Volume II: 2.4 Information Technology Policies

2.4 Information Technology Policies

2.4.1 Acceptable Use of College Computer and Network Systems Policy

<table>
<thead>
<tr>
<th>ACCEPTABLE USE OF COLLEGE COMPUTER AND NETWORK SYSTEMS POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effective Date:</strong></td>
</tr>
<tr>
<td>May 6, 2019</td>
</tr>
<tr>
<td><strong>Policy Number:</strong></td>
</tr>
<tr>
<td>II – 2.4.1</td>
</tr>
<tr>
<td><strong>Supersedes:</strong></td>
</tr>
<tr>
<td>Not Applicable.</td>
</tr>
<tr>
<td><strong>Issuing Authority:</strong></td>
</tr>
<tr>
<td>President</td>
</tr>
<tr>
<td><strong>Responsible Officer:</strong></td>
</tr>
<tr>
<td>Chief Information Officer</td>
</tr>
<tr>
<td><strong>Applicability:</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>History:</strong></td>
</tr>
</tbody>
</table>

**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 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 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 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 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.

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 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 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. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, 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. 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 PHI—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.)
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.

PROCEDURES/GUIDELINES

I. Conditions of Use

In using the college’s 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 information systems;
3. Authorized Users of the college’s 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 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 information systems; to copy, remove, or otherwise alter any information/data or system that may undermine the authorized use of the college’s information systems; and to do so with or without notice to the user in order to protect the integrity of the college’s 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 information systems, including but not limited to the right to review, access, and audit 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 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 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 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; and 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 information systems sent to or from, or stored in, the college’s systems cannot be guaranteed in the event of legal or disciplinary proceedings.

Authorized Users are responsible for exercising good judgment regarding the personal use of the college’s information systems. If there is any uncertainty regarding personal use of the college’s 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 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 information systems. Under no circumstances shall a user of the Canisius College’s information systems:

1. Engage in any illegal activity using college information systems assets;
2. Engage in any activity contrary to college policy using College information systems assets;
3. Introduce malicious software into the campus information systems;
4. Reveal college information or allow the unauthorized use of college 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 information systems using another user’s account information;
7. Use college information systems to violate intellectual property laws;
8. Use Canisius College 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 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 information systems (especially systems and software) are to be governed by an organized methodology;
12. Attempt to modify or repair college 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 information systems assets at college locations, with the exception of external storage devices;
14. Give, loan, or relocate college information systems assets without ITS approval;
15. Use any software on personal devices connected to college information systems that provides network or file services to others (such as web servers, file servers, network protocols);
16. Use the college’s information systems to assume the identity of another (e.g., by sending forged electronic mail);
17. Utilize the college’s 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 information systems to engage in any conduct that is likely to result in retaliation against the 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 who become aware of 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

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, 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.

- **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.
- **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.
- **Retired Faculty**—full-time faculty who have retired from the college will be permitted to retain their email privileges if their account remains active. 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.
- **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.
- **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.
- **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.
- **Expelled students**—if a student is expelled from the college, email privileges will be terminated immediately.
- **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 greater than one year are 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 protection; 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 information systems if privileges are not revoked. This is a necessary action taken to prevent further misuse and does not presume 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 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
Acquisition and Disposal Policy
Audit and Accountability Control Policy
Cloud Computing Policy
Configuration Management Policy
Copyright and Intellectual Property Policy
Data Classification Policy
Email Retention Policy
### 2.4.2 Access Control Policy

<table>
<thead>
<tr>
<th><strong>ACCESS CONTROL POLICY</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effective Date:</strong></td>
<td>May 9, 2019</td>
</tr>
<tr>
<td><strong>Policy Number:</strong></td>
<td>II – 2.4.2</td>
</tr>
<tr>
<td><strong>Supersedes:</strong></td>
<td>Enterprise Resource Planning (ERP) Access Policy.</td>
</tr>
<tr>
<td><strong>Issuing Authority:</strong></td>
<td>President</td>
</tr>
<tr>
<td><strong>Responsible Officer:</strong></td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td><strong>Applicability:</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

**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.

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 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.

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 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 college information systems is granted by the applicable Data Owner. The request for access must be submitted, in an email message to banner.security@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 Data, 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 an 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 an 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, 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 information systems 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 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;
   e. 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;
3. Each individual granted administrator access must refrain from abuse of privilege and only conduct investigations as directed by the chief information officer;  
4. Each individual granted administrator access must use a password escrow to enable ITS to gain access to the system in an emergency.  
5. 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, switches 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.  

1. 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.  
e. 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 an appropriate 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 use 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;  
i. 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;  
j. 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;  
k. Authorized Users may not provide the user’s NetID and LDAP password to other individuals;  
l. 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);
m. 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);
n. Authorized Users must understand their responsibilities for protecting Private College Data, and the consequences for mishandling such data.

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;
   b. 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;
   c. 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;
   d. Periodically review (on at least an annual basis) existing Authorized User accounts for validity; and
   e. 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. .
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;
   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
2.4.3 Cloud Computing Policy

<table>
<thead>
<tr>
<th>CLOUD COMPUTING POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
</tr>
<tr>
<td>Policy Number:</td>
</tr>
<tr>
<td>Supersedes:</td>
</tr>
<tr>
<td>Issuing Authority:</td>
</tr>
<tr>
<td>Responsible Officer:</td>
</tr>
<tr>
<td>Applicability:</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.

POLICY

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").

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 it conforms to all relevant federal, state, and local laws and regulations. Finally, any 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, as well as 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. 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, 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. 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);
4. 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.

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);
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 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 systems.

Visitors and others third party users who violate the provisions of the policy are subject to loss of access to 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

2.4.4. Computer Asset Disposal Policy

<table>
<thead>
<tr>
<th>COMPUTER ASSET DISPOSAL POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
</tr>
<tr>
<td>Policy Number:</td>
</tr>
<tr>
<td>Supersedes:</td>
</tr>
<tr>
<td>Issuing Authority:</td>
</tr>
<tr>
<td>Responsible Officer:</td>
</tr>
<tr>
<td>Applicability:</td>
</tr>
</tbody>
</table>

PURPOSE

The 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. 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, 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

Any computer 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 Data 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 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 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

2.4.5 Computer Asset Replacement Policy

<table>
<thead>
<tr>
<th>COMPUTER ASSET REPLACEMENT POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effective Date:</strong></td>
</tr>
<tr>
<td><strong>Policy Number:</strong></td>
</tr>
<tr>
<td><strong>Supersedes:</strong></td>
</tr>
<tr>
<td><strong>Issuing Authority:</strong></td>
</tr>
<tr>
<td><strong>Responsible Officer:</strong></td>
</tr>
<tr>
<td><strong>Applicability:</strong></td>
</tr>
<tr>
<td><strong>History:</strong></td>
</tr>
</tbody>
</table>

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 fill-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

2.4.6. Electronic Accessibility Policy

<table>
<thead>
<tr>
<th>ELECTRONIC ACCESSIBILITY POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
</tr>
<tr>
<td>Policy Number:</td>
</tr>
<tr>
<td>Supersedes:</td>
</tr>
<tr>
<td>Issuing Authority:</td>
</tr>
<tr>
<td>Responsible Officer:</td>
</tr>
<tr>
<td>Applicability:</td>
</tr>
<tr>
<td>History:</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.

DEFINITIONS

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.
   c. 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.

f. 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.

2.4.7 Email Retention Policy

<table>
<thead>
<tr>
<th>EMAIL RETENTION POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
</tr>
<tr>
<td>Policy Number:</td>
</tr>
<tr>
<td>Supersedes:</td>
</tr>
<tr>
<td>Issuing Authority:</td>
</tr>
<tr>
<td>Responsible Officer:</td>
</tr>
<tr>
<td>Applicability:</td>
</tr>
</tbody>
</table>

PURPOSE

The purpose of this policy is to establish the college’s policy guidelines and procedures regarding the retention of college employee emails on the Microsoft Exchange server.

POLICY

College employees are responsible for maintaining their Microsoft Exchange email account in accordance with the procedures and guidelines set forth in this policy.

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

**PROCEDURES/GUIDELINES**

Microsoft Exchange automatically deletes old emails according to the following rules:

- Emails located in the "Inbox" and "Sent Items" folders are deleted after 120 days.
- Emails located in the "Deleted Mail" folder are deleted after 30 days.
- Subfolders, and emails within those subfolders, created inside the Inbox, Sent Items, and Deleted Mail folders are deleted after 120 days (Inbox, Sent Items) or 30 days (Deleted Mail).

All other folders do not fall within this policy. Messages within folders outside the Inbox, Sent Items, and Deleted mail folders will remain until manually deleted by the user.

The user can store emails beyond the 120-day limit by creating folders outside the Inbox, Sent Items, and Deleted mail folders, and moving mail from the Inbox, Sent Items, and Deleted mail folders to these outside folders.

Canisius College’s current learning management system (LMS) sends emails with the User’s email address as the return address. However, emails sent from the LMS can be stored within a “sent mail” folder. Emails within the LMS “sent mail” folder are not governed by the Email Retention Policy, and are not purged after 120 days.

Since the LMS applies the sender’s email address as the return address to any outgoing email, subsequent email conversations connected to an LMS sent email takes place entirely outside the LMS. Therefore, any emails sent in reply to an email sent by college employees from the LMS will go to the initial sender’s (faculty or staff) Exchange account Inbox, and therefore will be governed by this policy. Any subsequent reply by the initial sender in the same email conversation will be stored in their Exchange Sent Items folder, and will thus be governed by this policy.

For detailed instructions on how to save emails, Canisius College employees are directed to a tutorial at the following address: [https://wiki.canisius.edu/x/cwHj](https://wiki.canisius.edu/x/cwHj).

**RELATED POLICIES**

Acceptable Use of College Computer and Network Systems Policy

---

### 2.4.8. Information Security Program Policy

<table>
<thead>
<tr>
<th>INFORMATION SECURITY PROGRAM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effective Date:</strong></td>
</tr>
<tr>
<td><strong>Policy Number:</strong></td>
</tr>
<tr>
<td><strong>Supersedes:</strong></td>
</tr>
<tr>
<td><strong>Issuing Authority:</strong></td>
</tr>
<tr>
<td><strong>Responsible Officer:</strong></td>
</tr>
<tr>
<td><strong>Applicability:</strong></td>
</tr>
<tr>
<td><strong>History:</strong></td>
</tr>
</tbody>
</table>

**PURPOSE**

The purpose of this policy is to define the college’s information security 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 ISP in compliance with the Gramm Leach Bliley Act (GLBA). The objective of the 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 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 Asses Disposal Policy
- Computer Asset Replacement Policy
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/CV2/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. 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, 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 stripe data or equivalent on a chip, CAV2/CV2/CV2/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:

1. Appoint an 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 ISP on an annual basis.

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 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 develops and maintains a registry of all computers attached to the college network. This registry includes, 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 keeps records of patching activity. Furthermore, ITS seeks 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 reviews its procedures for patches to operating systems and software, and keeps 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.

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 via the college’s administrative software systems.

In compliance with the GLBA, the college’s ISP includes the following elements:

1. Oversee service providers and contracts, and
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. Evaluate and adjust the ISP on an annual basis.

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 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.

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 policies, controls and procedures, 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, 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.

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 ISP 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;
g. The chief information officer will gather any necessary background information and make a recommendation to approve or deny the request;
h. The chief information officer will approve or deny the request for an exception;
i. The requestor will be notified of the decision to approve or deny;
j. 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
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

2.4.9 Information Technology Change Control Policy

| 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 in a rational and predictable manner so that college employees can plan accordingly.

POLICY

All changes to the college’s 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 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. 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/CV2/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. Change Control Process**

Information Technology Services ("ITS") constantly assesses the college's information 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 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 information systems 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 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 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:

1. An explicit acknowledgement that the contract allows the vendor to 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 vendor;
3. 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;
4. 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;
5. 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;
6. 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;
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.

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
Peer-to-Peer File Sharing Policy
Procurement Policy and Purchasing Procedures

2.4.10 Mass Email Policy

<table>
<thead>
<tr>
<th>MASS EMAIL POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effective Date:</strong></td>
</tr>
<tr>
<td><strong>Policy Number:</strong></td>
</tr>
<tr>
<td><strong>Supersedes:</strong></td>
</tr>
<tr>
<td><strong>Issuing Authority:</strong></td>
</tr>
<tr>
<td><strong>Responsible Officer:</strong></td>
</tr>
</tbody>
</table>
Applicability: All members of the Canisius College Community.

History:

PURPOSE

The purpose of this policy is to provide guidelines for the distribution of mass e-mails to distribute official and commercial messages to members of the Canisius College community or on behalf of the college for commercial purposes.

POLICY

It is the policy of Canisius College that all authorized users of assigned college email accounts desiring to send a mass email, whether it be an official college email message or commercial messages (see Definitions), conform with the guidelines set forth in this policy, as well as the requirements of the CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing) and, when applicable, the Canadian Anti-Spam Legislation (CASL). Note that all mass emails must also adhere to all other existing College policies (e.g., Acceptable Use of College Computer and Network Systems Policy, the Use of the College Name, Seals and Logos Policy, etc.).

DEFINITIONS

Commercial Email Messages—a mass email message that offers or promotes products and services.

Official Email Messages—emails messages which alert the college community to substantial changes in governance, policy, or practice; to immediate threats to health, safety, property, or research; to computer or telecommunications issues; and to shared community interests.

Listserv—an internet communication tool that offers its members the opportunity to exchange ideas, make suggestions, or ask questions to a large number of people at the same time.

Mass Email—any unsolicited electronic mailing sent to more than 50 addressees.

PROCEDURES/GUIDELINES

Pursuant to the CAN-SPAM Act and CASL, the college has adopted different policies and procedures for official and commercial mass email messages sent via a college email account.

I. Distribution of Official Messages

Official messages alert the college community to substantial changes in governance, policy, or practice; to immediate threats to health, safety, property, or research; to computer or telecommunications issues; and shared interests; and approved surveys (see the college’s Survey Policy). Shared interest messages do not include messages of commercial interest (see Commercial Messages below for further explanation). Since official messages relate to an employment or transactional relationship and are non-commercial in nature, they are exempt from the decline (opt out) provision in the CAN-SPAM Act of 2003.

To facilitate official communications, the Office of Information Technology Services (ITS) maintains email lists based on administrative data (for example, Faculty, Staff, Graduate Students, Undergraduate Students and many other lists). Please contact ITS for the most current list names based on administrative data. All official messages are exempt from the decline (opt out) provision in the CAN-SPAM Act of 2003 and must be approved by the appropriate vice president and Office of Marketing and Communication prior to distribution.

Announcements that do not meet the official message criteria outlined above may not be distributed via mass e-mail. Additionally, inappropriate uses of mass e-mail include:

- Messages that are not aligned with the mission of the college;
- Messages that are personal in nature;
- Messages that are commercial in nature, with the exception of those messages that are in support of college business;
- Messages that solicit participation in, support of, or advocacy for events, activities, or campaigns that are not aligned with and/or sanctioned by the college.
- Messages that do not conform to the Acceptable Use of College Computer and Network Systems Policy or other college policy.
- Messages that are not targeted.

II. Commercial Messages

Commercial messages that offer or promote college products and services are specifically covered by the CAN-SPAM Act of 2003 or CASL. Both require the sender to provide recipients with a clear and conspicuous opportunity to decline (opt-out) to receive further commercial messages. Moreover, CASL requires express or implied consent from the recipient prior to sending the email.

All commercial emails must receive advance approval from the Office of Marketing and Communication and the appropriate vice president. Once approved, the college department or organization desiring to send the email must coordinate with ITS to create an appropriate list serve (listserv) to communicate/broadcast the email.

The following guidelines must be adhered to when sending a commercial message:

- The message must include a non-deceptive subject line, from, and to fields;
- The message must include an opt-out mechanism to unsubscribe from the sender’s e-mail list;
- The message must contain the sender’s physical mailing address; and
- If the email message is being sent to a recipient in the United States and is unsolicited (exchange not initiated by the recipient), the email must clearly indicate that it is an advertisement or solicitation. Include the word “advertisement” or “solicitation” in the subject line as appropriate.

III. Exceptions
Individuals exempt from the requirement to obtain approval to use the mass email account groups to disseminate official communications include members of the Senior Leadership Team and their designees acting in their official capacities.

IV. Sanctions

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

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy

2.4.11. Mobile Device Use and Support Policy

<table>
<thead>
<tr>
<th>Mobile Device Use and Support Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
</tr>
<tr>
<td>Policy Number:</td>
</tr>
<tr>
<td>Supersedes:</td>
</tr>
<tr>
<td>Issuing Authority:</td>
</tr>
<tr>
<td>Responsible Officer:</td>
</tr>
<tr>
<td>Applicability:</td>
</tr>
</tbody>
</table>

PURPOSE

The purpose for this policy is to outline the requirements and user expectations for reading and manipulating Private 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 Private 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 Private 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.

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. 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, 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 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, microfim, 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. 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:

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

IV. Initial Configuration

To ensure proper initial configuration of 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 Devices on campus or at a college activity 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

2.4.12. Password Policy

<table>
<thead>
<tr>
<th>PASSWORD POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date:</td>
</tr>
<tr>
<td>Policy Number:</td>
</tr>
<tr>
<td>Supersedes:</td>
</tr>
<tr>
<td>Issuing Authority:</td>
</tr>
<tr>
<td>Responsible Officer:</td>
</tr>
</tbody>
</table>
Application:
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 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.

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 Private 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 may 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 applicable information systems.

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 Private College Data. 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 must support authentication of individual users, not groups;
2. Applications must not store passwords in clear text or in any easily reversible form;
3. Applications must 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 must 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
2.4.13 Peer-to-Peer File Sharing Policy

PEER-TO-PEER FILE SHARING POLICY

Effective Date: May 8, 2017
Policy Number: II – 2.4.13
Supersedes: Not Applicable.
Issuing Authority: President
Responsible Officer: Chief Information Officer
Applicability: All members of the College community.

PURPOSE

The purpose of this policy is to provide for annual disclosures to students regarding the college’s policies and sanctions related to unauthorized peer-to-peer file sharing, as required by The Higher Education Opportunity Act of 2008 (the “HEOA”), as well as outline the college’s fulfillment of its obligations in the area of copyright enforcement under the HEOA.

POLICY

In compliance with the HEOA, it is the policy of the college to prohibit the use of peer-to-peer file sharing programs and applications for the unauthorized acquisition or distribution of copyrighted or licensed material on any college computer or network system. In addition, peer-to-peer file sharing programs and applications commonly used for these illicit purposes may not be installed on any applicable college computer or network system asset and technological deterrents will be used to block their use.

Users of the college’s college computer or network system are prohibited from attempting to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by the college to prevent illegal file sharing. Legal alternatives to illegal file sharing practices include the use of services such as Apple iTunes, Netflix, Hulu, Amazon, Google Play Store, etc.

Canisius College will annually inform students of this Policy and associated procedures and guidelines, consistent with the requirements of the HEOA.

DEFINITIONS

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.

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

Digital Millennium Copyright Act (P.L. 105-304)—a 1998 amendment to the Copyright Act of 1976 that establishes certain limitations of copyright infringement liability for online service providers (OSPs), including colleges and universities, when certain requirements are met by the OSP. The Act contains a number of other provisions, including prohibitions on circumvention of technological protection measures among others.

DMCA Notice or Takedown Request—a warning or request issued from a copyright holder or a representative of the copyright holder. These copyright holders have identified computers on the college’s network as having potentially violated the DMCA and issue warnings regarding the particular infringement to the college.

Information Technology Resources—college computing resources, information technologies, networks, voice messaging equipment, computer software, data networking systems, including remote and wireless and electronically stored institutional data and messages owned, controlled, or managed by the college.

Peer-to-Peer—a network environment where participants share their resources (such as files, disk storage, or processing power) directly with their peers without having to go through an intermediary network host or server.

Peer-to-Peer file Sharing Applications and Programs—Programs or services that use peer-to-peer technology to share music, movies, software, or other digitally stored files.

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

PROCEDURES/GUIDELINES

The college’s obligations under HEOA are handled using a variety of methods.

Technical Limitations
Technologies are utilized at the network border in order to block peer-to-peer file transfer protocols with no legitimate use. Users who require an exception may request one, in writing, from ITS.

Communication to Students

The college makes readily available to the campus community, including enrolled and prospective students, the college’s policies and sanctions related to peer-to-peer file sharing including: (i) a statement that explicitly informs individuals that unauthorized peer-to-peer file sharing may subject the student to civil and criminal liabilities; (ii) a summary of the penalties for violation of Federal copyright laws; and (iii) this policy.

DMCA Notices

All Digital Millennium Copyright Act notices are addressed in accordance with the college’s Copyright and Intellectual Property Policy.

Sanctions

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 the college’s computer or network systems.

Visitors and other third party users who violate the provisions of the policy are subject to loss of access to the college’s computer or network system. Moreover, the vice president for business and finance may administer other appropriate sanctions.

In addition to the above, violators of this policy may be subject to criminal and civil sanctions.

Policy Review

This policy is reviewed yearly by ITS to ensure that it still meets the requirements and objectives for which it was drafted.

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
Copyright and Intellectual Property Policy
Mobile Device Use and Support Policy

2.4.14 Remote Access Policy

<table>
<thead>
<tr>
<th>REMOTE ACCESS POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effective Date:</strong></td>
</tr>
<tr>
<td><strong>Policy Number:</strong></td>
</tr>
<tr>
<td><strong>Supersedes:</strong></td>
</tr>
<tr>
<td><strong>Issuing Authority:</strong></td>
</tr>
<tr>
<td><strong>Responsible Officer:</strong></td>
</tr>
<tr>
<td><strong>Applicability:</strong></td>
</tr>
</tbody>
</table>

**PURPOSE**

The purpose of this policy is to define standards for VPN-based remote access to the Canisius college network by employees utilizing an off-campus internet connection. These standards are designed to minimize the possibility of information disclosure to unauthorized parties, while still providing necessary informational resources to the college community.

**POLICY**

The appropriate area vice president approves area positions that are granted VPN user credentials. All VPN credentialed employees wishing to connect to the college VPN must do so with a computer that has been built and audited by Canisius College ITS. This machine must be provided by the employee’s department, and will not be used for any non-college purpose.
DEFINITIONS

College Informational Resources—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, 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.

PROCEDURES/GUIDELINES

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Canisius College resources.
- VPN access is to be controlled using the employee’s NetID and LDAP password.
- When connected to the college VPN, all traffic from the user will be sent through the encrypted tunnel. All other traffic will be dropped.
- Split-tunneling is not enabled.
- The VPN concentrator(s) will be set up and maintained by Canisius College ITS.
- All computers connecting to the college VPN must have active, up-to-date antivirus software and operating system patches.
- VPN users will be automatically disconnected from the network after 60 minutes of inactivity.
- 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.
- Only VPN clients approved by Canisius College ITS may be used to connect to the college VPN.
- 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.

Enforcement

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

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
Cloud Computing Policy
Copyright and Intellectual Property Policy
Standards of Ethical Conduct
Information Security Program
Mobile Device Use and Support Policy

2.4.15. Information Technology Maintenance Policy

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

**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. 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/CV2/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. 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.
   f. 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;
   g. 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;
   h. Sanitizes equipment to remove all Private College Data from associated media prior to removal from college facilities for off-site maintenance or repairs; and
   i. 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;
   c. Audits remote maintenance and diagnostic sessions; and
   d. Reviews the records of the remote maintenance and diagnostic sessions.

III. Supported Software

For supported software packages (see 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 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 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

2.4.16. Wireless Access Points Policy

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 Billey 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.

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 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/CAV2/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.

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.

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

Copyright and Intellectual Property Policy

Information Security Program

Mobile Device Use and Support Policy