to _____/_____/_____

Start                                             End

Description of Intern Responsibilities:

_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________
_____________________________________________________________________________

Department Head Signature Date

Please submit this form to Human Resources.
INTERN RELEASE AND WAIVER OF LIABILITY

Please read this document carefully before signing

I, __________________________________________________, desire to voluntarily participate in this unpaid internship without compensation in the department of__________________________, at Canisius College. Therefore, I hereby covenant with Canisius College that I shall not sue or bring any legal action or proceeding against Canisius College or its board of trustees, employees, agents, officers, faculty, students, or representatives on account of any injury or damage, including death, that I may sustain by virtue or arising out of my work as a volunteer and/or use of the equipment of Canisius College.

I acknowledge that my work as an unpaid intern and/or use of the equipment of Canisius College shall be at my sole risk and that Canisius College, its board of trustees, employees, agents, officers, faculty, students, or representatives shall not have any responsibility whatsoever with respect thereto.

I acknowledge that I have read this document carefully and that I fully understand and accept all provisions of the waiver.

I certify I am at least eighteen years of age and voluntarily sign this waiver.

Signature__________________________________________Date________________________

Witness_________________________________________Date________________________
**ADMISSION OF APPLICANTS WITH PRIOR HISTORY OF CRIMINAL BEHAVIOR OR DISCIPLINARY ACTION FOR CONDUCT**

**Effective Date:** May 6, 2019

**Policy Number:** V –

**Supersedes:**

**Issuing Authority:**

**Responsible Officer:**

**Applicability:** All persons enrolled or seeking admission to Canisius College.

**History:**

---

**PURPOSE**

The purpose of this policy is to protect the college community where admission of an applicant with a prior history of criminal behavior or disciplinary action for conduct may endanger the health, safety or welfare of others.

**POLICY**

It is the policy of Canisius College to reserve the right to deny or place conditions on admission, continued enrollment, or re-enrollment of applicants, students or former students whose personal history and background, including their criminal record, indicates that their presence at the college may endanger the health, safety, welfare, or property of members of the college community or interfere with the orderly and effective performance of the college's functions.

Applicants for admission to the college are required to disclose any prior criminal convictions or pending criminal charges, as well as any past disciplinary suspensions or dismissals from higher educational institutions on the application for enrollment. Additional review may be required for those applicants seeking admission to the following academic programs:

[LIST PROGRAMS THAT REQUIRE FORMAL SCREENING].

Prior criminal or disciplinary actions are not an automatic bar to admission to the college. The college recognizes that automatically depriving past offenders of an education may not be in the best interest of the individual, the educational mission of the college, or society at large. However, this recognition must be balanced against the college’s need to carefully evaluate and determine the possibility that admission or presence of the student on campus may endanger the health, safety, welfare, or property of members of the college community or interfere with the orderly and effective performance of the college's functions. In determining whether or not to admit the applicant based on the evidence, the [ADMISSIONS DEPARTMENT OR ADMISSIONS COMMITTEE] will adhere to the procedures and factors set forth in the Procedures/Guidelines section of this policy. While the [ADMISSIONS DEPARTMENT OR ADMISSIONS COMMITTEE] will exercise its judgment in a reasonable manner, the decision of the college as to whether or not to admit the applicant is in the college’s absolute and sole discretion.
Applicants who fail to give complete and accurate responses to the conduct section of the admission application may be subject to denial of admission, disciplinary action, invalidation of credits or degrees earned and rescission of admission upon discovery of the misstatement or omission.

All records, reports, and proceedings are considered private by the college and shared only as reasonably necessary for review of the applicant’s request for admission, subject to any applicable state or federal laws that may compel disclosure of all or part of such records.

The college reserves the right to deny admission to any applicant and to deny and/or rescind admission to any applicant consistent with college policies, including for applicants who provide false or misleading information to the college.

DEFINITIONS

Not Applicable.

PROCEDURES/GUIDELINES

I. Review Procedures

The [ADMISSIONS DEPARTMENT OR ADMISSIONS COMMITTEE] will review the information provided by the applicant and make a determination as to whether or not to offer admission to the applicant, assuming all other application requirements are satisfied.

Factors considered by the [ADMISSIONS DEPARTMENT OR ADMISSIONS COMMITTEE] as part of the past crime or disciplinary offense review process include, but are not limited to:

1. Amount of time that has passed since crime or offense;
2. Successful completion of sentence;
3. Severity of the crime or offense;
4. Nature of the crime or offense;
5. Other educational programs attended since time of crime or offense; and
6. Nature of the academic program in which the applicant seeks to enroll.

Admission may be denied to an applicant based on prior criminal convictions, including but not limited to in instances where admission creates a risk to the safety or welfare of the college community, to specific individuals or to the public, or where admission poses a potential risk to property.

After evaluating all information provided by the applicant as well as other information available to the [ADMISSIONS DEPARTMENT OR ADMISSIONS COMMITTEE], the [ADMISSIONS DEPARTMENT OR ADMISSIONS COMMITTEE] will make a determination as to whether or not the applicant will be eligible to enroll to the college. The applicant will be informed of the college’s decision in writing. Applicants who are denied admission by the college may appeal the determination in accordance with Section IV below.

II. Conditions Applicable to all Applicants Determined Eligible to Enroll

If the [ADMISSIONS DEPARTMENT OR ADMISSIONS COMMITTEE] decides the applicant is eligible to enroll, the following conditions apply to all applicants who enroll at the college:
1. The applicant must not be charged with any further crimes pursued by a prosecuting jurisdiction;
2. The applicant must complete all court ordered requirements (as applicable);
3. The applicant must meet with the Senior Associate Dean of Students, no later than one week prior to the academic semester, to discuss and comply with any additional conditions. Such condition may include, for example, the following:
   a. A probationary period for all or part of enrollment with or without stipulations;
   b. Participation in a drug and alcohol evaluation or counseling support; and
   c. Restriction on housing, activities, and/or employment on campus.

If an applicant fails to comply with these or any other admission conditions prior to enrollment, the college may revoke its prior determination and make the applicant not eligible to enroll. If the applicant fails to comply with admission conditions after enrollment, it is a potential violation of the Community Standards and the case will be referred to the Senior Associate Dean of Students.

III. Registered Sex Offenders

If the college determines a registered sex offender is eligible to enroll, the [ADMISSIONS DEPARTMENT OR ADMISSIONS COMMITTEE] will determine whether the applicant is eligible to reside in college housing. Such decision will be communicated to the student in writing. If an admitted sex offender is allowed to reside on campus, individual must comply with any and all registration requirements per state law, in addition to registering with the college’s Public Safety Department.

IV. Appeals

Applicants who are denied admission by the [ADMISSIONS DEPARTMENT OR ADMISSIONS COMMITTEE] may appeal this determination to the Vice President for Enrollment Management as follows:

1. An appeal must be submitted in writing to the Vice President for Enrollment Management within ten (10) days of receiving the [ADMISSIONS DEPARTMENT OR ADMISSIONS COMMITTEE]’s determination.
2. The appeal will be reviewed by the Vice President for Enrollment Management, additional potentially relevant information may be obtained, and a decision will be made within a reasonable amount of time given the individual circumstances.
3. The Vice President for Enrollment Management may consult with the Vice President for Student Affairs and other campus official as appropriate in reaching a determination.
4. The applicant will be informed of the outcome of the appeal in writing.
5. The Vice President for Enrollment Management’s decision is final and is not appealable.

RELATED POLICIES

Community Standards
NOTICE OF NONDISCRIMINATION POLICY

Canisius College does not discriminate on the basis of age, race, religion or creed, color, sex, national or ethnic origin, sexual orientation, marital status, military status, genetic information, predisposition or carrier status, gender identity or expression (including transgender status), familial status, domestic victim status, pregnancy (including childbirth and related medical conditions), citizen status, disability, or any other status protected by state or federal law in administration of its educational policies, employment practices, admissions policies, scholarship and loan programs, and athletic and other school administered programs.

Canisius admits students of any age, race, religion or creed, color, sex, national or ethnic origin, sexual orientation, marital status, military status, genetic information, predisposition or carrier status, gender identity or expression (including transgender status), familial status, domestic victim status, pregnancy (including childbirth and related medical conditions), citizen status, disability, or any other status protected by state or federal law to all rights, privileges, programs, and activities generally accorded or made available to students at the College.

It is also the policy of Canisius College to provide working and learning environments that are free from harassment based on any such status.

It also continues to be the policy of Canisius College to provide disabled persons with reasonable accommodations in employment, admissions and access to its programs and facilities in accordance with applicable laws.

REV 2-2019
PURPOSE

The purpose of this policy is to ensure that all official college websites include a link to the college’s Privacy Policy statement about the information that is collected by the page (both automatically and voluntarily), how that information is used by the college, and how the college complies with multiple regulations, including the European Union General Data Protection Regulation (“EU GDPR”).

POLICY

It is the policy of Canisius College that all college websites comply with regulations addressing privacy practices and inform online users of how information at that site is managed through the posting of a Privacy Policy statement. Accordingly, members of the college community responsible for maintaining a college website must ensure that each page of the website display a link to the college’s Privacy Policy (see https://www.canisius.edu/canisius-college-privacy-policy).

Note: The Institutional Review Board (IRB) is responsible for reviewing sites conducting web-based research. The IRB develops its own guidelines for the use of websites in research and applies those guidelines to research projects requiring IRB review.

DEFINITIONS

Member of the College Community—includes any person who is a student, faculty member, staff member, organization, club, group, team, alumni, volunteer, trustee, or any other person employed by the college. This definition also includes all college departments, offices and programs.

College Website—any website operated on (a) the college network, (b) by a college department, organization or program, or (c) using college resources, whether or not it is accessed through a www.canisius.edu address.

See also the Definitions and Legal References section of the Privacy Policy statement below.
Thank you for visiting our site. This statement discloses the privacy practices for the Canisius College website and any related offline print and electronic publications. By using our site or one of our offline print or electronic publications, you agree to the collection, use and disclosure of your personal data as described in this statement. If you do not agree to the terms of this statement, then please do not use the site or such publications. BY USING THIS SITE, YOU AGREE TO OUR COLLECTION, USE AND MAINTENANCE OF YOUR DATA OR PERSONAL DATA IN THE UNITED STATES. If you are visiting the site from a location outside of the United States, your connection will be through and to servers located in the United States. All personal data you provide will be processed and securely maintained in our web servers and internal systems located within the United States.

If you have any questions regarding this Privacy Policy, please send us an e-mail (info@canisius.edu). Contact us by mail at 2001 Main Street, Buffalo NY 14208-1517.

Please read this Privacy Policy carefully.

Definitions and interpretation
In this Privacy Policy, the following definitions are used:

Data or Personal Data
collectively all information that you submit to Canisius College via the Website that directly, indirectly, or in connection with other information — including a personal identification number — allows for the identification or identifiability of a natural person. This definition incorporates, where applicable, the definitions provided in the Data Protection Act 1998;

Data Subject
The natural person to whom the Personal Data refers;

Cookies
a small text file placed on your computer by this Website when you visit certain parts of the Website and/or when you use certain features of the Website. Details of the cookies used by this Website are set out in the clause below (Cookies);

UK and EU Cookie Law
the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011;

User or you
any third party that accesses the website (i.e., www.canisius.edu) who, unless otherwise specified, coincides with the Data Subject and is not either (i) employed by Canisius College and acting in the course of their employment or (ii) engaged as a consultant or
otherwise providing services to Canisius College and accessing the Website in connection with the provision of such services;

and

Usage Data

Information collected automatically through www.canisius.edu (or third-party services employed in www.canisius.edu), which can include: the IP addresses or domain names of the computers utilized by the Users who use ucumberlands.edu, the URI addresses (Uniform Resource Identifier), the time of the request, the method utilized to submit the request to the server, the size of the file received in response, the numerical code indicating the status of the server's answer (successful outcome, error, etc.), the country of origin, the features of the browser and the operating system utilized by the User, the various time details per visit (e.g., the time spent on each page within the Application) and the details about the path followed within the application with special reference to the sequence of pages visited, and other parameters about the device operating system and/or the User's IT environment.

Website

the website that you are currently using, canisius.edu, and any sub-domains of this site unless expressly excluded by their own terms and conditions.

Data Processor (or Data Supervisor)

The natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the college, as described in this privacy policy.

Data Controller (or Owner)

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, including the security measures concerning the operation and use of www.canisius.edu.

Service

The service provided by www.canisius.edu as described in the relative terms (if available) and on this site/application.

European Union (OR EU)

Unless otherwise specified, all references made within this document to the European Union include all current member states to the European Union and the European Economic Area.

Cookies

Small piece of data stored in the User's device.
Privacy Policy

Collection of Data

Among the types of Personal Data that ucumberlands.edu collects, by itself or through third parties, there are: cookies, usage data, first name, last name, gender, date of birth, phone number, company name, profession, address, fax number, country, state, province, email address, ZIP/Postal code, city, field of activity and user ID. Complete details on each type of personal data collected are provided below, in other dedicated sections of this policy, or by specific explanation texts displayed prior to the data collection. Personal data may be freely provided by the user, or, in case of usage data, collected automatically when using www.canisius.edu.

Unless specified otherwise, all data requested by www.canisius.edu is mandatory and failure to provide this data may make it impossible for www.canisius.edu to provide its services. In cases where www.canisius.edu specifically states that some data is not mandatory, users are free not to communicate this data without consequences to the availability or the functioning of the service. Users who are uncertain about which personal data is mandatory are welcome to contact the college or applicable owner.

Credit & Debit Card Data

We do not store credit card details nor do we share customer details with any 3rd parties.

Specific Examples of Data Collected:

Our online and offline registration forms require users to give us contact information including name, e-mail address and postal address. We may also collect your telephone number, and other data. We use this contact information to send you information about the specific solutions or services that match your interests.

We may also collect contact and other data from you if you: (1) participate in one of our contests or sweepstakes or apply for an offering from us; (2) order from us; (3) take part in one of our surveys; (4) contact us; or (5) otherwise voluntarily submit information to us, including in our online communities. You always have the ability to opt out of receiving future mailings and special offers; see the “Opt Out” section below.

If you use any of our tell-a-friend features, we ask for your friend’s name and e-mail address. We use this information only to send the communication you requested and to monitor the effectiveness of our tell-a-friend features. You are responsible for any third-party personal data obtained, published or shared through www.canisius.edu and confirm that you have the third party's consent to provide the data to the college.

As part of the standard operation of the site, we may collect certain non-personal data from you, including but not limited to your browser type, operating system, IP address and the domain name from which you accessed the site. In addition, we may collect data about your browsing behavior, such as the date and time you visit the site, the areas or pages of the site that you visit, the amount of time you spend viewing the site, the number of times you return to the site and other click-stream data. We do not combine this non-personal data with your personal data. We use this data to: (1) provide you with customized content and advertising; (2) administer the site, monitor its usage and diagnose problems with it; (3) remember you when you return to the site, so that you don’t have to re-submit information and preferences; and (4) conduct research to improve our
content and services. In addition, we use software that uses your IP address to determine roughly where you are located, so that we can deliver advertisements to you, while you are on the site, based on your location and therefore as relevant to you as possible. We use web beacons, which are tiny graphic images, in our e-mails. These help us measure the effectiveness of our e-mail campaigns, by telling us whether the messages have been received, opened or otherwise acted upon. We also work with a company that serves advertisements on our behalf. The company uses cookies, web beacons or similar technologies to collect anonymous information about your visits to the site and other websites, so that we may serve you advertisements that are relevant to your interests. Our ad serving company does not collect personal data about you, and we do not share any personal data with it. We will never share your IP address with a third party (except for our service providers) without first securing your express permission to do so.

Any use of cookies – or of other tracking tools – by www.canisius.edu or by the owners of third-party services used by the college serves the purpose of providing a service required by the user, in addition to any other purposes described in the cookie policy (see below).

All personal data is stored securely in accordance with the principles of the Data Protection Act 1998 and EU GDPR. For more details on security see the clause below (Security).

Methods of Processing Personal Data

The college takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of your data.

Data processing is carried out using computers and/or information technology enabled tools, following college procedures and modes strictly related to the purposes indicated. In addition to the college, in some cases, your data may be accessible to certain types of persons in charge, involved with the operation of www.canisius.edu (administrators, admissions, system administration) or external parties (such as third-party technical service providers, mail carriers, hosting providers, information technology companies, communications agencies) appointed, if necessary, as data processors by the college. You may request an updated list of these parties from the college at any time.

Legal Basis of Processing Personal Data

The college may process your data if one of the following applies:

1. You have given consent for one or more specific purposes. Note: Under some legislations the college may be allowed to process your data until you object to such processing (“opt-out”), without having to rely on consent or any other of the following legal bases. This, however, does not apply, whenever the processing of Personal Data is subject to European data protection law;

2. Provision of your data is necessary for the performance of an agreement with you and/or for any pre-contractual obligations thereof;

3. Processing is necessary for compliance with a legal obligation to which the college is subject;

4. Processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in the college;
5. Processing is necessary for the purposes of the legitimate interests pursued by college or by a third party.

There will be some instances where the collection and processing of your personal data will be pursuant to other lawful bases. In any case, the college will help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of your data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

We do not collect your personal data through our website and other platforms, unless it is voluntarily provided by you. In such instances, we will never sell or trade the personal data you provide to us, unless we have your consent in doing so, or if the data is needed for legal processes.

Note: As GDPR is a new law, the conditions identified above may be subject to change as more guidance is given or precedents are set.

**Place of Processing**

Your data is processed at the college's operating offices and in any other places where the parties involved in the processing are located.

Depending on your location, data transfers may involve transferring your data to a country other than your own.

You are also entitled to learn about the legal basis of data transfers to a country outside the European Union or to any international organization governed by public international law or set up by two or more countries, such as the UN, and about the security measures taken by the college to safeguard its data.

If any such transfer takes place, you may find out more by checking the relevant sections of this policy or inquire with the college using the information provided in the contact section.

**Retention Time**

The college keeps the personal data it collects in accordance with the retention periods of applicable federal law and the college’s Record Retention Schedule. Your data will be destroyed upon your request unless applicable law requires destruction after the expiration of an applicable retention period. The manner of destruction shall be appropriate to preserve and ensure the confidentiality of your data given the level of sensitivity, value and criticality to the college.

**Cookies**

1. This Website may place and access certain Cookies on your computer. Canisius College uses Cookies to improve your experience of using the Website and to improve our range of products and services. Canisius College has carefully chosen these Cookies and has taken steps to ensure that your privacy is protected and respected at all times.

2. All Cookies used by this Website are used in accordance with current US, UK, and EU Cookie Law.

3. Before the Website places Cookies on your computer, you will be presented with a message bar requesting your consent to set those Cookies. By giving your consent to the placing of Cookies, you are enabling Canisius College to provide a better experience and service to you. You may, if you wish, deny consent to the placing of Cookies; however certain features of the Website may not function fully or as intended.
4. This website may place the following Cookies:
   a. Strictly necessary cookies: These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website, use a shopping cart or make use of e-billing services.

5. Disabling and Deleting Cookies
   a. You can choose to enable or disable Cookies in your internet browser. By default, most internet browsers accept Cookies, but this can be changed. For further details, please consult the help menu in your internet browser.
   b. You can choose to delete Cookies at any time; however, you may lose any information that enables you to access the Website more quickly and efficiently including, but not limited to, personalization settings.
   c. It is recommended that you ensure that your internet browser is up-to-date and that you consult the help and guidance provided by the developer of your internet browser if you are unsure about adjusting your privacy settings.

**Information Use**

For purposes of the Data Protection Act 1998, Canisius College is the “data controller”. We will retain any data you submit for 12 months.

We may use the data we collect from and about you for any of the following purposes:

1. To fulfill your requests for products and services;
2. To provide you with targeted offers, site content and advertising on the site;
3. To contact you with information and promotional materials and offers from the college, as well as from our affiliates, other related companies, educational institutions, marketing partners and other third parties, if you have agreed to receive such communications;
4. To contact you when necessary;
5. To review site and product usage and operations;
6. To address problems with the site, our business or our products and services; and
7. To protect the security or integrity of the site and our business.

You may find further detailed information about such purposes of processing and about the specific personal data used for each purpose in the respective sections of this policy.

**Information Disclosure**

In addition to disclosing your information to our partners, with your consent, as described above, we may disclose the information collected from and about you as follows:

1. To our affiliated companies, with your consent;
2. To our service providers, who may use it only on our behalf;
3. As necessary, if we believe that there has been a violation of our site Terms of Use or of our rights or the rights of any third party;
4. To respond to judicial process and provide information to law enforcement agencies or in connection with an investigation on matters related to public safety, as permitted by law, or otherwise as required by law; and

5. As disclosed to you at the point of collection. In addition, if the college or substantially all of its assets are acquired, your personal data may be one of the transferred assets.

Any personal data or content that you voluntarily upload or submit for posting to a site (including your name and information in your blogs, a site community, bios, videos and comments) becomes publicly available and can be collected and used by others. It may also be available to third party search engines.

It is in violation of the site’s Terms of Use for you to post any content that requests personally identifiable information. We may share aggregate, non-personally identifiable information about you with third parties for research and other purposes.

We may disclose your personal data as follows:

1. **Consent**: We may disclose your personal data if we have your consent to do so.

2. **Emergency Circumstances**: We may share your personal data when necessary to protect your interests and you are physically or legally incapable of providing consent.

3. **Employment Necessity**: We may share your personal data when necessary for administering employment or social security benefits in accordance with applicable law, subject to the imposition of appropriate safeguards to prevent further unauthorized disclosure.

4. **Charitable Organizations**: We may share your personal data with applicable college foundations and other not-for-profit organizations in connection with charitable giving subject to the imposition of appropriate safeguards to prevent further unauthorized disclosure.

5. **Public Information**: We may share your personal data if you have manifestly made it public.

6. **Archiving**: We may share your personal data for archiving purposes in the public interest, and for historical research, and statistical purposes.

7. **Performance of a Contract**: We may share your personal data when necessary to administer a contract you have with the college.

8. **Legal Obligation**: We may share your personal data when the disclosure is required or permitted by international, federal, and state laws and regulations.

9. **Service Providers**: We use third parties who have entered into a contract with the college to support the administration of college operations and policies. In such cases, we share your personal data with such third parties subject to the imposition of appropriate safeguards to prevent further unauthorized disclosure.

10. **College Affiliated Programs**: We may share your personal data with parties that are affiliated with the college for the purpose of contacting you about goods, services, charitable giving, or experiences that may be of interest to you.
11. **De-Identified and Aggregate Information:** We may use and disclose your personal data in de-identified or aggregate form without limitation.

If your personal data is transferred to third party service providers, we will take steps to ensure that your personal data receives the same level of protection as if it remained within the EU, including by entering into data transfer agreements or by relying on certification schemes. You have a right to obtain details of the mechanism under which your personal data is transferred outside of the EU by contacting info@canisius.edu. Moreover, we contractually require agents, service providers, and affiliates who may process your personal data to provide the same level of protections for personal data as required by the college.

**Your Rights**

Pursuant to the GDPR, you have the following rights:

1. To be notified if we intend to transfer your personal data to another country or international organization and the identity of the recipients of your personal data;
2. To be notified of the period your personal data will be stored;
3. To access and require us to correct the personal data we hold about you if it is incorrect;
4. To require us to erase your personal data subject to the retention periods of applicable federal law and the college's Record Retention Schedule;
5. To require us to restrict our data processing activities and, where our processing is based on your consent, you may withdraw that consent, without affecting the lawfulness of our processing based on consent before its withdrawal;
6. To receive from us the personal data we hold about you which you have provided to us, in a reasonable format specified by you, including for the purpose of you transmitting that personal data to another data controller;
7. To object, on grounds relating to your particular situation, to any of our particular processing activities where you feel this has a disproportionate impact on your rights;
8. To be notified of the existence of any automated decision-making regarding the use of your personal data, including meaningful information about the logic involved and its significance and consequences of such processing;
9. To be notified if the collected personal data will be further processed for a purpose other than that for which it was collected;
10. To file a complaint with the appropriate supervisory authority in the European Union if you feel we have not complied with applicable foreign laws regulating information created in the European Union that is transferred out of the European Union to the college.

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply.

**Opt Out**

Users who have opted in through our online and offline registration forms can opt out of receiving future communications from us. Users may also request removal directly from our partners at any time in the future. We make every effort to honor their request; however, we expressly disclaim responsibility for the actions of partners or other third parties beyond our control. To remove
information from our database, users can send us an e-mail (info@canisius.edu) or contact us by
mail at 2001 Main Street, Buffalo NY 14208-1517. You may also use the opt-out mechanism that
is contained in each email.

Access
You have the right to ask for a copy of any of your personal data held by Canisius College.
To access, correct or request that we make no further use of your personal data, please send us an
e-mail info@canisius.edu or contact us by mail at 2001 Main Street, Buffalo NY 14208-1517.

Controlling use of your Personal Data
Wherever you are required to submit personal data, you will be given options to restrict our use of
that data. This may include the following:

1. Use of personal data for direct marketing purposes; and
2. Sharing personal data with third parties.

Functionality of the Website

1. To use all features and functions available on the website, you may be required to submit
certain Data.
2. You may restrict your internet browser’s use of Cookies. For more information see the
Cookies clause.

Third party websites and services
Canisius College may, from time to time, employ the services of other parties for dealing with
certain processes necessary for the operation of the Website. The providers of such services have
access to certain personal data provided by Users of this Website.

Any data used by such parties is used only to the extent required by them to perform the services
that we request. Any use for other purposes is strictly prohibited. Furthermore, any Data that is
processed by third parties will be processed within the terms of this privacy policy and in
accordance with the Data Protection Act 1998 and GPDR.

Links to other websites
This Website may, from time to time, provide links to other websites. We have no control over
such websites and are not responsible for the content of these websites. This privacy policy does
not extend to your use of such websites. You are advised to read the privacy policy or statement
of other websites prior to using them.

Changes of Business Ownership and Control
Canisius College may, from time to time, expand or reduce our business and this may involve the
sale and/or the transfer of control of all or part of Canisius College. Data provided by you will,
where it is relevant to any part of our business so transferred, be transferred along with that part
and the new owner or newly controlling party will, under the terms of this privacy policy, be
permitted to use the data for the purposes for which it was originally supplied to us.

We may also disclose data to a prospective purchaser of our business or any part of it.
In the above instances, we will take steps with the aim of ensuring your privacy is protected.
Security

Canisius College has taken certain physical, electronic, contractual and managerial steps to safeguard and secure your personal data. It is your responsibility to maintain the confidentiality of your site account information, including your password, and you are responsible for all use of the site accessed through it. You agree to notify us immediately of any unauthorized use of your account or any other actual or suspected breach of site security. You may report suspected violations to the Webmaster at the address listed below.

Children

We do not direct the site to, nor do we knowingly collect any personal information from, children under thirteen.

General

1. You may not transfer any of your rights under this privacy policy to any other person. We may transfer our rights under this privacy policy where we reasonably believe your rights will not be affected.

2. If any court or competent authority finds that any provision of this privacy policy (or part of any provision) is invalid, illegal or unenforceable, that provision or part-provision will, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of this privacy policy will not be affected.

3. Unless otherwise agreed, no delay, act or omission by a party in exercising any right or remedy will be deemed a waiver of that, or any other, right or remedy.

4. This privacy policy is governed by and interpreted according to the laws of the United States of America. All disputes arising under this privacy policy are subject to the jurisdiction of the courts of the United States of America.

Changes to this Privacy Policy Statement

Please note that we review our privacy policy from time to time, and that our practices are subject to change. We ask that you bookmark and periodically review this page to ensure continuing familiarity with the most current version of our privacy policy. All amended terms shall be automatically effective after they are posted on the site and applied retroactively if you use the site after this policy is amended.

Your Acceptance of These Terms

By using this website, you signify your acceptance of this privacy policy. If you do not agree to this statement, please do not use our website. Your continued use of the website following the posting of changes to this statement will be deemed your acceptance of those changes.

Contact Us

If you have any questions about this privacy policy statement, the practices of the website, or dealings with the website or with us, contact:

Canisius College
2001 Main Street, Buffalo NY 14208-1517
Phone: (716) 883-7000
info@canisius.edu
RELATED POLICIES

Not Applicable.
AUDIT AND ACCOUNTABILITY CONTROL POLICY

Effective Date: May 6, 2019
Policy Number:
Supersedes: Not Applicable
Issuing Authority: President
Responsible Officer: Chief Information Officer
Applicability: All College Information Systems that collect, process, maintain, use, share, disseminate or dispose of College Data (“applicable information system(s)”), as well as all Authorized Users who access, use, or handle those resources.
History:

PURPOSE

The purpose of this policy is to adapt and maintain a formal documented program for the monitoring, management, and review of applicable information systems and associated Authorized User activity.

POLICY

It is the policy of Canisius College to configure applicable information systems to produce, store, and retain audit records for the specific resource and Authorized User activity.

Under the leadership of the chief information officer, applicable resources are routinely reviewed to determine if such resources provide the necessary means whereby the Information Technology Services (“ITS”) may audit and establish individual accountability for any auditable event that can potentially cause access to, generation of, modification of, or affect the release of Private College Data.

DEFINITIONS

Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

Audit Event—any observable occurrence within a College Information System that is significant and relevant to the security of the system and the environment in which it operates in order to meet specific and ongoing audit needs. Audit events include any auditable event required by applicable local, state, and federal laws. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, etc.

College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.
*College Information System*—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

*Covered Data and Information*—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.

*Data Custodians*—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

*Data Owners*—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

*Members of the College Community*—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

*Mobile Device*—any handheld or portable computing device including running an operating system optimized or designed for mobile computing. Any device running a full desktop version operating system is not included in this definition.

*Non-Public Personal Information*—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

*Personally Identifiable Information or PII*—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

*Private College Data*—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to this policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive
Research Data, Protected Health Information, and Sensitive Authentication Data. See the College Data Classification Policy for additional information.

Public College Data—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

Security Incident—occurs when there is a serious threat of or unauthorized access or acquisition to a College Information System or an Authorized User’s computerized data that compromises the security, confidentiality, or integrity of the data, including Private College Data. A Security Incident also occurs where there has been unauthorized access or acquisition of encrypted data and the confidential process or key to the encryption is also compromised. Security Incidents can range from the unauthorized use of another Authorized User’s account or system privileges to the execution of malicious code, viruses, worms, Trojan horses, cracking utilities, or attacks by crackers or hackers. Security Incidents may also involve the physical theft of a college information system, a component thereof, or an Authorized User’s technology, such as a computer, mobile device, or other electronic media, or may occur as the result of a weakness in information systems or components (e.g., hardware design or system security procedures).

A non-exhaustive list of symptoms of incidents that qualify as Security Incidents include:

- A system alarm or similar indication from an intrusion detection tool;
- Suspicious entries in a system or network accounting;
- Accounting discrepancies; unexplained new user accounts or file names;
- Unexplained modification or deletion of data; system crashes or poor system performance;
- Unusual time of usage; and
- Unusual usage patterns.

Sensitive Authentication Data—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks).

Student Education Records—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

Student Financial Information—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

PROCEDURES/GUIDELINES
I. Auditable Events

Information systems designated by ITS as requiring authentication are configured to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact Security Incident investigations.

When resources or technology allows, ITS will configure applicable resources to audit the following additional events:

1. Authorized User identification;
2. Type of event;
3. Date;
4. Timestamp;
5. Logon/logoff;
6. Identity or name of resource/data/system component;
7. All system and data interactions concerning Private College Data, including failed access attempts for operating systems, databases, devices, and applications that collect, process, maintain, use, share, disseminate, or dispose of Private College Data;
8. Administrative access functions, including changes in the status of auditable events;
9. Creation of new accounts and elevation of privileges; and
10. All changes, additions, or deletions to accounts with root or administrative privileges.
11. Change of password;
12. Switching accounts or running administrator access functions from another account;
13. Subset of security administrator commands while logged on in an administrator access role;
14. Subset of system administrator commands while logged on in the Authorized User role;
15. Access to all audit functions;
16. Clearing of the audit log file;
17. Startup, pausing, and shutdown of audit functions;
18. Change of file or Authorized User permissions or privileges;
19. Remote access outside of college network communications channels (e.g., dedicated virtual private network) and all dial-in access to the system;
20. Changes made to an application or database by a batch file;
21. Application critical record changes;
22. Creation and deletion of system-level objects;
23. Changes to database or application records, where the application is bypassed to produce the change (via a file or other database utility); and
24. Additional platform specific events may also be required, based on the outcome of the risk assessment required by the Risk Assessment and Security Policy.
A. Auditable Events Review

Auditable events and review frequencies are documented by ITS. The documentation is evaluated on an annual basis by the chief information officer (or his/her designee) and updates to the audit and accountability program are introduced as necessary.

B. Changes by Authorized Individuals

Only authorized personnel designated by the chief information officer (or his/her designee) are permitted to make changes to the audit system. Changes to the audit system may include adjustments to capture more or less information to comply with investigation requirements, as well as modifications that would facilitate audit reduction, analysis, and reporting.

II. Content of Audit Records

As noted above, applicable information systems designated by ITS as requiring authentication must have the capability to create audit records. ITS is responsible for ensuring that such records contain sufficient information to, at a minimum establish what events occurred, when (date and time) the events occurred, the source of the events, the source of the event, the identity of any user associated with the event, and the event outcome.

Applicable resources may also include additional defined requirements in the audit records for audit events identified by type, location, or subject. An example of detailed information that the college may require in audit records is full-text recording of privileged commands or the individual identities of group account users.

ITS centrally manages the content of audit records, including those records generated by all web servers, database servers, messaging servers, file servers, print servers, middleware servers, DNS servers, routers, firewalls, IDS/IPS, and VoIP servers. Such records are maintained in accordance with the Record Retention Policy and Schedule.

The following information is never included in the audit records maintained by ITS:

1. Unencrypted Private College Data;
2. Session identification values (consider replacing with a hashed value if needed to track session specific events);
3. Access tokens (except nonce URLs that grant limited, specific purpose access);
4. Clear text authentication credentials (e.g., passwords);
5. Database connection strings;
6. Encryption keys; and
7. Information it is illegal to collect in the relevant jurisdiction.

III. Audit Storage Capacity

ITS is responsible for ensuring that applicable information systems requiring authentication have a sufficient amount of storage capacity allocated for audit records. ITS configures such systems to:

1. Reduce the likelihood of audit records exceeding storage capacity; and
2. Allow the records to be maintained for a period as designated by ITS.
When possible, ITS will off-load audit records onto a different information system than the one that is being audited to preserve the confidentiality and integrity of the audit records.

IV. Response to Audit Processing Failures

When possible, applicable information systems requiring authentication shall provide the capability to generate system alerts and send them to appropriate ITS staff in the event of an audit failure or audit storage capacity being reached. In the event of an audit processing failure, when possible, the system will be configured by ITS to shut down or provide limited functionality. ITS will then attempt to remediate logging discrepancies.

V. Audit Review, Analysis and Reporting Authority

Audit records are regularly reviewed and analyzed by ITS staff to identify unauthorized, inappropriate, unusual, suspicious activity, or other Security Incidents (see the Incident Response Policy). Such activities are investigated by ITS staff and reported to the chief information officer, in accordance with the Incident Response Policy.

A. Frequency of Review and Analysis

Assigned ITS staff review audit records for applicable resources and associated components to identify anomalies or suspicious activity as follows:

1. The following audit records are reviewed by ITS at least daily:
   a. All security events;
   b. Logs of all system components that store, process, or that could impact the security of Private College Data.;
   c. Logs of all critical system components; and
   d. Logs of all servers and system components that perform security functions. As applicable, this includes, but is not limited to:
      i. Firewalls;
      ii. Intrusion Detection Systems (IDS);
      iii. Intrusion Prevention Systems (IPS);
      iv. Authentication servers (e.g., Active Directory domain controllers); and
      v. E-commerce redirection servers;

2. ITS staff reviews other audit records in accordance with the annual risk assessment (see the Risk Assessment and Security Policy); and

3. ITS staff report exceptions and anomalies identified during the review process to the chief information officer (or his/her designee) and follow up as appropriate.

B. Risk Escalation

If there is an increased risk to operating systems, databases or applications, review and analysis will be performed more frequently. See the Risk Assessment and Security Policy.

C. Integrate Alert Processes
Audit review, analysis, and reporting processes are integrated to support investigations and subsequent responses to suspicious activities.

D. Correlate Audit Repositories

Audit records are analyzed and correlated across different repositories by ITS to gain organizational situational awareness.

VI. Time Stamps

ITS is responsible for ensuring that applicable information systems are configured to use internal system clocks to generate time stamps for audit records. Time stamps generated by the system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

Data Owners must ensure that the time stamps on applicable resources they are responsible for are configured properly and validate the following:

1. The applicable resource is configured to synchronize time with college servers;
2. The applicable resource has the correct and consistent time; and
3. Time data is protected from unauthorized modification.

VII. Audit Information Protection

Audit records are protected from unauthorized modification, access, or deletion while online and during offline storage as follows:

1. Only authorized Data Owners and Custodians with administrative access credentials, as well as select staff from ITS are permitted access to audit logs and audit tools;
2. Audit logs containing Private College Data are encrypted in accordance with the System and Communications Protection Policy;
3. Audit files are protected from unauthorized modifications via the use of Login ID and authentication;
4. ITS is responsible for ensuring that applicable resources are configured to either allow real-time backup or audit the transfer of trail files to a centralized log server or media that is difficult to alter;
5. ITS is responsible for ensuring that applicable resources are configured to write logs for external-facing technologies onto a secure, centralized, internal log server or media devices; and
6. Where feasible, ITS implements File Integrity Monitoring (FIM) or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.

VIII. Audit Record Retention

The college retains audit records for a time sufficient to provide support after-the-fact security investigations as determined by the chief information officer (or his/her designee) and to meet regulatory and applicable college record retention requirements as delineated in the Record Retention Policy and Schedule.
IX. Exception Requests

For details on requesting an exception request to this Policy, please contact the chief information officer.

RELATED POLICIES

Access Control Policy
Acquisition and Disposal Policy
Configuration Management Policy
Data Classification Policy
Incident Response Policy
Information Security Program
Information Technology Configuration Management Policy
Media Protection Policy
Passwords Policy
Payment Card Security Policy
Record Retention Policy
Risk and Security Assessment Policy
System and Communication Protection Policy
System and Information Integrity Policy
PURPOSE
The purpose of this policy is to establish baseline configurations for applicable information systems based on the overall needs of the college, as well as to define the need for asset management and change management, which are necessary parts of configuration management.

POLICY
It is the policy of Canisius College to protect the integrity, availability, and security of applicable information systems by adopting standard baseline configuration management practices.

DEFINITIONS

Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

College Information System—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.
**Data Custodians**—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

**Data Owners**—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

**Members of the College Community**—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

**Mobile Device**—any handheld or portable computing device including running an operating system optimized or designed for mobile computing. Any device running a full desktop version operating system is not included in this definition.

**Non-Public Personal Information**—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

** Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to this policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, and Sensitive Authentication Data. See the College Data Classification Policy for additional information.

**Public College Data**—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

**Sensitive Authentication Data**—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

**Student Education Records**—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in
handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

**PROCEDURES/GUIDELINES**

I. **Baseline Configurations**

All applicable information systems at Canisius College shall have a formal, documented baseline configuration. This configuration is maintained by Information Technology Services (“ITS”).

Baseline configurations at the college include, at the minimum, the following:

1. System components, such as standard software packages installed for workstations, servers, college-owned or leased Mobile Devices, etc.;
2. Current version numbers of operating systems and software applications;
3. Current patch information;
4. Configuration settings and parameters;
5. College Network topology; and
6. Placement of hardware within the applicable information system architecture.

A. **ITS Responsibilities**

In establishing baseline configurations, ITS:

1. Identifies, documents, and applies more restrictive security configurations information systems that store or permit access to Private College Data, as necessary;
2. Maintains records that document the application of baseline security configurations;
3. Monitors systems for security baselines and policy compliance;
4. Reviews and revises all security configuration standards annually, or more frequently, as needed;
5. Reapplies all security configurations to systems, as appropriate, when the system undergoes a material change, such as an operating system upgrade;
6. Modifies individual system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning;

7. Requires creation and periodic review of a list of hardware and software assets;

8. Reviews and updates the baseline configuration of all information system:
   a. Once a year at a minimum;
   b. When required due to a significant configuration change or a demonstrated vulnerability; and
   c. As an integral part of information system component installations and upgrades;

9. Develops and maintains a college-defined list of software programs authorized to execute on the information system;

10. Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system; and

11. Maintains a baseline configuration for development and test environments that are managed separately from the operational baseline configuration.

B. Record Retention

Previous baseline configurations shall be retained by ITS in accordance with college record retention requirements.

C. Baseline Exceptions

For exceptions to a baseline configuration, please contact the director of user services for desktop and mobile devices, or the director of infrastructure for servers and network infrastructure.

II. Configuration Change Control

ITS staff coordinates and the chief information officer approves configuration change control activities. Data Owners and Custodians must obtain approval prior to implementation of changes that affect security on a college information system.

ITS documents and implements configuration management so that changes to an information system environment does not compromise security controls. Specifically, ITS:

1. Determines the types of changes to the information system that are configuration controlled;

2. Obtains approval from the chief information officer (or designee) for all configuration-controlled changes to the system with explicit consideration for security impact analyses (see Section III below);

3. Documents approved configuration-controlled changes to the system;

4. Tests and validates changes to the information system before implementing the changes on the system. In conducting tests, ITS:
   a. Utilizes separate environments for development/testing/staging and production;
   b. Utilizes a separation of duties between development/testing/staging and production environments;
c. Removes test data and accounts before production systems become active / goes into production.

5. Documents changes to the information system as follows:
   a. The impact of the change;
   b. The administrator(s) who approved the change;
   c. The results of functionality testing; and

6. In situations where the college cannot conduct testing of an operational system, the college employs compensating controls (e.g., providing a replicated system to conduct testing).

7. Retains and reviews records of configuration-controlled changes to the system: and

8. Audits activities associated with configuration-controlled changes to the system.

III. Security Impact Analysis

ITS analyzes changes to the information system to determine potential security impacts prior to change implementation. Security impact analyses are conducted by ITS staff with information security responsibilities. Personnel conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications.

Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system.

IV. Access Restrictions

Access restrictions for configuration change assist in preventing any unauthorized changes to the hardware, software, and/or firmware components of the information system and reduce the potential for significant effects on the overall security of the system.

Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized ITS staff are permitted to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the college become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries.

Examples of access restrictions include, for example, physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Some or all of the enforcement mechanisms and processes necessary to
implement this security control are included in other control policies (i.e., Access Control and Audit and Accountability policies). For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes.

V. Configuration Settings

Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections.

ITS:

1. Establishes and documents mandatory configuration settings for information technology products employed within the information system;

2. Changes vendor default passwords and other vendor default settings prior to system implementation in order to prevent a system from being compromised by malicious individuals making use of standard configuration parameters;

3. Implements configuration settings;

4. Identifies, documents, and receives approval from chief information officer for all exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and

5. Monitors and controls changes to the configuration settings.
   a. As required, ITS will assess the as-built configurations of all servers and network components against the configuration database and investigate and resolve any discrepancies;
   b. This monitoring can be accomplished either manually or using software tools specifically for this purpose; and
   c. Firewall and router rule sets are be reviewed on a regular basis.

See the System and Communications Protection Policy for applicable configuration setting requirements.

VI. Component Inventory

An accurate and frequently updated inventory of information system components is vital to maintain the integrity and security of the information system. Accordingly, ITS develops, documents, and maintains a current inventory of each information system's components and relevant ownership information. The inventory is available for review and audit.

VII. Exception Requests

For details on requesting a Configuration Management Policy exception request, please contact the chief information officer.

RELATED POLICIES

Access Control Policy
Acquisition and Disposal Policy
Audit and Accountability Control Policy
Cloud Computing Policy
Confidential Information Policy
Configuration Management Policy
Conflict of Interest and Commitment
Identification and Authentication Policy
Information Security Program
Information Technology Change Control Policy
Information Technology Personnel Security Policy
Information Technology Physical and Environmental Protection Policy
Information Technology Security Awareness and Training Policy
Media Protection Policy
Mobile Device Use and Support Policy
Password Policy
PURPOSE

The purpose of this policy is to implement appropriate safeguards to ensure Authorized Users granted access to College Information Systems and Private College Data have been properly vetted.

POLICY

It is the policy of Canisius College to limit access to College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data (“information systems”) to Authorized Users that are trustworthy and meet established security criteria and to ensure that such information systems are protected during and after personnel actions such as terminations and transfers.

DEFINITIONS

Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

College Information System—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and
electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

Data Custodians—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

Data Owners—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

Members of the College Community—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

Non-Public Personal Information—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

Personally Identifiable Information or PII—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

Private College Data—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the College Data Classification Policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, Cardholder Data, and Sensitive Authentication Data. See the Data Classification Policy for additional information.

Public College Data—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

Sensitive Authentication Data—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

Student Education Records—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that
contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

**PROCEDURES/GUIDELINES**

**I. Personnel Screening**

Prior to Information Technology Services (“ITS”) granting access authorization via a unique Login ID to an information service to an Authorized User, the individual must be screened in accordance with the following procedures:

1. In accordance with the Background, Reference, and Verification Screen Policy, screens of new employees working in areas that regularly work with Private College Data are conducted by Human Resources prior to the Data Owner and supervisor authorizing ITS to issue a unique login ID to the information service;

2. If the Data Owner and supervisor agree that the individual has a favorably adjudicated background screen commensurate with the defined position sensitivity levels, a request for access will be submitted electronically by the supervisor to bannersecurity@canisius.edu;

   a. ITS then creates the login ID and assigns the level of access to the new Authorized User. Only the requested and approved access that is specific to an Authorized User’s responsibilities will be granted by ITS;

   b. ITS will maintain a list of all information systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data for each unit, as well as unit personnel granted access to those resources;

3. The Authorized User’s supervisor will advise the Authorized User to follow all terms of use, including applicable college policies and associated controls; and

4. The new Authorized User will receive appropriate training to comply with all terms of use and policies and controls associated with the resource.

Note: Individuals must be rescreened if the length of employment separation exceeds 90 days.

**II. Employee Termination**

Upon termination of individual employment:
1. Access to an information system will be removed by ITS immediately upon termination of employment or, in the case of a vendor or other third-party, cessation of the individual’s engagement with the college.
   a. In the event that the access privilege is to remain active after a voluntary termination (e.g., extended electronic mail access), the supervisor must document that a need or benefit to the college exists;
2. All security-related property will be retrieved by the user’s supervisor (e.g., hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes);
3. Prior to archiving or permanent disabling the individual’s account, the user’s supervisor will ensure that all Private College Data is transferred to appropriate personnel or archived; and
4. ITS will confirm that the following activities have been performed upon termination of employment or, in the case of a vendor or other third-party, cessation of the individual’s engagement with the college:
   a. Lock the computer accounts and access control and after a specified time period delete them.
   b. Update access control lists, mailing lists, etc.;
   c. Collection of all keys/access cards, badges, and similar items; and
   d. Electronic data records are accessible and properly secured, filed, or appropriately disposed.

III. Employee Transfer
Access authorizations are modified appropriately by ITS as an Authorized User’s job responsibilities change due to a transfer as follows:
1. Access authorizations to information services are reviewed by the appropriate Data Owner and supervisor when Authorized Users are reassigned or transferred to other positions within the college.
   a. The actions undertaken are driven by the individual’s new position duties in accordance with the Access Control Policy;
2. ITS, upon being notified of the transfer by the Authorized User’s new supervisor or Human resources, performs the following activities for all Authorized Users, including third-party contractors, upon employee reassignment or transfer:
   a. Locks all Login ID’s;
   b. Updates access control lists;
   c. Confirms that electronic data records are accessible and properly secured, filed, or appropriately disposed;
   d. Closes previous information system accounts unless the original Data Owner and the new Data Owner carefully review the account to ensure that no resources or
access privileges are left on the account and the account has only the resources and
privileges appropriate to the person’s new role and responsibilities;
e. Updates the Authorized User’s access privileges;
f. Reviews and updates the individual’s access privileges and authorizations to ensure
alignment with the new position on the effective date; and

3. The employee’s former supervisor, in collaboration with Human Resources, is responsible
for:
a. The collection old keys/access cards, identification cards, authentication tokens,
etc., as appropriate; and
b. As appropriate, confirming that new keys/access cards, identification cards,
authentication tokens, etc. have been issued.

4. The above is initiated immediately upon being notified of the formal transfer action.

IV. Name Changes and Permission Changes

It is the responsibility of the supervisor to notify ITS whenever an Authorized User account must
be modified to accommodate name changes or permission changes. In the event of permission
changes, the procedures set forth in Section III above will be followed.

V. Third-Party Contractors

Third-Party contractors and vendors providing services to the college must possess the same level
of security clearance as a college employee to access the same information system or College Data.
The applicable vice president or supervisor overseeing the contract is responsible for making sure all current and future contracts include personnel security requirements.

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
Cloud Computing Policy
Data Classification Policy
Identification and Authentication Policy
Information Security Program
Information Technology Personnel Security Policy
Information Technology Security Awareness and Training Policy
Health Insurance Portability and Accountability Act Policy
Mobile Device Use and Support Policy
Password Policy
Payment Card Information Security Policy
Physical and Environmental Protection Policy
Record Retention Policy and Schedule
DATA CLASSIFICATION POLICY

Effective Date: May 6, 2019

Policy Number: Not Applicable

Issuing Authority: President

Responsible Officer: Chief Information Officer

Applicability: All College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data (“applicable information system(s)”), as well as all Authorized Users who access, use, or handle those resources.

PURPOSE

The purpose of this policy is to provide a framework for classifying College Data based on its level of sensitivity, value, regulatory requirements, and criticality to the college. Classification of data will aid in determining baseline security policies and corresponding controls for the protection of College Data.

POLICY

It is the policy of Canisius College to maintain College Data in a secure, accurate, and reliable manner and to make it readily available for authorized use. Data security controls at the college are implemented commensurate with data value, sensitivity, and risk.

Members of the college community designated as Data Owners are responsible for evaluating and classifying College Data for which they are responsible according to the classification system adopted by the college and described below. If College Data of more than one level of classification exists in the same collection of data, such data must be classified at the highest level of classification. Data Owners must communicate the data security classifications and associated security controls to Data Custodians and Authorized Users granted administrative access to such data.

Data Custodians and Authorized Users must (i) understand the college’s data classifications; (ii) consider how these classifications apply to College Data under their control; (iii) implement the security controls for each classification as specified by applicable college and departmental policies; and (iv) consult with the applicable Data Owner or Information Technology Services (“ITS”) regarding circumstances that may warrant the application of higher security standards.

DEFINITIONS

Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.
**College Data**—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

**College Employees**—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

**College Information System**—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

**Covered Data and Information**—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.

**Data Custodians**—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

**Data Owners**—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

**Members of the College Community**—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

**Non-Public Personal Information**—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to this policy. By definition, Private College Data includes, but is not limited
to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, and Sensitive Authentication Data. See the College Data Classification Policy for additional information.

Public College Data—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

Sensitive Authentication Data—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

Student Education Records—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

Student Financial Information—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

PROCEDURES/GUIDELINES

I. Data Classification Categories

Data classification, in the context of data security, is the classification of data based on its level of sensitivity and the impact to the college should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All College Data must be classified into one of three sensitivity levels, or classifications:

A Private-Highly Restricted

Private-Highly Restricted College Data is College Data that is not Public and is available within the college only to those with a legitimate need to know and are so highly sensitive that the loss of confidentiality of the data could either (a) cause significant personal, college, or other harm or (b) a law, regulation or contract require a high degree of security.

Examples of Private-Highly Restricted College Data include, but is not limited to:

1. Personally Identifiable Information or PII: any information about an individual that:
a. Can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records

b. Is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and

c. Is protected by federal, state or local laws and regulations or industry standards;

2. Student Education Records: as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or departmental policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records;

3. Covered Data and Information within the meaning of Title V of the Gramm Leach Bliley Act of 1999 (Public Law 106-102, 11 Statute 1338) (as amended) and its implementing regulations;

4. Human Subjects Research Data or Other Sensitive Research Data;

5. Protected Health Information (“PHI”): As defined by Health Insurance Portability and Accountability Act (HIPAA), PHI is information, whether oral or recorded in any form or medium, that: is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university; and relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past present or future payment for the provision of health care to an individual; and includes demographic data, that permits identification of the individual or could reasonably be used to identify the individual;

6. Payment Card Information: as regulated by the Payment Card Industry Data Security Standard (PCI DSS), payment card information is defined as Cardholder Data or Sensitive Authentication Payment Data:

   a. Cardholder Data - full magnetic stripe or the Primary Account Number (PAN) plus any of the following: cardholder name; expiration date; service code; CVC2/CVV2/CID (a three- or four-digit number displayed on the signature panel of the card or, in the case of American Express, on the face of the card; and

   b. Sensitive Authentication Data—magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks;

Note: Canisius College does not store cardholder data in any of its information systems. Cardholder data is stored by third-party vendors, which are contractually obligated to comply with the PCI DSS.

7. An Authentication Verifier: any piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some rare
instances, an Authentication Verifier may be shared amongst a small group of individuals. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include passwords and cryptographic private keys;

8. Export Controlled Materials: any information or materials that are subject to United States export control regulations including, but not limited to, the Export Administration Regulations (“EAR”) published by the U.S. Department of Commerce and the International Traffic in Arms Regulations (“ITAR”) published by the U.S. Department of State;

9. Federal Tax Information: any return, return information or taxpayer return information that is entrusted to the college by the Internal Revenue Services;

10. Passport and social security numbers; and

11. Legal investigation records conducted by the college.

Unauthorized access to, or disclosure of, Private-Highly Restricted College Data will generally require notification to affected parties under the guidelines of state and federal breach notification laws or applicable contract provisions.

B. Private-Restricted

Private-Restricted College Data is College Data that by law is not Public and is available within the college only to those with a legitimate need to know but are not so highly sensitive that the loss of confidentiality of the data would cause significant personal, institutional, or other harm, and no law, regulation, or contract require a higher degree of security.

Examples of Private-Restricted College Data include, but is not limited to:

1. Student Directory Information (if student has requested non-disclosure (suppressed): name, address, email address, telephone/mobile device number, dates of enrollment/registration, enrollment/registration status, major, adviser, college/school, class, academic awards and honors received, and degree received;

2. Linking a library patron’s personal identity with materials requested or borrowed by the person or with a specific subject about which the person has requested information or materials;

3. Exam questions or answers;

4. Human Resources employment data;

5. Law enforcement investigation data, judicial proceedings data; includes student disciplinary or judicial action information;

6. Information Technology infrastructure data;

7. Trade secret data;

8. Protected data related to research;

9. College intellectual property;

10. College proprietary data;

11. Data protected by external non-disclosure agreements;
12. Inter- or intra-agency data which are not: statistical or factual tabulations; instructions to staff that affect the public; final agency policy or determination; external audit data;

13. A student or employee college identification card number;

14. Licensed software;

15. Information created by a health care provider and used or maintained for the purposes of patient treatment, patient payment, or health care provider operations that is not regulated by HIPAA.

C. Public College Data

College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional or other harm.

Examples of Public College Data include, but is not limited to:

1. General access data on a college webpage;

2. Student Directory Information (if student has not requested non-disclosure (suppressed): name, address, email address, telephone/mobile device number, dates of enrollment/registration, enrollment/registration status, major, adviser, college/school, class, academic awards and honors received, and degree received;

3. Employee Directory/Contact Information (not designated by the owner as private): name, addresses (campus and home), email address, listed college telephone and mobile device number(s), dates of current employment, and position(s);

4. Campus maps, job postings, press releases, course information, research publications, newsletters, newspapers and magazines.

II. Reclassification of College Data

Data Owners should periodically reevaluate information classifications to ensure the delegated classification is still appropriate. Changes to laws and rules, contractual obligations, or how certain information is used can result in modification to the information’s value to the college and its classification.

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
Access Control Policy
Audit and Accountability Control Policy
Cloud Computing Policy
Confidential Information Policy
Configuration Management Policy
Health Insurance Portability and Accountability Act Policy
Identification and Authentication Policy
Information Security Program
Information Technology Personnel Security Policy
Information Technology Physical and Environmental Protection Policy
Information Technology Security Awareness and Training Policy
Media Protection Policy
<table>
<thead>
<tr>
<th>Mobile Device Use and Support Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Policy</td>
</tr>
<tr>
<td>Student Records (FERPA) Policy</td>
</tr>
</tbody>
</table>

**Revision Feedback for Data Classification Policy**

[Submit Feedback]
IDENTIFICATION AND AUTHENTICATION POLICY

Effective Date: May 6, 2019
Policy Number:
Supersedes: Not Applicable
Issuing Authority: President
Responsible Officer: Chief Information Officer
Applicability: All College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data (“applicable information system(s)”), as well as all Authorized Users who access, use, or handle those resources.

History:

PURPOSE
The purpose of this policy is to provide identification and authentication requirements for applicable information systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data. A comprehensive and well-defined identification and authentication policy and associated controls are necessary to maintain secure information systems.

POLICY
It is the policy of Canisius College to protect information systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data from unauthorized access. Unauthorized access to such systems can potentially lead to modification, disclosure, or destruction of the resource and the Private College Data contained on the resource.

All Authorized Users of applicable information systems are assigned a unique identity to securely authenticate to the systems that they have been authorized to access. Access to such systems is authorized based on the principle of least privilege. This means that an Authorized User is given the minimum access level to a given resource in order to perform assigned job duties. Each Authorized User must use the user’s unique account and password (or other authenticator) when logging into a system the user has been authorized to access.

Applicable information systems are audited by the Information Technology Services (“ITS”) for appropriate login data. Should a resource containing Private College Data become compromised, the Authorized User who was logged in at the time of the compromise will be contacted by ITS for information regarding any investigation. Unauthorized or improper access to any information system that collects, processes, maintains, uses, shares, disseminates, or disposes of Private College Data is subject to disciplinary action.

DEFINITIONS
Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.
College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

College Information System—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

Data Custodians—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

Data Owners—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

Members of the College Community—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

Non-Public Personal Information—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

Personally Identifiable Information or PII—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

Private College Data—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the College Data Classification Policy. By definition, Private College Data
includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, and Sensitive Authentication Data. See the College Data Classification Policy for additional information.

Public College Data—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

Sensitive Authentication Data—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

Student Education Records—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

Student Financial Information—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

PROCEDURES/GUIDELINES

I. Identification and Authentication of College Authorized Users

Authorized Users must be uniquely identified and authenticated to access College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data. Accordingly, ITS configures applicable systems to uniquely identify and authenticate Authorized Users of the system.

Authentication of Authorized User identities at the college is accomplished primarily through the use of passwords. For some resources, PINS/tokens, biometrics, or multifactor authentication, or some combination thereof with passwords may be utilized.

II. Identifier Management

ITS manages Authorized User identifiers as follows:

1. ITS assigns a unique login ID to all Authorized Users as appropriately authorized upon hiring or transfer in accordance with the granting of access procedures set forth in the Access Control Policy;
2. Login IDs are unique to each Authorized User and the reuse or sharing of a login ID is prohibited (see the Password Policy);

3. ITS uses the login ID that has been assigned as the Authorized User’s unique identifier throughout the Authorized User’s employment or association with the college;

4. The reissuance of a user Login ID number by ITS is prohibited for the period up to three years after the account has been deleted; and

5. Applicable information systems are configured by ITS to disable a login ID after 90-days of inactivity.

See also the Access Control and Information Technology Security Personnel Security policies.

III. Authenticator Management

ITS, in collaboration with applicable Data Owners, Data Custodians, and employee supervisors, manages information system authenticators (i.e., passwords, keys, tokens, Public Key Infrastructure (PKI) certificates, biometrics) by:

1. Verifying, at the time of issuance of the login ID, the identity of the Authorized User receiving the initial authenticator (see the Information Technology Personnel Security Policy);

2. Issuing an initial password (or other authenticator as applicable to the Authorized User);

3. Ensuring that the initial password (or other authenticator as applicable) has sufficient strength;

4. Enforcing the procedures set forth in the Password Policy for initial password distribution, for lost/compromised or damaged passwords, and revoking passwords;

5. Changing the default content of passwords/authenticators upon information system installation in accordance with the System and Communications Protection Policy;
   a. Default passwords provided for initial entry to a system are changed by ITS staff before implementation of the information system or component (e.g. routers, switches, firewalls, printers, workstations, servers);
   b. ITS staff confirm that software and/or hardware upgrades, updates, and patches have not reinstalled default passwords;

6. Enforcing the minimum and maximum password lifetime restrictions and reuse conditions for authenticators. For password restrictions and reuse, see the Password Policy;

7. Requiring that Authorized Users to change/refresh passwords every six months (for Authorized User-level access);

8. Protecting authenticator content from unauthorized disclosure and modification by adhering to the following requirements:
   a. Having passwords (other than initial) be chosen by Authorized Users as opposed to being assigned by ITS staff;
   b. Access to files containing passwords or password hashes are limited to the information system and its Data Owner.
9. Requiring Authorized Users to take specific measures to safeguard authenticators:
   a. Passwords must be safeguarded in accordance with the Password Policy;
   b. Devices must be configured to safeguard authenticators (e.g., certificates, passwords);
10. Configuring applicable resources, for password-based authentication, to enforce the controls set forth in the Password Policy;
11. Requiring that Authorized Users be trained on the password construction guidelines set forth in the Password Policy;
12. Requiring that forgotten initial passwords be replaced rather than reissued in accordance with the Password Policy;
13. Ensuring that passwords are not included in any type of batch login file, clear text file, script or procedure:
   a. The use of an “auto-login” feature to automatically log a computer onto the college network is strictly prohibited, unless the system is functioning as a kiosk;
14. Requiring passwords to be set on device management user interfaces for all college network-connected devices; and
15. Documenting and storing hardware passwords securely.

IV. Password Feedback
In accordance with the Password Policy, passwords must be masked upon entry by Authorized Users (e.g., displaying asterisks or dots when a user types a password) and not displayed in clear text. This requirement helps protect information from possible exploitation or use by unauthorized users.

V. Cryptographic Authentication
ITS configures its information systems to use mechanisms for authentication to a cryptographic module.

VI. Identification and Authentication of Non-College Users
ITS configures applicable resources to uniquely identify and authenticate non-organizational users (i.e., special access users) in accordance with the controls set forth in the Access Control Policy.

VII. Exception Requests
For details on requesting an Identification and Authentication Policy exception request, please contact the Chief Information Officer.

RELATED POLICIES
Acceptable Use of College Computer and Network Systems Policy
Access Control Policy
Audit and Accountability Control Policy
Data Classification Policy
Configuration Management Policy
Information Security Program
<table>
<thead>
<tr>
<th>Information Technology Personnel Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology Security Awareness and Training Policy</td>
</tr>
<tr>
<td>Mobile Device Use and Support Policy</td>
</tr>
<tr>
<td>Password Policy</td>
</tr>
</tbody>
</table>

**Revision Feedback for Identification and Authentication Policy**

[Submit Feedback]
MEDIA PROTECTION POLICY

Effective Date: May 6, 2019
Policy Number:
Supersedes: Not Applicable
Issuing Authority: President
Responsible Officer: Chief Information Officer
Applicability: All media containing Private College Data, as well as all Authorized Users who access, use, or handle associated media containing Private College Data.

PURPOSE

The purpose of this policy is to provide guidance for protecting and sanitizing Media at the college. Media protection is critical for securing the confidentiality of Private College Data by guarding the data from unauthorized access and disclosure throughout the lifetime of the Media.

POLICY

It is the policy of Canisius College to employ Media protection controls to prevent improperly managed media from becoming the source of unauthorized access to any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the Data Classification Policy. The college controls address Media access concerns throughout the Media lifecycle, from secure use, storage, transportation, and ultimately destruction.

DEFINITIONS

Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

College Information System—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and
electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

**Data Custodians**—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

**Data Owners**—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

**DeGaussing**—demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.

**Disintegration**—a physically destructive method of sanitizing data; the act of separating into component parts.

**Incineration**—a physically destructive method of sanitizing media; the act of burning completely to ashes.

**Media**—includes, but is not limited to, paper, hard drives, random access memory (RAM), read-only memory (ROM), disks, flash drives, memory devices, phones, Mobile Devices, networking devices, and all-in-one printers.

**Media Sanitization**—the process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

**Members of the College Community**—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

**Mobile Device**— any handheld or portable computing device including running an operating system optimized or designed for mobile computing. Any device running a full desktop version operating system is not included in this definition.

**Non-Public Personal Information**—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed
without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to this policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, and Sensitive Authentication Data. See the Data Classification Policy for additional information.

**Public College Data**—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

**Pulverization**—a physically destructive method of sanitizing media; the act of grinding to a powder or dust.

**Purging**—a media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting (i.e., a "laboratory attack"), exceeds the value to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

**Removable Media**—devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and software disks not provided by the college.

**Sensitive Authentication Data**—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

**Student Education Records**—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

**PROCEDURES/GUIDELINES**
I. Media Access

Access to digital media (e.g., disks, magnetic tapes, external/removable hard drives, flash drives) and non-digital media (e.g., paper, microfilm), when either type of media contains Private College Data, is restricted to Authorized Users in accordance with the controls set forth in the Access Control, Identification and Authentication, Physical and Environmental Access, and Use of Mobile Devices policies [INSERT LINKS].

II. Media Storage

The college physically and logically protects media containing Private College Data while at rest, stored, or actively being accessed as follows:

1. Media back-ups are stored in a secure location designated by ITS, and this location’s security is reviewed on a monthly basis as part of the risk assessment process.
   a. 
2. ITS ensures the inventorying of media containing Private College Data at least annually.
3. Data Owners, Data Custodians, and Unit Managers ensure that their units physically and logically protect media containing Private College Data while at rest, stored, or actively being accessed in accordance with the media storage guidelines set forth below, as well as the controls identified in the Access Control, Identification and Authentication, Physical and Environmental Access, System and Communication Protection, and Mobile Device Use and Support policies [INSERT LINKS].
   a. It is the responsibility of Authorized Users of media containing Private College Data to ensure appropriate media storage guidelines (see below) are in place and followed.

Media Storage Guidelines

Media storage guidelines to follow include:

1. Utilizing appropriate FIPS-validated encryptions to protect Private College Data from unauthorized exposure while at rest in accordance with the System and Communications Protection Policy [INSERT LINK];
2. Adhering to the physical security control guidelines set forth in the Physical and Environmental Access Policy [INSERT LINK];
3. Securing electronic and paper media containing Private College Data by:
   a. Storing the Private College Data in a secure manner (i.e., File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Private College Data are to be locked when not in use etc.);
   b. Accessing or viewing the Private College Data electronically or via document printouts in a physically secure location;
   c. Not leaving hard copy printouts containing Private College Data out in public view when not in use;
   d. Erasing whiteboards, dry-erase boards, writing tablets, etc. containing Private College Data in when not in use;
e. Immediately retrieving hard copy printouts from a printer when printed; and

f. Immediately retrieving hard copies from a copying machine when making extra copies.

B. Media Transport

Data Owners, Data Custodians, and supervisors are responsible for ensuring that their units protect and control media during transport outside of controlled areas on campus, and restrict the pickup, receipt, transfer and delivery of such media to only Authorized Users.

Units are required to control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents;
2. Limiting the collection, disclosure, sharing, and use of Private College Data; and
3. Following the least privilege and role-based rules for allowing access (see the Access Control Policy [INSERT LINK]).

It is the responsibility of Authorized Users transmitting Private College Data to ensure appropriate risk mitigation measures are in place to protect such data from unauthorized exposure. Guidelines to follow include:

1. Ensuring they have their supervisor’s approval prior to transmitting media (including when media is distributed to individuals) classified as Private-Highly Restricted;
2. Packaging hard copy printouts for physical transport in such a way as to not have any Private College Data information viewable;
3. When mailing or shipping, send by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery;
4. Encryption must always be used to protect Private College Data transmitted over data networks to protect against risks of interception. This includes when accessing network services which require authentication (for example, usernames and passwords) or when otherwise sending or accessing Private College Data (for example, in electronic mail);
5. Where Private College Data is stored on or accessed from Mobile Devices (for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders), the devices themselves must be encrypted (using "full disk" encryption), irrespective of ownership:
   a. When traveling with Mobile Devices containing Private College Data, or using them in public places, appropriate physical security precautions must be taken to prevent loss, theft, damage, or unauthorized access. Use of tracking and recovery software on applicable Mobile Devices is encouraged.
   b. Authorized Users must be aware that government agencies in any country may require a device or files to be decrypted on entry or exit from the country. If travelling abroad with encrypted Private College Data, this means that there is a risk that the data may have to be disclosed. Wherever possible, Data Owners should not permit Private College Data to be taken abroad.
6. Where Private College Data is transmitted for storage in a public, cloud-based storage facilities, the data must be encrypted prior to storing to ensure that it is not possible for the cloud service provider to decrypt the data (see the Cloud Computing Policy) [INSERT LINK]; and

7. Where peer-to-peer or instant messaging is used to transmit Private College Data, traffic flows between peers must be encrypted and access only allowed to manage instant messaging servers that provide gateways to public services.

III. Media Sanitization

It is the policy of the college to sanitize media prior to disposal, release outside of college control, or release for reuse. This applies to all system media, both digital and non-digital, and whether or not the media is considered removable.

While the primary purpose of this policy is to protect Private College Data, it is often very difficult to separate these classifications on the media or determine conclusively that remnants of Private College Data are not recoverable. Therefore, it is often most expedient and cost effective to purge all College Data from the media before reuse or disposal rather than try to selectively sanitize the Private College Data.

Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. If physical destruction is contracted to a third party outside the college, that third party must hold certifications for destruction of media and must provide the college with written guarantee that the media was destroyed.

A. Sanitization and Destruction Guidelines

Data Owners, in conjunction with Data Custodians and supervisor, are responsible for ensuring that the sanitization and destruction guidelines below are adhered to by their respective units:

1. Paper Media

Data Owners, in conjunction with Data Custodians, supervisors, and Authorized Users, are responsible for ensuring that all paper media under their control is destroyed after the appropriate retention period has expired (see the Records Retention Policy and Schedule) [INSERT LINK] and provided the department does not need the records for legal, research, or other valid purpose. Paper Media may be destroyed as follows:

   1. Any paper-based or other hard copy media containing Private College Data must be shredded with a cross-cut shredder before disposal or transferred to the authorized third party contracted by the college for secure disposition of documents.

   2. Incineration and/or recycling by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media.

2. Electronic Storage Media

All electronic storage media, such as hard disk drives in computers, copiers, external hard drives, USB flash drives, magnetic tapes, etc. containing Private College Data in electronic form must be sent to ITS for sanitization prior to disposal, release outside of college control, or release for reuse.
ITS will sanitize Private College Data from the media utilizing a method that will ensure data recovery is impossible, such as purging, degaussing, or destroying the media utilizing a destruction method that will be able to withstand a laboratory attack (e.g., shredding, disintegration, pulverization, melting or incineration). If purging is done by overwriting the data, the entire media/device will be overwritten with a minimum of three passes.

Equipment that has stored Private College Data and is leaving the control of the college permanently must have all data storage devices removed by ITS before disposition. If the equipment leaving college control must retain the data storage devices, all Private College Data must be properly purged. When a vendor is contracted to service a media device, any hardware requiring replacement must be reset to factory default and all data must be sanitized.

3. **Optical Media**

Optical media (e.g., CDs and DVDs) containing Private College Data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

5. **Mobile Devices**

Pursuant to the Use of Mobile Devices Policy [INSERT LINK], all Mobile Devices, regardless of whether the device is college-issued, that have been used to store, access and/or process Private College Data must be wiped to remove such data before they are transferred to someone else through sale or gifting or otherwise disposed of. It is also advisable to purge all other data from the device before reuse or disposal to protect the user’s PII.

B. **Secure Storage**

Media containing Private College Data that is waiting to be destroyed must be securely stored.

C. **Tracking and Documentation**

ITS reviews, approves, tracks, documents and verifies college media sanitization and disposal actions. Tracking and documentation actions may include, but are not limited to:

1. Date of decommission of the item.
2. Description of items and serial numbers;
3. Inventory numbers;
4. Process and sanitization tools used; and
5. The name and address of the organization the equipment was transferred to, if transferred.

C. **Record Retention**

Prior to requesting the destruction of storage media, Data Owners are responsible for transferring data required to be retained based on established records retention requirements in the Records Retention Policy and Schedule. [INSERT LINK]

IV. **Management of Removable Media**

All users of an information system are encouraged to never store Private College Data on removable media, however Authorized Users of an information system may use Removable Media in their work computers if it is unavoidable. Private College Data may be stored on Removable Media only when required in the performance of assigned duties or when responding to legitimate
requests for information. When Private College Data is stored on Removable Media it must be encrypted.

Users are encouraged to contact ITS to discuss storage of Private College Data on removable media to attempt to discover alternate solutions.

V. Exception Requests
For details on requesting a Media Protection Policy exception request, please contact the chief information officer.

VI. Enforcement and Sanctions
ITS is responsible for the appropriate enforcement of this policy.

Individuals who violate the provisions of the policy are subject to disciplinary action pursuant to applicable disciplinary policies, as well as loss of access to applicable information systems. They may also be subject to criminal and/or civil proceedings.

Visitors and others third party users who violate the provisions of the Policy are subject to loss of access to the college network. They may also be subject to criminal and/or civil proceedings. In addition, the vice president for business and finance may administer other appropriate sanctions.

RELATED POLICIES
Access Control Policy
Acquisition and Disposal Policy
Audit and Accountability Policy
Cloud Computing Policy
Confidentiality of Employee Records Policy
Confidentiality of Student Records Policy
Configuration Management Policy
Data Classification Policy
Identification and Authentication Policy
Incident Response Policy
Information Security Program
Information Technology Personnel Security Policy
Information Technology Physical and Environmental Protection Policy
Information Technology Security Awareness and Training Policy
Identity Theft Prevention Policy
Media Protection Policy
Mobile Device Use and Support Policy
Passwords Policy
Record Retention Policy and Schedule
INFORMATION SECURITY AWARENESS AND TRAINING POLICY

Effective Date: May 6, 2019
Policy Number: Not Applicable
Supersedes: Not Applicable
Issuing Authority: President
Responsible Officer: Chief Information Officer
Applicability: All Authorized Users of College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data.

PURPOSE
The purpose of this policy is to provide guidance in developing and implementing appropriate training regarding the protective policies and associated controls in place at the college that support the confidentiality, integrity, and availability of applicable information systems and College Data.

POLICY
It is the policy of Canisius College to provide information security awareness education to all Authorized Users of College Information Systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

Authorized Users granted access to Private College Data are adequately trained to perform their information security-related duties and responsibilities consistent with related college policies, legal requirements, regulations, and agreements. The chief information officer, ITS, and the SSC work in cooperation with Human Resources to develop training and education programs for all employees who have access to Private College Data, reviews the information security awareness program annually and appropriate updates are applied based on the findings of the annual reviews. Directors and supervisors are ultimately responsible for ensuring compliance with information security policies and associated control.

DEFINITIONS

*Authorized User*—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

*College Data*—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

*College Employees*—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.

*College Information System*—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term...
system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

**Covered Data and Information**—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

**Data Custodians**—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

**Data Owners**—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

**Members of the College Community**—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

**Non-Public Personal Information**—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the Data Classification Policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, and Sensitive Authentication Data. See the Data Classification Policy for additional information.

**Public College Data**—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.
**Sensitive Authentication Data**—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

**Student Education Records**—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

**Student Financial Information**—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

**PROCEDURES/GUIDELINES**

I. **General Training**

A. **Employee Training**

During employee orientation, each new employee to be granted authenticated access to Private College Data receives general training on the importance of confidentiality of Private College Data, actions needed to be taken to maintain security, information on how to respond to suspected security incidents, and the need for physical operations security.

Specific topics addressed include, but are not limited to:

1. The proper use of College Data and passwords;
2. A review of policies and associated controls in place at the college to prevent employees from providing College Data to an unauthorized individual, (i.e., training on appropriate use of encryption use, etc.);
3. A review of physical security policies and controls to protect Private College Data;
4. How to properly dispose of documents that contain College Data in accordance with the Record Retention Policy and Schedule; and
5. Protecting College Data from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

General training will be conducted when required by system changes.

As a supplement to the training programs listed above, general employee education is also attained through regular electronic mails sent by ITS, as well as Social Media postings that highlight...
relevant information technology security topics. ITS also provides one-on-one training upon request. Users of the administrative information systems of the college who do not participate in any required training are subject to loss of their access privileges.

Collectively, the above general training efforts help minimize risk and safeguard College Data.

2. Student Training

ITS provides students with general information security education. This material is made available on the ITS Website.

II. Administrator Account Training

ITS The end user department delivers specific role-based training for individuals authorized to use administrator access accounts prior to them receiving privileged access. ITS resources are available to assist in this end user training as needed. This training is documented and archived by the end user department and includes, but is not limited to the following topics:

1. Each individual that uses administrator access accounts is trained to use the account or access privilege most appropriate for the requirements of the work being performed (e.g., Authorized User account vs. administrator account);

2. Each individual that uses administrator access accounts will receive training regarding abuse of privilege:
   a. Investigations conducted by individuals that uses administrator access accounts shall be conducted as directed by the chief information officer, after consultation with the area vice president of the college.
   b. In those cases where law enforcement agencies request access in conjunction with an investigation, the request must be presented in writing (e.g., subpoena, court order). All individuals that use administrator access accounts that receive such a written request must report the matter to the chief information officer, who will consult with the area vice president of the college before any action is taken.

3. The password for a shared administrator access account must change under the following conditions:
   a. An individual knowing the password leaves the college or department;
   b. Job duties change such that the individual no longer performs functions requiring administrator access; and
   c. A third-party contractor or vendor with role account access leaves or completes the contracted work.

4. A password escrow must be in place for all administrative accounts to enable someone other than the custodian to gain access to the system in an emergency.

Administrative access training is reviewed annually by the end user department supervisor, upon necessary system changes, and updated accordingly.

III. Special Account Training
Third-parties, such as suppliers, contractors, vendors, and partners, granted special account access by ITS are required to understand their roles and responsibilities regarding information system security requirements. See the Information Security Program document.

Depending upon the nature of the third-party relationship, the roles and responsibilities may vary greatly. If a third-party is granted access privileges to Private College Data, the third-party will be required to have in place a training program that meets the same level of requirements as the college’s information security training and awareness program. In the event the third-party does not have an adequate information security awareness and training program, the college, at its discretion, may administer its training and awareness program for the third-party.

**RELATED POLICIES**

- Acceptable Use of College Computer and Network Systems Policy
- Access Control Policy
- Acquisition and Disposal Policy
- Audit and Accountability Control Policy
- Configuration Management Policy
- Data Classification Policy
- Email Retention Policy
- Identification and Authentication Policy
- Incident Response Policy
- Information Security Program
- Information Technology Personnel Security Policy
- Information Technology Physical and Environmental Protection Policy
- Identity Theft Prevention Policy
- Mass Email Policy
- Media Protection Policy
- Mobile Device Use and Support Policy
- Password Policy
- Record Retention Policy and Schedule
- Wireless Access Points Policy
PURPOSE

The purpose of this policy is to provide physical and environmental protection requirements for applicable information systems that access or store Private College Data and for the facilities in which they operate. Documented physical protection security controls are needed to ensure applicable information systems are properly protected against physical threats.

POLICY

It is the policy of Canisius College to use information technology security control measures to:

1. Protect applicable information systems that access or store Private College Data against unauthorized access and use;
2. Maintain the integrity of Private College Data;
3. Ensure Private College Data residing on any information system is available when needed; and
4. Comply with the appropriate federal, state and other legislative, regulatory and industry requirements.

DEFINITIONS

Authorized User—are all individuals, including, but not limited to, employees, temporary employees, faculty, students, alumni, trustees, campus visitors, contractors, vendors, consultants and their related personnel, and other individuals authorized by the college to access a college computer, the college network(s), or information systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

College Data—any information collected, manipulated, stored, reported, or presented in any format, on any medium, at any location by any department, program or office of the college in support of the college’s mission.

College Employees—includes Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.
**College Information System**—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

**Covered Data and Information**—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

**Data Custodians**—the custodian of College Data is generally responsible for the processing and storage of College Data. The custodian is responsible for the administration of controls as specified by the Data Owner. By definition, Data Custodians are also Authorized Users.

**Data Owners**—the owner of a collection of College Data is usually the manager responsible for the creation of that data or the primary user of that information. This role often corresponds with the management of department. In this context, ownership does not signify proprietary interest, and ownership may be shared. By definition, Data Owners are also Authorized Users.

**Members of the College Community**—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.

**Mobile Device**—any handheld or portable computing device including running an operating system optimized or designed for mobile computing. Any device running a full desktop version operating system is not included in this definition.

**Non-Public Personal Information**—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.

**Private College Data**—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to this policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information, Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive
Research Data, Protected Health Information, and Sensitive Authentication Data. See the Data Classification Policy for additional information.

Public College Data—College Data that by law are available to the public upon request, and that the loss of the data would not cause significant personal, institutional, or other harm.

Sensitive Authentication Data—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

Student Education Records—as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or department policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records.

Student Financial Information—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CRF §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

PROCEDURES/GUIDLINES

I. Physical Access Authorization Management

A. Sensitive Areas

Access to college data processing center(s), data equipment closets, and areas that house systems that store, process, or transmit Private College Data (hereinafter “sensitive areas”) is limited to authorized individuals.

Only authorized individuals may access sensitive areas through the use of authorization credentials (key cards/keys/college ID badges, etc.).

The chief information officer (or his/her designee) reviews and grants authorization access to authorized individuals.

Information Technology Services (“ITS”) maintains and annually reviews the list of individuals with authorized access to sensitive areas.

Authorized individuals must be removed from the list when access is no longer required, or the employee is terminated or transferred. Upon termination or transfer, all physical access mechanisms, such as keys, access cards, etc., are returned or disabled (see the Information Technology Personnel Security Policy).
Note: maintenance staff, cleaners and others who require periodic access to the sensitive area must be screened and their names added to the access list.

B. Office Environments

Access to offices that process, maintain, or store College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the College Data Classification Policy must follow the principle of least privilege access. Only authorized personnel will have physical access to non-public office locations. Access to these office locations should be based on role or responsibilities, and a determination that access is required for individuals to perform their job functions.

Appropriate managerial staff of secured office locations are required approve personnel with authorized access to the office. Access is removed and the access card, key, or lock deactivated, or combination changed as applicable in response to notification of changes in staff or staff responsibility. Removal of individuals who no longer require access is automated through the college provisioning system. When HR terminates an individual their ID card access is removed and keys collected.

Security clearance for visitors to such areas may include, but is not limited to, a sign in book, employee escort within a secure area, and ID badges for visitors.

II. Physical Access Control

A. Sensitive Areas

1. Authorized Employee Physical Access

Sensitive areas are protected by the following physical entry controls to ensure that only authorized college employees are allowed access to these areas:

1. Sensitive areas are restricted to only authorized employees and authorized third parties when escorted (see Visitor Physical Access section below);

2. At no time may the sensitive area be left unsecured allowing access by unauthorized personnel. All personnel must be validated and approved by the applicable Data Custodian or the Director of Public Safety prior to accessing the sensitive area.

3. Key/combination/access control card systems are used to authorize and validate access to sensitive areas:

   a. Upon approval of the chief information officer, key/combination/access control cards are issued to authorized employees in accordance with Key Policy.

   b. The sharing of issued keys/combinations/access cards is prohibited;

   c. Lost keys/access cards must be reported to the chief information officer.

   d. Keys/combinations/access cards are changed when keys/access card are lost/combinations are compromised or individuals are transferred or terminated and the key/access card is not returned, as applicable.

4. All doors and entrance locations of sensitive areas shall be locked when unattended;

5. Console login screens are locked when unattended;

6. Sensitive areas are protected during non-business hours by an alarm system;
7. All authorized employees must have in their possession a college-issued identification cards when accessing sensitive areas;

8. College employees must notify college security when they encounter unescorted visitors or any non-authorized personnel accessing a sensitive area;

9. ITS, in collaboration with the appropriate Data Owner, Data Custodian, and supervisor, maintains a physical access audit log for specified entry/exit points to these areas;

10. ITS shall document and maintain maintenance records, including documentation of repairs and modifications to data processing center doors, locks, walls, access cards, etc.

11. Physical access to publicly accessible network jacks is restricted by either:
   a. Preventing physical access to the network jack via a key/combo/combination/access control card system; or
   b. 

12. Physical access to Wireless Access Points (WAPs), gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.
   a. ITS employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to applicable resource systems

13. Unauthorized physical access to devices that capture credit and payment card data (e.g., Point of Sale (PoS) devices) is enforced

2. Visitor Physical Access to Sensitive Areas

Visitors, including third-party support services personnel, are granted access to sensitive areas only when required, authorized, and monitored by ITS or other appropriate college staff:

1. ITS must authorize visitors before entering specific controlled sensitive areas;

2. Visitors must sign in and out of the sensitive area logbook, documenting their name, company if any, purpose of visit, time of entry and departure, and the name of the college employee authorizing the access;
   a. The log must be readily accessible for at least three (3) months

3. Visitors must be escorted by authorized ITS or other appropriate college staff;

4. ITS issues visitors a badge or other identification that expires and that visibly distinguishes them from members of the college community; and

5. Visitors must turn in their badge or identification before leaving the sensitive area.

B. Office Environments

Physical access to Private College Data regardless of form (paper, CD/Disk/external drives, PCs/Laptops, portable devices/smartphones/etc.) must be restricted to authorized personnel.

1. Data Owner Responsibilities
Data Owners are responsible for ensuring the physical security of Private College Data including provisions for:

1. Organization of workstations, printers, fax machines, etc. to minimize security risks of physical exposure to Private College Data:
   a. Workstations, printers, fax machines, etc. should not be located in public sections of walkways, hallways, waiting areas, etc. To the extent reasonable, efforts should be made to limit the viewing of data on these workstations to Authorized Users with legitimate business need to do so; and
   b. Data Owners should request computer moves through ITS;
2. Restricting physical access to workstations and other applicable information systems accessing Private College Data to authorized employees granted Authorized User status pursuant to the college Access Control Policy;
3. Restriction of the distribution of keys/access cards which provide entry to secure areas in compliance with the Key Policy to only Authorized Users in the department:
   a. The sharing of issued keys/access cards is prohibited;
   b. Lost keys/access cards must be reported to the Data Owner.
   c. Keys/access cards are changed when keys/access card is lost or individuals are transferred or terminated and the key/access card is not returned, as applicable.
4. Proper disposal of all materials containing Private College Data in accordance with the Media Protection policy.
5. Proper location of fax machines and printers which receive and print documents containing Private College Data.
6. Proper archiving and disposal of all customer and college banking related information. (i.e. lock box payments, deposits, credit card receipts, direct deposit requests, any personally identifiable payment related information)

2. Data User Responsibilities

Authorized Users are responsible for the physical security of and access to applicable information systems that collect, process, maintain, use, share, disseminate, or dispose of Private College Data entrusted to their use. When practical, the following physical security practices must be followed:

1. Not sharing work area issued keys and/or access cards with others;
2. For those Authorized Users working in open, common or otherwise unsecured areas, users are required to logoff or lock their computers when the computer will be unattended for example, by pressing the ctrl-alt-del keys and then press the "lock computer" button;
   a. It is suggested that workstations which access Private College Data have a password protected screensaver enabled. The automatic time out configuration might also be enabled;
   b. To the extent possible, workstations which access Private College Data must be located in areas that have some degree of physical separation from the public and where possible should face away from public view. When applicable, computer
screens should face away from other employees to ensure privacy of sensitive information;

3. Laptops and Mobile Devices, regardless of ownership, used to access Private College Data must be stored securely when unattended. Appropriate secure storage methods include a locking security cable attached directly to the device, storage in a locked cabinet or closet, storage in a locked private office, or the like;

4. Whenever possible, locking doors and entrance locations to the work area when unattended;

5. Locking private desk drawers, personal computers, peripherals, and related equipment when not in use;

6. Exiting running applications and closing any open documents when not in use; and

7. Adhering to media storage and sanitation control guidelines identified in the Media Protection Policy.

III. Environmental Controls

ITS has implemented the following controls to protect the college’s data processing center(s) from damage, destruction and/or interruption due to environmental factors such as fire, humidity, water, power outage, etc.:

1. Business Continuity and Disaster Recovery Program: ITS has developed disaster recovery and contingency planning to support restoration of data in the event of an emergency or disaster.

2. Power Equipment and Cabling: Where feasible, ITS has placed power equipment and cabling for applicable information systems in safe locations to prevent environmental and/or man-made damage and destruction.

3. Emergency Shutoff: Multiple shutoffs are located in the data processing center(s) for personnel to cut power in emergency situations.

4. Emergency Power: An uninterruptible power supply has been installed in the data processing center(s) to facilitate transition to long-term alternate power in the event of a primary power source loss.

5. Emergency Lighting: The data processing center and building are covered by emergency lighting in the event of a power outage.

6. Fire Protection: The data processing center(s) is protected by a fire detection and automatic suppression system. The system is inspected annually by the college.

7. Temperature and Humidity Controls: Temperature and humidity are maintained and monitored in the data processing center. Alarms are setup if temperature or humidity exceed acceptable levels.

IV. Exception Requests

For details on requesting a Physical and Environmental Protection Policy exception request, please contact the chief information officer.

VI. Enforcement and Sanctions
ITS is responsible for the appropriate enforcement of this policy. Data Owners and Users who violate the provisions of the Policy are subject to disciplinary action pursuant to applicable disciplinary policies, as well as loss of access to applicable information systems. They may also be subject to criminal and/or civil proceedings.

Visitors and others third party users who violate the provisions of the Policy may be subject to criminal and/or civil proceedings. In addition, the vice president for business and finance may administer other appropriate sanctions.

**RELATED POLICIES**

- Access Control Policy
- Data Classification Policy
- Identification and Authentication Policy
- Identity Theft Prevention Policy
- Information Security Program
- Key Policy
- Media Protection Policy
- Mobile Device Policy
- Passwords Policy

---

**Revision Feedback for IT Physical and Environmental Protection Policy**

[Submit Feedback]
Confidentiality of Library Records Policy

**Effective Date:** May 6, 2019

**Policy Number:**

**Supersedes:** Not Applicable

**Issuing Authority:** President

**Responsible Officer:**

**Applicability:**

**History:**

Andrew L. Bouwhuis, SJ Library

**Confidentiality of patron records**

Library records relating to an individual patron’s use of the Library and its resources are confidential. These records will not be disclosed to others except with the consent of the library patron, or as required by law.

The American Library Association Policy Manual 54.14 – Code of Ethics, states, “Librarians must protect each user’s right to privacy. Confidentiality extends to information sought or received, and materials consulted, borrowed, acquired, and includes database search records, reference interviews, circulation records, interlibrary loan records, and other personally identifiable uses of library materials, facilities, or services.” It is the ethical responsibility of library staff to protect the privacy of library patrons.

New York, NY CPLR 4509 states: *Library records, which contain names or other personally identifying details regarding the users of public, free association, school, college and university libraries and library systems of this state, including but not limited to records related to the circulation of library materials, computer database searches, interlibrary loan transactions, reference queries, requests for photocopies of library materials, title reserve requests, or the use of audio-visual materials, films or records, shall be confidential and shall not be disclosed except that such records may be disclosed to the extent necessary for the proper operation of such library and shall be disclosed upon request or consent of the user or pursuant to subpoena, court order or where otherwise required by statute.*

Any information on an individual patron record or any information regarding who has borrowed particular items is confidential and is not to be disclosed by any library staff member or student assistant. One patron should not be given information about another patron. A parent should not be given information about student library use without the permission of that student. Outside parties or entities should not be given patron information unless it is pursuant to library
operations (a contracted vendor providing service to the library where such information is necessary for functionality) or by order of a court with jurisdiction.

All registration and circulation records are confidential and should not be disclosed except as follows:

a. by a person acting within the scope of his or her duties within the administration of the library (e.g. library staff can perform necessary updating to patron records)

b. by a person authorized, in writing, by the individual to whom the records pertain, to inspect the records

c. by order of a court with the appropriate jurisdiction

Patrons should be aware that Federal legislation (USA PATRIOT Act of 2001, The USA Freedom Act) have expanded the circumstances under which a federal agent may request patron records held by the Library; if such records are requested by federal authorities, the Library is prohibited by law from notifying the patron of that request. The Library forwards any law enforcement requests for patron records to the College’s legal counsel.
REPORTABLE BUSINESS RELATIONSHIPS POLICY

Effective Date: May 6, 2019
Policy Number: III – 3.3.25
Supersedes: Not Applicable.
Issuing Authority: President
Responsible Officer: Associate Vice President, Human Resources & Compliance
Applicability: All Canisius College employees who are “State Persons” as defined by New York’s Public Integrity Reform Act, as well as the college’s trustees and officers.

PURPOSE

The purpose of this policy is to comply with New York’s Public Integrity Reform Act, which requires the college to publicly disclose Reportable Business Relationships with State Persons.

POLICY

It is the policy of Canisius College to comply with New York’s Public Integrity Reform Act (hereinafter “Act”), which requires the college, as both a registered lobbyist and a client of a lobbying firm(s), to publicly disclose information about Business Relationships with State Persons, regardless of when the relationship commenced, if the criteria for a Reportable Business Relationship exists (see Definitions).

Moreover, as required by the Act, it is also the policy of the college to report each Reportable Business Relationship of all its High-Level Individuals (i.e., college trustees and officers). This includes Reportable Business Relationships entered into by a High-Level Individual in his or her personal capacity, as well as Reportable Business Relationships entered into by another entity at the direction or request of the High-Level Individual.

In the higher education setting, the types of relationships described above most often arise in the context of the college employing a State Person (e.g., as an adjunct faculty member or staff employee) or from transactions between the college or one of its trustees or officers and outside businesses in which a State Person may be a partner or shareholder (e.g., law, accounting, or engineering firms).

DEFINITIONS

Aggregation—if the college has multiple Relationships with the same State Person, the same entity or entities in which a State Person has the Requisite Involvement, then the value of the Compensation paid for goods, services or anything of value relating to such Relationships must be aggregated. If the aggregated value of such Compensation is more than $1,000 annually (within 12 consecutive months), then each relationship is a Reportable Business Relationship (assuming all other criteria are satisfied).

Compensation—any salary, fee, gift, payment, benefit, loan, advance or any other thing of value. It does not include: commercially available consumer and business loans or lines of credit as available to the general public; goods and services and discounts available to the general public;
dividends or payments related to stock purchases; or contributions reportable under Article 14 of the New York State Election Law.

*High Level Individuals*—at Canisius College, the trustees of the college’s governing board, the president, the provost, and other vice presidents are High-Level Individuals.

*Intended to be Performed or Provided*—the goods, services or anything of value have not yet been performed or provided, but the college reasonably anticipates such goods, services, or value to be performed or provided in the future.

*Performed or Provided*—State Person or an entity in which the State Person has the Requisite Involvement either (i) actually performed or provided the goods, services or anything of value, or (ii) had a significant, but not necessarily exclusive or primary role, in performing or providing the goods, services or anything of value.

*Reason to Know*—whether the college has “reason to know” that (i) an individual is a State Person, or (ii) a State Person has the Requisite Involvement with an entity, is based on an examination of the totality of the facts and circumstances. If a reasonable person, looking at all the facts and circumstances, would conclude that the college should know that an individual is a State Person or that a State Person has the Requisite Involvement with the relevant entity, then the “reason to know” standard has been satisfied. Some, but not all, factors that may be considered in this analysis are: Origins of the relationship between the parties; Length of such relationship; The type and actual value of the goods, services or items provided; and/or Whether the fact that the individual is a State Person or the Requisite Involvement of the State Person with the entity at issue is generally known to the public. The college will be deemed to have had reason to know if the lack of knowledge results from willfully ignoring information that would lead a reasonable person to: conclude that the individual was a State Person, or that a State Person had the Requisite Involvement, or, undertake further research to determine whether either fact exists.

*Reportable Business Relationship*—a relationship, regardless of when the relationship commenced, in which a formal or informal agreement or understanding exists in which Canisius College or a High-Level Individual of the college pays, has paid or promises Compensation to:

1. An individual whom the college knows or has reason to know is a State Person;

2. A non-governmental entity for which the college knows or has reason to know that the State Person is a proprietor, partner, director, officer or manager of a non-governmental entity, or owns or controls 10% or more of the stock of such entity (or 1% in the case of a corporation whose stock is regularly traded on an established securities exchange) (These roles and positions are referred to as the “Requisite Involvement.”); or,

3. A third-party as directed by the State Person or as directed by the entity in which the State Person has the Requisite Involvement;

    **and**

The payment or promise of Compensation is or was in exchange for goods, services or anything of value, the total value of which exceeds $1,000 annually, either performed or provided or intended to be performed or provided by the State Person or an entity in which the State Person has the Requisite Involvement.
Exclusions: A Relationship in which the college or High-Level Individual provides Compensation to a State Person or an entity in which the State Person has Requisite Involvement that relate to the following are excluded from reporting requirements: Medical, dental and mental health services and treatment; and legal services with respect to: investigation or prosecution by law enforcement authorities; bankruptcy; and domestic relations matters.

Requisite Involvement in an Entity—when a State Person is a proprietor, partner, director, officer, or manager of a non-governmental entity, or owns or controls 10% or more of the stock of a non-governmental entity (or 1% in the case of a corporation whose stock is regularly traded on an established securities exchange).

State Person—individuals who are (i) statewide elected officials; (ii) members of the legislature or legislative employees; (iii) heads of State departments and their deputies and assistants, other than members of the board of regents of the university of the State of New York who receive no compensation or are compensated on a per diem basis; (iv) officers and employees of statewide elected officials; (v) officers and employees of State departments, boards, bureaus, divisions, commissions, councils, or other State agencies; and (vi) employees of public authorities (other than multi-state authorities), public benefit corporations and commissions at least one of whose members is appointed by the governor, and members or directors of such authorities, corporations, and commissions who are compensated other than on a per diem basis.

$1,000 Threshold—a Relationship whose total aggregated value of Compensation paid to the State Person or an entity in which the State Person has the Requisite Involvement exceeds $1,000 annually (within 12 consecutive months). Such threshold is met once more than $1,000 in Compensation is paid or owed to such State Person or entity for services Performed or Provided or Intended to be Performed or Provided.

PROCEDURES/GUIDELINES

I. Reporting to the College

In order for the college to comply with the Act, Canisius College requires that all full-time or part-time college employees who are also employed by the State of New York report their State Person status in writing or via email to the Canisius College Human Resources Office. Such reporting must occur at the time of securing State Person status, regardless of whether the outside employment activity is performed during non-college working hours. In addition, Human Resources will send an email notice to all college employees requesting disclosure of State Person status prior to the college’s semi-annual reporting deadline to the New York State Joint Commission on Public Ethics.

In addition, all college trustees and officers are required to immediately disclose Reportable Business Relationships with State Persons to the secretary of the Board of Trustees, as well as complete the Reportable Business Questionnaire (see Appendix) on a semi-annual basis. The college uses, and relies upon in good faith, responses to the questionnaire to determine whether such persons have business relationships that must be reported to the New York State Joint Commission on Public Ethics.

II. Reporting to the New York State Joint Commission on Public Ethics
[Human Resources or the Secretary of the Board of Trustees as applicable] will complete a Reportable Business Relationship Form and submit it to the New York State Joint Commission on Public Ethics within 10 (ten) days of being notified of the Reportable Business Relationship’s existence. For ongoing Reportable Business Relationships, [Human Resources or the secretary of the Board of Trustees as applicable] will disclose the relationship on a Reportable Business Relationship Form filed with the college’s Statements of Registration and/or Semi-Annual Reports covering periods in which the Reportable Business Relationship is in existence.

For each Reportable Business Relationship, the following information within the Reportable Business Relationship Form will be provided:

1. The name and public office address of the State Person or entity with which the State Person has the Requisite Involvement;
2. A description of the general subject or subjects of the transactions between the college and/or High-Level Individual and the State Person (or the entity with which the State Person has the Requisite Involvement); and
3. The actual or anticipated amount of Compensation, including reimbursable Expenses, to be paid and paid to the State Person (or entity with which the State Person has the Requisite Involvement) by virtue of the business relationship.

When multiple Relationships exist with the same State Person, the same entity, or entities in which a State Person has the Requisite Involvement, then the value of the Compensation paid for goods, services, or anything of value relating to such relationships will be aggregated. If the aggregated value of such Compensation is more than $1,000 annually (within 12 consecutive months), then each relationship is a Reportable Business Relationship (assuming all other criteria are satisfied).

**RELATED POLICIES**

- Outside Activities (Faculty) Policy
- Outside Activities (Staff) Policy
QUESTIONNAIRE – REPORTABLE BUSINESS RELATIONSHIP

This questionnaire is being sent to all Canisius College board members, officers, officers, directors or High-Level Individuals pursuant to the Reportable Business Relationship Policy. Such members of the college community are subject to certain disclosure requirements if they have a Reportable Business Relationship with a State Person.

To assist the college in determining whether a Reportable Business Relationship exits that requires the college to file a report with the New York State Joint Commission on Public Ethics, we request that you answer the following questions. Please complete, attach any requested additional detailed information, sign the acknowledgment below, and return this questionnaire to the Secretary of the Board of Trustees.

For purposes of this questionnaire, please refer to the following definitions and the definitions set forth in the Reportable Business Relationship Policy:

Name: _____________________________________
Title: ________________________________
Address: _____________________________________

1. Do you currently have any business relationships in which you purchased or will purchase goods or services valued at more than $1,000 annually from a person or entity located within the State of New York?
   Yes: ____ No: ____
   If “Yes,” go to Question #2. If “No,” sign and date the form.

   NOTE: Reportable Business Relationships include formal and informal relationships that may or may not be based on written contracts.

The value of any outstanding Compensation owed as well the value of goods or services to be performed must be considered when determining if the $1,000 threshold is met.

2. Do the services you are purchasing fall into one or more of the following categories:
   Treatments for medical, dental, and mental health services;
   Legal services with respect to: investigation or prosecution by law enforcement; bankruptcy; domestic relations.
   Yes: ____ No: ____
   If “Yes,” go to Question #3. If “No,” sign and date the form.

3. (a) If the business relationship is with a person, is that individual a New York State employee or a New York State elected official?
   Yes: ____ No: ____ Not that I am aware of: ____
NOTE: The answer “Not that I am aware of” is only appropriate when, based on the totality of the circumstances, the person signing this form does not have a “reason to know” that the business relationship is with a New York State employee or a New York State elected official.

3.(b) If the business relationship is with an entity, is a New York State employee or a New York State elected official a proprietor, partner, director, officer, or manager of the entity?

Yes: ____ No: ____ Not that I am aware of: ___

*NOTE:* The answer “Not that I am aware of” is only appropriate when, based on the totality of the circumstances, the person signing this form does not have a “reason to know” that the business relationship is with an entity in which a New York State employee or a New York State elected official is a proprietor, partner, director, officer, or manager.

3. (c) If the business relationship is with an entity, does a New York State employee or a New York State elected official own or control 10% or more of the stock of the entity (or 1% in the case of a corporation whose stock is regularly traded on an established securities exchange)?

Yes: ____ No: ____ Not that I am aware of: ___

NOTE: The answer “Not that I am aware of” is only appropriate when, based on the totality of the circumstances, the person signing this form does not have a “reason to know” that the business relationship is with an entity in which a New York State employee or a New York State elected official owns or controls 10% or more of the stock of the entity (or 1% in the case of a corporation whose stock is regularly traded on an established securities exchange).

I attest and affirm that the foregoing information is, to the best of my knowledge, true and accurate.

____________________________________________________________________________

Name ___________________________________________ Date ________________________

---

Revision Feedback for 3.3.25: Reportable Business Relationships Policy

Submit Feedback
PURPOSE
The purpose of this policy is to establish guidelines regarding the acceptance of a Secondary Assignment within the college.

DEFINITIONS
Secondary Assignments—are additional assignments within the college where the duties are clearly outside of the regular responsibilities of the employee’s primary job with the college.

POLICY
It is the policy of Canisius College to permit employees to accept a Secondary Assignment within the college under certain approved circumstances and in accordance with the guidelines set forth in this policy. Secondary Assignments are generally temporary and are not benefit-eligible, except where required by law.

Note: This policy does not govern secondary employment outside of Canisius College.

PROCEDURES/GUIDELINES
I. General Requirements for Secondary Assignments
   1. The responsibilities associated with Secondary Assignment are clearly outside of the employee’s primary job responsibilities.
   2. The intended Secondary Assignment does not diminish the employee’s effectiveness in the employee’s primary job with the college.
   3. The college’s best interest is served by allowing the Secondary Assignment.
   4. The employee is qualified to perform the responsibilities of the Secondary Assignment.

II. Procedures Applicable to All Secondary Assignments
   1. Employees who seek a Secondary Assignment within Canisius College, including part-time teaching engagements, must obtain prior written approval from the employee’s current direct supervisor and area vice president. In determining Secondary Assignment
eligibility, the supervisor and area vice president considers whether the assignment meets the general requirements described in this policy.

2. **All Secondary Assignment pay is based on the applicable pay structure for the work to be performed and must be reported and paid in accordance with current payroll and FLSA guidelines:**
   a. A non-exempt employee must be compensated on an hourly basis for any Secondary Assignment and is entitled to overtime pay where applicable.
   b. A non-exempt employee’s total hours among assignments will be accumulated to determine weekly overtime.

3. **Supervisors are responsible for monitoring and ensuring compliance with this policy.**

4. **It is the responsibility of both the primary and secondary supervisors to coordinate with one another regarding applicable leave administration and compensation, including eligibility for overtime pay for non-exempt employees, where due.**

5. **Continuation of the Secondary Assignment will be reviewed at the time of the employee’s annual evaluation. If either the employee’s current direct supervisor and area vice president determines that the employee’s Secondary Assignment within the college interferes with the performance or ability of the employee to meet his or her primary job requirements, the Secondary Assignment will be terminated.**

### III. Procedures Relating to Staff Accepting Adjunct Teaching Assignments

The following procedures apply to staff employees seeking to accept an instructional assignment that are not part of their normal job responsibilities.

**A. Staff Accepting Adjunct Teaching Assignments**

Any staff member interested in adjunct teaching must possess the proper academic credentials or other demonstrated equivalent experience that provides evidence to support effective teaching and student achievement, as well as meet all institutional, accreditation, and regulatory requirements applicable to course instructors.

The teaching assignment must be approved by the staff member’s supervisor. If approved, the details of the teaching assignment and the compensation will be determined by the appropriate academic department chair, the academic dean, and the vice president for academic affairs. Staff approved to teach courses must continue to fulfill their primary employment responsibilities and otherwise meet the requirement set forth in Sections B and C below.

**B. Balancing Primary and Secondary Adjunct Teaching Assignments**

An eligible staff employee may seek a Secondary Assignment to teach a course as an adjunct instructor under one of the following conditions:

1. The staff member teaches the course during non-work hours (i.e., evenings or weekends);
2. The staff member, supervisor and area vice president agree on a flexible work schedule by which the staff member performs part of his or her primary job responsibilities outside normal work hours; or
3. The staff member teaches without charge to the college if the teaching is done during regular working hours and the employee’s supervisor and area vice president approves the teaching assignment.

Staff who teach as adjunct faculty in accordance with paragraph (1) or (2) above shall be compensated according to the regular compensation schedule for adjuncts. Adjunct compensation is not provided for staff whose normal job responsibilities include teaching as part of their primary assignment and on which their contract and base salary are based.

C. Course Limitations

A staff member is not permitted to accept a Secondary Assignment to teach more than one course per semester.

REFERENCING THE POLICY

Hours of Work Policy
Outside Activities Policy
Overtime Policy
Payment of Services Policy