# Volume II: 2.4 Information Technology Policies

- 2.4.1 Acceptable Use of College Computer and Network Systems Policy
- 2.4.2 Access Control Policy
- 2.4.3 Cloud Computing Policy
- 2.4.4. Computer Asset Disposal Policy
- 2.4.5 Computer Asset Replacement Policy
- 2.4.6. Electronic Accessibility Policy
- II. Training
- 2.4.7 Email Retention Policy
- 2.4.8. Information Security Program Policy
- 2.4.9 Information Technology Change Control Policy
- 2.4.10 Mass Email Policy
- 2.4.11. Mobile Device Use and Support Policy
- 2.4.12. Password Policy
- 2.4.13 Peer-to-Peer File Sharing Policy
- 2.4.14 Remote Access Policy
- 2.4.15. Information Technology Maintenance Policy
- 2.4.16. Wireless Access Points Policy
- 2.4.17. Audit and Accountability Control Policy
- 2.4.18. Configuration Management Policy
- 2.4.19. Personnel Security Policy
- 2.4.20. Data Classification Policy
- 2.4.21. Identification and Authentication Policy
- 2.4.22. Media Protection Policy
- 2.4.23. Information Security Awareness and Training Policy
- 2.4.24. Payment Card Information Security Policy

## 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><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 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, Highly Restricted College Data pursuant to the Data Classification Policy.

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

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

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

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

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

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

**Personally Identifiable Information or PII**—any information about an individual that (i) can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records, (ii) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and (iii) is protected by federal, state or local laws and regulations or industry standards.
**Private College Data**—any College Data classified as Private—Highly Restricted and Private—Restricted pursuant to this policy. By definition, Private College Data includes, but is not limited to, Covered Data and Information, Student Financial Information,Personally Identifiable Information, Student Education Records, Human Subjects Research Data or Other Sensitive Research Data, Protected Health Information, and Sensitive Authentication Data. See the College Data Classification Policy for additional information.

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

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

**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, audit and monitor files/messages on Authorized Users’ assigned computers, mobile devices, and emails;
6. The college reserves the right to take emergency action to safeguard the integrity and security of its 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 incident to the Title IX coordinator. See the college’s Sexual and Gender-Based Misconduct Policy for additional information, including confidential reporting procedures.

V. Withdrawal of Access

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

A partial list of possible factors for termination include:

1. Observance of relevant college policies and associated controls, guidelines, laws, and contractual obligations;
2. The requester’s need to know;
3. The information’s sensitivity;
4. System load;
5. Availability of training;
6. Risk of damage to or loss by the college; and
7. The Authorized User’s previous history of use.

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

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

VI. Use of College Email Systems

A. Access to College Email System(s)

1. Account Creation

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

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

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

2. Account Termination

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

1. Faculty who leave before retirement—full-time faculty who leave before retirement and have not been granted emeritus status 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.
2. Staff who leave before retirement—staff who leave 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. If such separation is for cause, email privileges may be immediately revoked without notice.
3. Retired Faculty—full-time faculty who have retired and/or have been granted emeritus status 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 an email notification to which they must respond, otherwise the account will be subject to deletion.
4. Retired Staff—staff who have retired from the college will have email privileges removed effective on their last worked day. Exceptions for business continuity may be made upon request of the department head and approval by the chief information officer.
5. Volunteers and Guests—volunteers and guest who leave the college will have email privileges removed effective on their last day worked. If such separation is for cause, email privileges may be immediately revoked without notice.
6. Students who leave before graduation—students who leave the college without completion of their degree or other program may keep their email privileges for 180 days from the last term when they were registered.
7. Expelled students—if a student is expelled from the college, email privileges will be terminated immediately.
8. Alumni—students who have graduated from the college will be permitted to retain their email privileges provided their account remains active. All email accounts that are inactive for a period greater than one year are subject to removal and will be referred to setting up their own gmail, yahoo, or other free e-mail service using whatever their NetID had been while attending the college.

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. Conversely, college email should not be used for personal communications.
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 or personal communications 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
2.4.2 Access Control Policy

ACCESS CONTROL POLICY

Effective Date: May 9, 2019

Policy Number: II – 2.4.2


Issuing Authority: President

Responsible Officer: Chief Information Officer

Applicability: All College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data ("applicable information system(s)"), as well as all Authorized Users who access, use, or handle those resources.

History:

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

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 format.

Personally Identifiable Information or PI—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 §265.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

PROCEDURES/GUIDELINES

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

A. Granting of Access

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

Access to forms containing Private College 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 who loan their 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;
1. Each individual granted administrator access receives appropriate security awareness training in accordance with the Information Technology Security Awareness and Training Policy;
2. Each individual granted administrator access must use the account or access privilege most appropriate for the requirements of the work being performed (e.g., Authorized User account vs. administrator account);
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 is generally not allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares). Such exceptions require the approval of the chief information officer and documentation which justifies the need for a shared account:
   a. The password for a shared administrator access account must change under the following conditions:
      i. An individual knowing the password leaves the college or department;
      ii. Job duties change such that the individual no longer performs functions requiring administrator access; and
      iii. A vendor or third-party contractor with administrator account access leaves or completes its work.

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

2. 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;

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

4. 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
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, CA2/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**

I. **Contract Approval Procedures**

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

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

1. The Cloud Computing vendor meets established college data security requirements as set forth in applicable college information security-related policies and conforms to all relevant federal, state and local laws and regulations;
2. The Cloud Computing vendor provides appropriate levels of recovery for Private College Data by the college and not solely by the individual who placed the data in the Cloud Computing environment;
3. The Cloud Computing vendor accepts and is contractually bound to implement the college’s explicit restrictions on storage of Private College Data (i.e., Private College Data must be encrypted in transit and encrypted at rest);
The use of such service, in the judgement of the chief information officer (or his/her designee) does not place the college at an unreasonable risk of experiencing data breach, data loss/non-recovery, or degradation of applicable information systems and College Data.

II. Enforcement

ITS is responsible for the appropriate enforcement of this policy. During the course of any investigation of alleged inappropriate or unauthorized use of cloud computing environment, it may be necessary to temporarily suspend an Authorized User’s network or computing privileges, but only after determining there is at least a prima facie case against the individual, as well as a risk to applicable information 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 other 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>
<tr>
<td>History:</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.

Disposals—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, name, date and place of birth, mother’s maiden name or 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 full-time employees in their area who will receive new computer assets, as will each full-time employee receiving a new computer or device. Each person getting a new asset will have an “allotment” from the replacement budget, sufficient to fund their recommended asset. If a faculty or staff member needs or desires a model that is above the standard amount, the request will need to be justified to vice presidents, deans, and chairs.

IV. Useful Computer Life

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

V. De-accessioning

Please consult the Computer Asset Disposal Policy.

VI. Accessibility

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

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

RELATED POLICIES
- Capitalization and Depreciation Policy
- Configuration Management Policy
- Computer Asset Disposal Policy
- Electronic Accessibility Policy
- Information Technology Change Control Policy
- Procurement Policy and Purchasing Procedures

2.4.6. Electronic Accessibility Policy

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

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

Cardholder Data - full magnetic stripe or the Primary Account Number (PAN) plus any of the following: cardholder name; expiration date; service code; CVC2/CVV2/CID (a three- or four-digit number displayed on the signature panel of the card or, in the case of American Express, on the face of the card. 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. By definition, Private College Data includes, but is not limited to, Covered Data and Information. 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.

Public College Data—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to this policy. By definition, Public College Data includes, but is not limited to, Covered Data and Information. 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.

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
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.

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 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 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

<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY CHANGE CONTROL 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 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—an 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 un tethered 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

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

III. Notification Requirements

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

IV. Accessibility

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

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

V. Additional Acquisition Guidelines

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

A. Requests for Proposals

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

1. Required security capabilities;
2. Required design and development processes;
3. Required test and evaluation procedures; and Required documentation as determined by ITS; and
4. The requirements in the request for proposal must also include text requiring the vendor to update security controls as new threats/vulnerabilities are identified and as new technologies are implemented.
See also the Information Security Program for additional information regarding provisions that must be included in final contracts with service vendors.

B. Information System Documentation

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

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

C. Software Restrictions

Authorized Users are prohibited from installing software on applicable college-owned and leased information system resources that are not approved by ITS. ITS identifies 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>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>
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; to 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—are 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 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 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 PIIP—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 of updates to their installed applications that include the latest vulnerability fixes.

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

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

Student Financial Information—information the college or its affiliates have obtained from a student in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 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 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, password, 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 gifting;
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><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>
**Purpose**

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

**Policy**

It is the policy of Canisius College that anyone who has been issued authentication credentials for an account on any information system that resides at any Canisius College facility, has access to the Canisius College network, or stores any non-public Canisius College information, including both members of the Canisius community, such as faculty, staff, or students, as well as members of third-party organizations granted access to college resources, 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 upper and lowercase letters, 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.
8. Enrollment in Multi Factor Authentication (MFA) is required for Banner Administrative users, otherwise strongly encouraged for all staff/faculty.

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. 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;
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.

For those who have enabled Multi-Factor Authentication (MFA), their passwords will be scheduled to expire one year 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
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 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 college 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> II – 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>
<tr>
<td><strong>History:</strong></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](http://wiki.canisius.edu) for a current listing), ITS provides consulting services, training, documentation, and acts as a technical liaison between Authorized Users and the vendor’s software consultants. Software that is not listed as supported will receive “limited support.” ITS will provide consulting for such software on a time available basis. Please note that ITS does not have the expertise to recommend the statistical methods appropriate for particular data analysis.

IV. Supported Equipment and Computer Repair

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

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

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

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

Authorized Users should 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

<table>
<thead>
<tr>
<th>WIRELESS ACCESS POINTS 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 provide guidelines regarding the installation and use of wireless access points on the college campus.

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

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

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

DEFINITIONS

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

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

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

**College Information System**—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.
**Covered Data and Information**—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 ("GLBA"), including Student Financial Information. 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/CVV2/CID, and PINs/PIN blocks.

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

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

**Wireless Access Point**—a network device that serves as a common connection point for devices in a wireless network. Access points use radio frequency spectrum instead of wired ports for access by multiple users of the wireless network. Access points are shared bandwidth devices connected to the college wired network.

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

**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 other 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

2.4.17. Audit and Accountability Control Policy

<table>
<thead>
<tr>
<th>AUDIT AND ACCOUNTABILITY CONTROL 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 adapt and maintain a formal documented program for the monitoring, management, and review of applicable information systems and associated Authorized User activity.

POLICY
It is the policy of Canisius College to configure applicable information systems to produce, store, and retain audit records for the specific resource and Authorized User activity.

Under the leadership of the chief information officer, applicable resources are routinely reviewed to determine if such resources provide the necessary means whereby the Information Technology Services (“ITS”) may audit and establish individual accountability for any auditable event that can potentially cause access to, generation of, modification of, or affect the release of Private College Data.

**DEFINITIONS**

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

**Audit Event**—any observable occurrence within a College Information System that is significant and relevant to the security of the system and the environment in which it operates in order to meet specific and ongoing audit needs. Audit events include any auditable event required by applicable local, state, and federal laws. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, etc.

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

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

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

**Covered Data and Information**—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.

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

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

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

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

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

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

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

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

**Security Incident**—occurs when there is a serious threat of or unauthorized access or acquisition to a College Information System or an Authorized User’s computerized data that compromises the security, confidentiality, or integrity of the data, including Private College Data. A Security Incident also occurs where there has been unauthorized access or acquisition of encrypted data and the confidential process or key to the encryption is also compromised. Security Incidents can range from the unauthorized use of another Authorized User’s account or system privileges to the execution of malicious code, viruses, worms, Trojan horses, cracking utilities, or attacks by crackers or hackers. Security Incidents may also involve the physical theft of a college information system, a component thereof, or an Authorized User’s technology, such as a computer, mobile device, or other electronic media, or may occur as the result of a weakness in information systems or components (e.g., hardware design or system security procedures).

A non-exhaustive list of symptoms of incidents that qualify as Security Incidents include:

- A system alarm or similar indication from an intrusion detection tool;
- Suspicious entries in a system or network accounting;
- Accounting discrepancies; unexplained new user accounts or file names;
- Unexplained modification or deletion of data; system crashes or poor system performance;
- Unusual time of usage; and
• Unusual usage patterns.

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

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

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

PROCEDURES/GUIDELINES

I. Auditable Events

Information systems designated by ITS as requiring authentication are configured to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact Security Incident investigations.

When resources or technology allows, ITS will configure applicable resources to audit the following additional events:

1. Authorized User identification;
2. Type of event;
3. Date;
4. Timestamp;
5. Logon/logoff;
6. Identity or name of resource/data/system component;
7. All system and data interactions concerning Private College Data, including failed access attempts for operating systems, databases, devices, and applications that collect, process, maintain, use, share, disseminate, or dispose of Private College Data;
8. Administrative access functions, including changes in the status of auditable events;
9. Creation of new accounts and elevation of privileges; and
10. All changes, additions, or deletions to accounts with root or administrative privileges.
11. Change of password;
12. Switching accounts or running administrator access functions from another account;
13. Subset of security administrator commands while logged on in an administrator access role;
14. Subset of system administrator commands while logged on in the Authorized User role;
15. Access to all audit functions;
16. Clearing of the audit log file;
17. Startup, pausing, and shutdown of audit functions;
18. Change of file or Authorized User permissions or privileges;
19. Remote access outside of college network communications channels (e.g., dedicated virtual private network) and all dial-in access to the system;
20. Changes made to an application or database by a batch file;
21. Application critical record changes;
22. Creation and deletion of system-level objects;
23. Changes to database or application records, where the application is bypassed to produce the change (via a file or other database utility); and
24. Additional platform specific events may also be required, based on the outcome of the risk assessment required by the Risk Assessment and Security Policy.

A. Auditable Events Review

Auditable events and review frequencies are documented by ITS. The documentation is evaluated on an annual basis by the chief information officer (or his/her designee) and updates to the audit and accountability program are introduced as necessary.

B. Changes by Authorized Individuals

Only authorized personnel designated by the chief information officer (or his/her designee) are permitted to make changes to the audit system. Changes to the audit system may include adjustments to capture more or less information to comply with investigation requirements, as well as modifications that would facilitate audit reduction, analysis, and reporting.

II. Content of Audit Records

As noted above, applicable information systems designated by ITS as requiring authentication must have the capability to create audit records. ITS is responsible for ensuring that such records contain sufficient information to, at a minimum establish what events occurred, when (date and time) the events occurred, the source of the events, the source of the event, the identity of any user associated with the event, and the event outcome.

Applicable resources may also include additional defined requirements in the audit records for audit events identified by type, location, or subject. An example of detailed information that the college may require in audit records is full-text recording of privileged commands or the individual identities of group account users.

ITS centrally manages the content of audit records, including those records generated by all web servers, database servers, messaging servers, file servers, print servers, middleware servers, DNS servers, routers, firewalls, IDS/IPS, and VoIP servers. Such records are maintained in accordance with the Record Retention Policy and Schedule.

The following information is never included in the audit records maintained by ITS:
1. Unencrypted Private College Data;
2. Session identification values (consider replacing with a hashed value if needed to track session specific events);
3. Access tokens (except nonce URLs that grant limited, specific purpose access);
4. Clear text authentication credentials (e.g., passwords);
5. Database connection strings;
6. Encryption keys; and
7. Information it is illegal to collect in the relevant jurisdiction.

III. Audit Storage Capacity

ITS is responsible for ensuring that applicable information systems requiring authentication have a sufficient amount of storage capacity allocated for audit records. ITS configures such systems to:

1. Reduce the likelihood of audit records exceeding storage capacity; and
2. Allow the records to be maintained for a period as designated by ITS.

When possible, ITS will off-load audit records onto a different information system than the one that is being audited to preserve the confidentiality and integrity of the audit records.

IV. Response to Audit Processing Failures

When possible, applicable information systems requiring authentication shall provide the capability to generate system alerts and send them to appropriate ITS staff in the event of an audit failure or audit storage capacity being reached. In the event of an audit processing failure, when possible, the system will be configured by ITS to shut down or provide limited functionality. ITS will then attempt to remediate logging discrepancies.

V. Audit Review, Analysis and Reporting Authority

Audit records are regularly reviewed and analyzed by ITS staff to identify unauthorized, inappropriate, unusual, suspicious activity, or other Security Incidents (see the Incident Response Policy). Such activities are investigated by ITS staff and reported to the chief information officer, in accordance with the Incident Response Policy.

A. Frequency of Review and Analysis

Assigned ITS staff review audit records for applicable resources and associated components to identify anomalies or suspicious activity as follows:

1. The following audit records are reviewed by ITS at least daily:
   a. All security events;
   b. Logs of all system components that store, process, or that could impact the security of Private College Data;
   c. Logs of all critical system components; and
   d. Logs of all servers and system components that perform security functions. As applicable, this includes, but is not limited to:
      i. Firewalls;
      ii. Intrusion Detection Systems (IDS);
      iii. Intrusion Prevention Systems (IPS);
      iv. Authentication servers (e.g., Active Directory domain controllers); and
      v. E-commerce redirection servers;

2. ITS staff reviews other audit records in accordance with the annual risk assessment (see the Risk Assessment and Security Policy); and
3. ITS staff report exceptions and anomalies identified during the review process to the chief information officer (or his/her designee) and follow up as appropriate.

B. Risk Escalation

If there is an increased risk to operating systems, databases or applications, review and analysis will be performed more frequently. See the Risk Assessment and Security Policy.

C. Integrate Alert Processes

Audit review, analysis, and reporting processes are integrated to support investigations and subsequent responses to suspicious activities.

D. Correlate Audit Repositories

Audit records are analyzed and correlated across different repositories by ITS to gain organizational situational awareness.

VI. Time Stamps

ITS is responsible for ensuring that applicable information systems are configured to use internal system clocks to generate time stamps for audit records. Time stamps generated by the system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

Data Owners must ensure that the time stamps on applicable resources they are responsible for are configured properly and validate the following:

1. The applicable resource is configured to synchronize time with college servers;
2. The applicable resource has the correct and consistent time; and
3. Time data is protected from unauthorized modification.
VII. Audit Information Protection

Audit records are protected from unauthorized modification, access, or deletion while online and during offline storage as follows:

1. Only authorized Data Owners and Custodians with administrative access credentials, as well as select staff from ITS are permitted access to audit logs and audit tools;
2. Audit logs containing Private College Data are encrypted in accordance with the System and Communications Protection Policy;
3. Audit files are protected from unauthorized modifications via the use of Login ID and authentication;
4. ITS is responsible for ensuring that applicable resources are configured to either allow real-time backup or audit the transfer of trail files to a centralized log server or media that is difficult to alter;
5. ITS is responsible for ensuring that applicable resources are configured to write logs for external-facing technologies onto a secure, centralized, internal log server or media devices; and
6. Where feasible, ITS implements File Integrity Monitoring (FIM) or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.

VIII. Audit Record Retention

The college retains audit records for a time sufficient to provide support after-the-fact security investigations as determined by the chief information officer (or his/her designee) and to meet regulatory and applicable college record retention requirements as delineated in the Record Retention Policy and Schedule.

IX. Exception Requests

For details on requesting an exception request to this Policy, please contact the chief information officer.

RELATED POLICIES

Access Control Policy
Acquisition and Disposal Policy
Configuration Management Policy
Data Classification Policy
Incident Response Policy
Information Security Program
Information Technology Configuration Management Policy
Media Protection Policy
Passwords Policy
Payment Card Security Policy
Record Retention Policy
Risk and Security Assessment Policy
System and Communication Protection Policy
System and Information Integrity Policy

2.4.18. Configuration Management Policy

<table>
<thead>
<tr>
<th>CONFIGURATION MANAGEMENT POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effective Date:</strong></td>
</tr>
<tr>
<td><strong>Policy Number:</strong></td>
</tr>
<tr>
<td><strong>Successors:</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 establish baseline configurations for applicable information systems based on the overall needs of the college, as well as to define the need for asset management and change management, which are necessary parts of configuration management.

POLICY

It is the policy of Canisius College to protect the integrity, availability, and security of applicable information systems by adopting standard baseline configuration management practices.

DEFINITIONS

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

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

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

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

Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.

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

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

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

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

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

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

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

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

Sensitive Authentication Data—Full track data (magnetic strip data or equivalent on a chip, CAV2/CVC2/ 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. Baseline Configurations

All applicable information systems at Canisius College shall have a formal, documented baseline configuration. This configuration is maintained by
Information Technology Services ("ITS").

Baseline configurations at the college include, at the minimum, the following:

1. System components, such as standard software packages installed for workstations, servers, college-owned or leased Mobile Devices, etc.;
2. Current version numbers of operating systems and software applications;
3. Current patch information;
4. Configuration settings and parameters;
5. College Network topology; and
6. Placement of hardware within the applicable information system architecture.

A. ITS Responsibilities

In establishing baseline configurations, ITS:

1. Identifies, documents, and applies more restrictive security configurations information systems that store or permit access to Private College
Data, as necessary;
2. Maintains records that document the application of baseline security configurations;
3. Monitors systems for security baselines and policy compliance;
4. Reviews and revises all security configuration standards annually, or more frequently, as needed;
5. Reapplies all security configurations to systems, as appropriate, when the system undergoes a material change, such as an operating system
upgrade;
6. Modifies individual system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the
results of vulnerability scanning;
7. Requires creation and periodic review of a list of hardware and software assets;
8. Reviews and updates the baseline configuration of all information system:
   a. Once a year at a minimum;
   b. When required due to a significant configuration change or a demonstrated vulnerability; and
   c. As an integral part of information system component installations and upgrades;
9. Develops and maintains a college-defined list of software programs authorized to execute on the information system;
10. Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system; and
11. Maintains a baseline configuration for development and test environments that are managed separately from the operational baseline
configuration.

B. Record Retention

Previous baseline configurations shall be retained by ITS in accordance with college record retention requirements.

C. Baseline Exceptions

For exceptions to a baseline configuration, please contact the director of user services for desktop and mobile devices, or the director of infrastructure for
servers and network infrastructure..

II. Configuration Change Control

ITS staff coordinates and the chief information officer approves configuration change control activities. Data Owners and Custodians must obtain approval
prior to implementation of changes that affect security on a college information system.

ITS documents and implements configuration management so that changes to an information system environment does not compromise security controls.
Specifically, ITS:

1. Determines the types of changes to the information system that are configuration controlled;
2. Obtains approval from the chief information officer (or designee) for all configuration-controlled changes to the system with explicit consideration
for security impact analyses (see Section III below);
3. Documents approved configuration-controlled changes to the system;
4. Tests and validates changes to the information system before implementing the changes on the system. In conducting tests, ITS:
   a. Utilizes separate environments for development/testing/staging and production;
   b. Utilizes a separation of duties between development/testing/staging and production environments;
   c. Removes test data and accounts before production systems become active / goes into production.
5. Documents changes to the information system as follows:
   1. The impact of the change;
   2. The administrator(s) who approved the change;
   3. The results of functionality testing; and
III. Security Impact Analysis

ITS analyzes changes to the information system to determine potential security impacts prior to change implementation. Security impact analyses are conducted by ITS staff with information security responsibilities. Personnel conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications.

Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system.

IV. Access Restrictions

Access restrictions for configuration change assist in preventing any unauthorized changes to the hardware, software, and/or firmware components of the information system and reduce the potential for significant effects on the overall security of the system.

Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized ITS staff are permitted to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the college become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries.

Examples of access restrictions include, for example, physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other control policies (i.e., Access Control and Audit and Accountability policies). For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes.

V. Configuration Settings

Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections.

ITS:

1. Establishes and documents mandatory configuration settings for information technology products employed within the information system;
2. Changes vendor default passwords and other vendor default settings prior to system implementation in order to prevent a system from being compromised by malicious individuals making use of standard configuration parameters;
3. Implement configuration settings;
4. Identifies, documents, and receives approval from chief information officer for all exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
5. Monitors and controls changes to the configuration settings.
   a. As required, ITS will assess the as-built configurations of all servers and network components against the configuration database and investigate and resolve any discrepancies;
   b. This monitoring can be accomplished either manually or using software tools specifically for this purpose; and
   c. Firewall and router rule sets are reviewed on a regular basis.

See the System and Communications Protection Policy for applicable configuration setting requirements.

VI. Component Inventory

An accurate and frequently updated inventory of information system components is vital to maintain the integrity and security of the information system. Accordingly, ITS develops, documents, and maintains a current inventory of each information system's components and relevant ownership information. The inventory is available for review and audit.

VII. Exception Requests

For details on requesting a Configuration Management Policy exception request, please contact the chief information officer.

RELATED POLICIES

Access Control Policy
Acquisition and Disposal Policy
Audit and Accountability Control Policy
Cloud Computing Policy
Confidential Information Policy
2.4.19. Personnel Security Policy

PURPOSE

The purpose of this policy is to implement appropriate safeguards to ensure Authorized Users granted access to College Information Systems and Private College Data have been properly vetted.

POLICY

It is the policy of Canisius College to limit access to College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data ("information systems") to Authorized Users that are trustworthy and meet established security criteria and to ensure that such information systems are protected during and after personnel actions such as terminations and transfers.

DEFINITIONS

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

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

College Employees—including 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 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 customer 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, Car De-identified Data, and Sensitive Authentication Data. See the Data Classification Policy for additional information.

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

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

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

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

**PROCEDURES/GUIDELINES**

**I. Personnel Screening**

Prior to Information Technology Services (“ITS”) granting access authorization via a unique Login ID to an Information Service to an Authorized User, the individual must be screened in accordance with the following procedures:

1. In accordance with the Background, Reference, and Verification Screen Policy, screens of new employees working in areas that regularly work with Private College Data are conducted by Human Resources prior to the Data Owner and supervisor authorizing ITS to issue a unique login ID to the information service;
2. If the Data Owner and supervisor agree that the individual has a favorably adjudicated background screen commensurate with the defined position sensitivity levels, a request for access will be submitted electronically by the supervisor to bannersecurity@canisius.edu;
   a. ITS then creates the login ID and assigns the level of access to the new Authorized User. Only the requested and approved access that is specific to an Authorized User’s responsibilities will be granted by ITS;
   b. ITS will maintain a list of all information systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data for each unit, as well as unit personnel granted access to those resources;
3. The Authorized User’s supervisor will advise the Authorized User to follow all terms of use, including applicable college policies and associated controls; and
4. The new Authorized User will receive appropriate training to comply with all terms of use and policies and controls associated with the resource.

Note: Individuals must be rescreened if the length of employment separation exceeds 90 days.

**II. Employee Termination**

Upon termination of individual employment:

1. Access to an information system will be removed by ITS immediately upon termination of employment or, in the case of a vendor or other third-party, cessation of the individual’s engagement with the college.
In the event that the access privilege is to remain active after a voluntary termination (e.g., extended electronic mail access), the supervisor must document that a need or benefit to the college exists;

2. All security-related property will be retrieved by the user’s supervisor (e.g., hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes);

3. Prior to archiving or permanent disabling the individual’s account, the user’s supervisor will ensure that all Private College Data is transferred to appropriate personnel or archived; and

4. ITS will confirm that the following activities have been performed upon termination of employment or, in the case of a vendor or other third-party, cessation of the individual’s engagement with the college:
   a. Lock the computer accounts and access control and after a specified time period delete them.
   b. Update access control lists, mailing lists, etc.;
   c. Collection of all keys/access cards, badges, and similar items; and
   d. Electronic data records are accessible and properly secured, filed, or appropriately disposed.

III. Employee Transfer

Access authorizations are modified appropriately by ITS as an Authorized User’s job responsibilities change due to a transfer as follows:

1. Access authorizations to information services are reviewed by the appropriate Data Owner and supervisor when Authorized Users are reassigned or transferred to other positions within the college.
   a. The actions undertaken are driven by the individual’s new position duties in accordance with the Access Control Policy;

2. ITS, upon being notified of the transfer by the Authorized User’s new supervisor or Human resources, performs the following activities for all Authorized Users, including third-party contractors, upon employee reassignment or transfer:
   a. Locks all Login ID’s;
   b. Updates access control lists;
   c. Confirms that electronic data records are accessible and properly secured, filed, or appropriately disposed;
   d. Closes previous information system accounts unless the original Data Owner and the new Data Owner carefully review the account to ensure that no resources or access privileges are left on the account and the account has only the resources and privileges appropriate to the person’s new role and responsibilities;
   e. Updates the Authorized User’s access privileges;
   f. Reviews and updates the individual’s access privileges and authorizations to ensure alignment with the new position on the effective date; and

3. The employee’s former supervisor, in collaboration with Human Resources, is responsible for:
   a. The collection old keys/access cards, identification cards, authentication tokens, etc., as appropriate; and
   b. As appropriate, confirming that new keys/access cards, identification cards, authentication tokens, etc. have been issued.

4. The above is initiated immediately upon being notified of the formal transfer action.

IV. Name Changes and Permission Changes

It is the responsibility of the supervisor to notify ITS whenever an Authorized User account must be modified to accommodate name changes or permission changes. In the event of permission changes, the procedures set forth in Section III above will be followed.

V. Third-Party Contractors

Third-Party contractors and vendors providing services to the college must possess the same level of security clearance as a college employee to access the same information system or College Data. The applicable vice president or supervisor overseeing the contract is responsible for making sure all current and future contracts include personnel security requirements.

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
Cloud Computing Policy
Data Classification Policy
Identification and Authentication Policy
Information Security Program
Information Technology Personnel Security Policy
Information Technology Security Awareness and Training Policy
Health Insurance Portability and Accountability Act Policy
Mobile Device Use and Support Policy
Password Policy
Payment Card Information Security Policy
Physical and Environmental Protection Policy
Record Retention Policy and Schedule

2.4.20. Data Classification Policy
PURPOSE

The purpose of this policy is to provide a framework for classifying College Data based on its level of sensitivity, value, regulatory requirements, and criticality to the college. Classification of data will aid in determining baseline security policies and corresponding controls for the protection of College Data.

POLICY

It is the policy of Canisius College to maintain College Data in a secure, accurate, and reliable manner and to make it readily available for authorized use. Data security controls at the college are implemented commensurate with data value, sensitivity, and risk.

Members of the college community designated as Data Owners are responsible for evaluating and classifying College Data for which they are responsible according to the classification system adopted by the college and described below. If College Data of more than one level of classification exists in the same collection of data, such data must be classified at the highest level of classification. Data Owners must communicate the data security classifications and associated security controls to Data Custodians and Authorized Users granted administrative access to such data.

Data Custodians and Authorized Users must (i) understand the college’s data classifications; (ii) consider how these classifications apply to College Data under their control; (iii) implement the security controls for each classification as specified by applicable college and departmental policies; and (iv) consult with the applicable Data Owner or Information Technology Services (“ITS”) regarding circumstances that may warrant the application of higher security standards.

DEFINITIONS

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

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

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

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

**Covered Data and Information**—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.

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

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

**Members of the College Community**—includes any person who is a student, college employee, volunteer, trustee, alumni, as well as college organizations, clubs, groups, and teams. This definition also includes all college departments, offices and programs.
Non-Public Personal Information—any personally identifiable financial or other personal information, not otherwise publicly available, that the college has obtained from a customer in the process of offering a financial product or service; such information provided to the college by another financial institution; such information otherwise obtained by the college in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, date and place of birth, mother’s maiden name, biometric records, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

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

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

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

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

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

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

PROCEDURES/GUIDELINES

I. Data Classification Categories

Data classification, in the context of data security, is the classification of data based on its level of sensitivity and the impact to the college should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All College Data must be classified into one of three sensitivity levels, or classifications:

A Private-Highly Restricted

Private-Highly Restricted College Data is College Data that is not Public and is available within the college only to those with a legitimate need to know and are so highly sensitive that the loss of confidentiality of the data could either (a) cause significant personal, college, or other harm or (b) a law, regulation or contract require a high degree of security.

Examples of Private-Highly Restricted College Data include, but is not limited to:

1. Personally Identifiable Information or PII: any information about an individual that:
   a. Can be used to distinguish or trace an individual’s identity, such as name, date and place of birth, mother’s maiden name or biometric records
   b. Is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual; and
   c. Is protected by federal, state or local laws and regulations or industry standards;
2. Student Education Records: as defined by the Family Educational Rights and Privacy Act (FERPA), student education records are all records which contain information directly related to a student and maintained by the college, including those files, documents, and other materials (in handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche) that contain information directly related to a student which are maintained by the college or by a person acting for the college pursuant to college or departmental policy. Information that is captured as a result of a student’s various activities at the college is part of the student record. This information includes, but may not be limited to, logs, databases or other records of: websites the student has visited, purchases made at college facilities, entry day/time into college facilities, library use and biometric records;
3. Covered Data and Information within the meaning of Title V of the Gramm Leach Billey Act of 1999 (Public Law 106-102, 11 Statute 1338) (as amended) and its implementing regulations;
4. Human Subjects Research Data or Other Sensitive Research Data;
5. Protected Health Information (“PHI”): As defined by Health Insurance Portability and Accountability Act (HIPAA), PHI is information, whether oral or recorded in any form or medium, that: is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university; and relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past present or future payment for the provision of health care to an individual; and includes demographic data, that permits identification of the individual or could reasonably be used to identify the individual;
6. Payment Card Information: as regulated by the Payment Card Industry Data Security Standard (PCI DSS), payment card information is defined as Cardholder Data or Sensitive Authentication Payment Data:
   a. Cardholder Data - full magnetic stripe or the Primary Account Number (PAN) plus any of the following: cardholder name; expiration date; service code; CVC2/CVV2/CID (a three- or four-digit number displayed on the signature panel of the card or, in the case of American Express, on the face of the card; and
   b. Sensitive Authentication Data—magnetic strip data or equivalent on a chip, CAV2/CVC2/CVV2/CID, and PINs/PIN blocks;
Note: Canisius College does not store cardholder data in any of its information systems. Cardholder data is stored by third-party vendors, which are contractually obligated to comply with the PCI DSS.

1. An Authentication Verifier: any piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some rare instances, an Authentication Verifier may be shared amongst a small group of individuals. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include passwords and cryptographic private keys;
2. Export Controlled Materials: any information or materials that are subject to United States export control regulations including, but not limited to, the Export Administration Regulations ("EAR") published by the U.S. Department of Commerce and the International Traffic in Arms Regulations ("ITAR") published by the U.S. Department of State;
3. Federal Tax Information: any return, return information or taxpayer return information that is entrusted to the college by the Internal Revenue Services;
4. Passport and social security numbers; and
5. Legal investigation records conducted by the college.

Unauthorized access to, or disclosure of, Private-Highly Restricted College Data will generally require notification to affected parties under the guidelines of state and federal breach notification laws or applicable contract provisions.

B. Private-Restricted

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

Examples of Private-Restricted College Data include, but is not limited to:

1. Student Directory Information (if student has requested non-disclosure (suppressed): name, address, email address, telephone/mobile device number, dates of enrollment/registration, enrollment/registration status, major, adviser, college/school, class, academic awards and honors received, and degree received;
2. Linking a library patron’s personal identity with materials requested or borrowed by the person or with a specific subject about which the person has requested information or materials;
3. Exam questions or answers;
4. Human Resources employment data;
5. Law enforcement investigation data, judicial proceedings data; includes student disciplinary or judicial action information;
6. Information Technology infrastructure data;
7. Trade secret data;
8. Protected data related to research;
9. College intellectual property;
10. College proprietary data;
11. Data protected by external non-disclosure agreements;
12. Inter- or intra-agency data which are not: statistical or factual tabulations; instructions to staff that affect the public; final agency policy or determination; external audit data;
13. A student or employee college identification card number;
14. Licensed software;
15. Information created by a health care provider and used or maintained for the purposes of patient treatment, patient payment, or health care provider operations that is not regulated by HIPAA.

C. Public College Data

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

Examples of Public College Data include, but is not limited to:

1. General access data on a college webpage;
2. Student Directory Information (if student has not requested non-disclosure (suppressed): name, address, email address, telephone/mobile device number, dates of enrollment/registration, enrollment/registration status, major, adviser, college/school, class, academic awards and honors received, and degree received;
3. Employee Directory/Contact Information (not designated by the owner as private): name, addresses (campus and home), email address, listed college telephone and mobile device number(s), dates of current employment, and position(s);
4. Campus maps, job postings, press releases, course information, research publications, newsletters, newspapers and magazines.

II. Reclassification of College Data

Data Owners should periodically reevaluate information classifications to ensure the delegated classification is still appropriate. Changes to laws and rules, contractual obligations, or how certain information is used can result in modification to the information’s value to the college and its classification.

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
Access Control Policy
Audit and Accountability Control Policy
Cloud Computing Policy
Confidential Information Policy
Configuration Management Policy
2.4.21. Identification and Authentication Policy

IDENTIFICATION AND AUTHENTICATION POLICY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>May 6, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number:</td>
<td>II- 2.4.21</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Issuing Authority:</td>
<td>President</td>
</tr>
<tr>
<td>Responsible Officer:</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Applicability:</td>
<td>All College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data (&quot;applicable information system(s)&quot;), 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 provide identification and authentication requirements for applicable information systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data. A comprehensive and well-defined identification and authentication policy and associated controls are necessary to maintain secure information systems.

POLICY

It is the policy of Canisius College to protect information systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data from unauthorized access. Unauthorized access to such systems can potentially lead to modification, disclosure, or destruction of the resource and the Private College Data contained on the resource.

All Authorized Users of applicable information systems are assigned a unique identity to securely authenticate to the systems that they have been authorized to access. Access to such systems is authorized based on the principle of least privilege. This means that an Authorized User is given the minimum access level to a given resource in order to perform assigned job duties. Each Authorized User must use the user’s unique account and password (or other authenticator) when logging into a system the user has been authorized to access.

Applicable information systems are audited by the Information Technology Services (“ITS”) for appropriate login data. Should a resource containing Private College Data become compromised, the Authorized User who was logged in at the time of the compromise will be contacted by ITS for information regarding any investigation. Unauthorized or improper access to any information system that collects, processes, maintains, uses, shares, disseminates, or disposes of Private College Data is subject to disciplinary action.

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

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

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

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

Covered Data and Information—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 ("GLBA"), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

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

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

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

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

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

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

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

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

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

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

PROCEDURES/GUIDELINES

I. Identification and Authentication of College Authorized Users

Authorized Users must be uniquely identified and authenticated to access College Information Systems that collect, process, maintain, use, share, disseminate or dispose of Private College Data. Accordingly, ITS configures applicable systems to uniquely identify and authenticate Authorized Users of the system.

Authentication of Authorized User identities at the college is accomplished primarily through the use of passwords. For some resources, PINS/tokens, biometrics, or multifactor authentication, or some combination thereof with passwords may be utilized.

II. Identifier Management

ITS manages Authorized User identifiers as follows:
ITS assigns a unique login ID to all Authorized Users as appropriately authorized upon hiring or transfer in accordance with the granting of access procedures set forth in the Access Control Policy; Login IDs are unique to each Authorized User and the reuse or sharing of a login ID is prohibited (see the Password Policy); ITS uses the login ID that has been assigned as the Authorized User’s unique identifier throughout the Authorized User’s employment or association with the college; The reissuance of a user Login ID number by ITS is prohibited for the period up to three years after the account has been deleted; and Applicable information systems are configured by ITS to disable a login ID after 90-days of inactivity.

See also the Access Control and Information Technology Security Personnel Security policies.

III. Authenticator Management

ITS, in collaboration with applicable Data Owners, Data Custodians, and employee supervisors, manages information system authenticators (i.e., passwords, keys, tokens, Public Key Infrastructure (PKI) certificates, biometrics) by:

1. Verifying, at the time of issuance of the login ID, the identity of the Authorized User receiving the initial authenticator (see the Information Technology Personnel Security Policy);
2. Issuing an initial password (or other authenticator as applicable to the Authorized User);
3. Ensuring that the initial password (or other authenticator as applicable) has sufficient strength;
4. Enforcing the procedures set forth in the Password Policy for initial password distribution, for lost/compromised or damaged passwords, and revoking passwords;
5. Changing the default content of passwords/authenticators upon information system installation in accordance with the System and Communications Protection Policy:
   a. Default passwords provided for initial entry to a system are changed by ITS staff before implementation of the information system or component (e.g. routers, switches, firewalls, printers, workstations, servers);
   b. ITS staff confirm that software and/or hardware upgrades, updates, and patches have not reinstalled default passwords;
6. Enforcing the minimum and maximum password lifetime restrictions and reuse conditions for authenticators. For password restrictions and reuse, see the Password Policy;
7. Requiring that Authorized Users change/refresh passwords every six months (for Authorized User-level access);
8. Protecting authenticator content from unauthorized disclosure and modification by adhering to the following requirements:
   a. Having passwords (other than initial) be chosen by Authorized Users as opposed to being assigned by ITS staff;
   b. Access to files containing passwords or password hashes are limited to the information system and its Data Owner.
9. Requiring Authorized Users to take specific measures to safeguard authenticators:
   a. Passwords must be safeguarded in accordance with the Password Policy;
   b. Devices must be configured to safeguard authenticators (e.g., certificates, passwords);
10. Configuring applicable resources, for password-based authentication, to enforce the controls set forth in the Password Policy;
11. Requiring that Authorized Users be trained on the password construction guidelines set forth in the Password Policy;
12. Requiring that forgotten initial passwords be replaced rather than reissued in accordance with the Password Policy;
13. Ensuring that passwords are not included in any type of batch login file, clear text file, script or procedure:
   a. The use of an “auto-login” feature to automatically log a computer onto the college network is strictly prohibited, unless the system is functioning as a kiosk;
14. Requiring passwords to be set on device management user interfaces for all college network-connected devices; and
15. Documenting and storing hardware passwords securely.

IV. Password Feedback

In accordance with the Password Policy, passwords must be masked upon entry by Authorized Users (e.g., displaying asterisks or dots when a user types in a password) and not displayed in clear text. This requirement helps protect information from possible exploitation or use by unauthorized users.

V. Cryptographic Authentication

ITS configures its information systems to use mechanisms for authentication to a cryptographic module.

VI. Identification and Authentication of Non-College Users

ITS configures applicable resources to uniquely identify and authenticate non-organizational users (i.e., special access users) in accordance with the controls set forth in the Access Control Policy.

VII. Exception Requests

For details on requesting an Identification and Authentication Policy exception request, please contact the Chief Information Officer.

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy
Access Control Policy
Audit and Accountability Control Policy
Data Classification Policy
Configuration Management Policy
Information Security Program
Information Technology Personnel Security Policy
Information Technology Security Awareness and Training Policy
2.4.22. Media Protection Policy

**MEDIA PROTECTION POLICY**

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>May 6, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number:</td>
<td>II-2.4.22</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 media containing Private College Data, as well as all Authorized Users who access, use, or handle associated media containing Private College Data.</td>
</tr>
<tr>
<td>History:</td>
<td></td>
</tr>
</tbody>
</table>

**PURPOSE**

The purpose of this policy is to provide guidance for protecting and sanitizing Media at the college. Media protection is critical for securing the confidentiality of Private College Data by guarding the data from unauthorized access and disclosure throughout the lifetime of the Media.

**POLICY**

It is the policy of Canisius College to employ Media protection controls to prevent improperly managed media from becoming the source of unauthorized access to any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to the Data Classification Policy. The college controls address Media access concerns throughout the Media lifecycle, from secure use, storage, transportation, and ultimately destruction.

**DEFINITIONS**

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

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

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

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

*Covered Data and Information*—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 (“GLBA”), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

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

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

*DeGaussing*—demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.

*Disintegration*—a physically destructive method of sanitizing data; the act of separating into component parts.

*Incineration*—a physically destructive method of sanitizing media; the act of burning completely to ashes.

*Media*—includes, but is not limited to, paper, hard drives, random access memory (RAM), read-only memory (ROM), disks, flash drives, memory devices, phones, Mobile Devices, networking devices, and all-in-one printers.
Media Sanitization—the process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

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

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

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

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

Private College Data—any College Data classified as Private-Highly Restricted and Private-Restricted pursuant to this policy. By definition, Private College Data includes, but is not limited to, Covered Data, 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.

Pulverization—a physically destructive method of sanitizing media; the act of grinding to a powder or dust.

Purging—a media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting (i.e., a "laboratory attack"), exceeds the value to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

Removable Media—devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and software disks not provided by the college.

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

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

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

PROCEDURES/GUIDELINES

I. Media Access

Access to digital media (e.g., disks, magnetic tapes, external/removable hard drives, flash drives) and non-digital media (e.g., paper, microfilm), when either type of media contains Private College Data, is restricted to Authorized Users in accordance with the controls set forth in the Access Control, Identification and Authentication, Physical and Environmental Access, and Use of Mobile Devices policies [INSERT LINKS].

II. Media Storage

The college physically and logically protects media containing Private College Data while at rest, stored, or actively being accessed as follows:

1. Media back-ups are stored in a secure location designated by ITS, and this location’s security is reviewed on a monthly basis as part of the risk assessment process.
   a. 
2. ITS ensures the inventorying of media containing Private College Data at least annually.
3. Data Owners, Data Custodians, and Unit Managers ensure that their units physically and logically protect media containing Private College Data while at rest, stored, or actively being accessed in accordance with the media storage guidelines set forth below, as well as the controls identified in the Access Control, Identification and Authentication, Physical and Environmental Access, System and Communication Protection, and Mobile Device Us and Support policies [INSERT LINKS].
   a. It is the responsibility of Authorized Users of media containing Private College Data to ensure appropriate media storage guidelines (see below) are in place and followed.

Media Storage Guidelines
Media storage guidelines to follow include:

1. Utilizing appropriate FIPS-validated encryptions to protect Private College Data from unauthorized exposure while at rest in accordance with the System and Communications Protection Policy [INSERT LINK];
2. Adhering to the physical security control guidelines set forth in the Physical and Environmental Access Policy [INSERT LINK];
3. Securing electronic and paper containing Private College Data by:
   a. Storing the Private College Data in a secure manner (i.e., File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Private College Data are to be locked when not in use etc.);
   b. Accessing or viewing the Private College Data electronically or via document printouts in a physically secure location;
   c. Not leaving hard copy printouts containing Private College Data out in public view when not in use;
   d. Erasing whiteboards, dry-erase boards, writing tablets, etc. containing Private College Data when in not in use;
   e. Immediately retrieving hard copy printouts from a printer when printed; and
   f. Immediately retrieving hard copies from a copying machine when making extra copies.

B. Media Transport

Data Owners, Data Custodians, and supervisors are responsible for ensuring that their units protect and control media during transport outside of controlled areas on campus, and restrict the pickup, receipt, transfer and delivery of such media to only Authorized Users.

Units are required to control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents;
2. Limiting the collection, disclosure, sharing, and use of Private College Data; and
3. Following the least privilege and role-based rules for allowing access (see the Access Control Policy [INSERT LINK]).

It is the responsibility of Authorized Users transmitting Private College Data to ensure appropriate risk mitigation measures are in place to protect such data from unauthorized exposure. Guidelines to follow include:

1. Ensuring they have their supervisor’s approval prior to transmitting media (including when media is distributed to individuals) classified as Private-Highly Restricted;
2. Packaging hard copy printouts for physical transport in such a way as to not have any Private College Data information viewable;
3. When mailing or shipping, send by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery;
4. Encryption must always be used to protect Private College Data transmitted over data networks to protect against risks of interception. This includes when accessing network services which require authentication (for example, usernames and passwords) or when otherwise sending or accessing Private College Data (for example, in electronic mail);
5. Where Private College Data is stored on or accessed from Mobile Devices (for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders), the devices themselves must be encrypted (using “full disk” encryption), irrespective of ownership:
   a. When traveling with Mobile Devices containing Private College Data, or using them in public places, appropriate physical security precautions must be taken to prevent loss, theft, damage, or unauthorized access. Use of tracking and recovery software on applicable Mobile Devices is encouraged.
   b. Authorized Users must be aware that government agencies in any country may require a device or files to be decrypted on entry or exit from the country. If travelling abroad with encrypted Private College Data, this means that there is a risk that the data may have to be disclosed. Wherever possible, Data Owners should not permit Private College Data to be taken abroad.
6. Where Private College Data is transmitted for storage in a public, cloud-based storage facilities, the data must be encrypted prior to storing to ensure that it is not possible for the cloud service provider to decrypt the data (see the Cloud Computing Policy) [INSERT LINK]; and
7. Where peer-to-peer or instant messaging is used to transmit Private College Data, traffic flows between peers must be encrypted and access only allowed to manage instant messaging servers that provide gateways to public services.

III. Media Sanitization

It is the policy of the college to sanitize media prior to disposal, release outside of college control, or release for reuse. This applies to all system media, both digital and non-digital, and whether or not the media is considered removable.

While the primary purpose of this policy is to protect Private College Data, it is often very difficult to separate these classifications on the media or determine conclusively that remnants of Private College Data are not recoverable. Therefore, it is often most expedient and cost effective to purge all College Data from the media before reuse or disposal rather than try to selectively sanitize the Private College Data.

Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. If physical destruction is contracted to a third party outside the college, that third party must hold certifications for destruction of media and must provide the college with written guarantee that the media was destroyed.

A. Sanitization and Destruction Guidelines

Data Owners, in conjunction with Data Custodians and supervisor, are responsible for ensuring that the sanitization and destruction guidelines below are adhered to by their respective units:

1. Paper Media

Data Owners, in conjunction with Data Custodians, supervisors, and Authorized Users, are responsible for ensuring that all paper media under their control is destroyed after the appropriate retention period has expired (see the Records Retention Policy and Schedule) [INSERT LINK] and provided the department does not need the records for legal, research, or other valid purpose. Paper Media may be destroyed as follows:

   a. Any paper-based or other hard copy media containing Private College Data must be shredded with a cross-cut shredder before disposal or transferred to the authorized third party contracted by the college for secure disposition of documents.
   b. Incineration and/or recycling by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media.

2. Electronic Storage Media
All electronic storage media, such as hard disk drives in computers, copiers, external hard drives, USB flash drives, magnetic tapes, etc. containing Private College Data in electronic form must be sent to ITS for sanitization prior to disposal, release outside of college control, or release for reuse.

ITS will sanitize Private College Data from the media utilizing a method that will ensure data recovery is impossible, such as purging, degaussing, or destroying the media utilizing a destruction method that will be able to withstand a laboratory attack (e.g., shredding, disintegration, pulverization, melting or incineration). If purging is done by overwriting the data, the entire media/device will be overwritten with a minimum of three passes.

Equipment that has stored Private College Data and is leaving the control of the college permanently must have all data storage devices removed by ITS before disposition. If the equipment leaving college control must retain the data storage devices, all Private College Data must be properly purged. When a vendor is contracted to service a media device, any hardware requiring replacement must be reset to factory default and all data must be sanitized.

3. Optical Media

Optical media (e.g., CDs and DVDs) containing Private College Data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

5. Mobile Devices

Pursuant to the Use of Mobile Devices Policy [INSERT LINK], all Mobile Devices, regardless of whether the device is college-issued, that have been used to store, access and/or process Private College Data must be wiped to remove such data before they are transferred to someone else through sale or gifting or otherwise disposed of. It is also advisable to purge all other data from the device before reuse or disposal to protect the user’s PII.

B. Secure Storage

Media containing Private College Data that is waiting to be destroyed must be securely stored.

C. Tracking and Documentation

ITS reviews, approves, tracks, documents and verifies college media sanitization and disposal actions. Tracking and documentation actions may include, but are not limited to:

1. Date of decommission of the item.
2. Description of items and serial numbers;
3. Inventory numbers;
4. Process and sanitization tools used; and
5. The name and address of the organization the equipment was transferred to, if transferred.

C. Record Retention

Prior to requesting the destruction of storage media, Data Owners are responsible for transferring data required to be retained based on established records retention requirements in the Records Retention Policy and Schedule. [INSERT LINK]

IV. Management of Removable Media

All users of an information system are encouraged to never store Private College Data on removable media, however Authorized Users of an information system may use Removable Media in their work computers if it is unavoidable. Private College Data may be stored on Removable Media only when required in the performance of assigned duties or when responding to legitimate requests for information. When Private College Data is stored on Removable Media it must be encrypted.

Users are encouraged to contact ITS to discuss storage of Private College Data on removable media to attempt to discover alternate solutions.

V. Exception Requests

For details on requesting a Media Protection Policy exception request, please contact the chief information officer.

VI. Enforcement and Sanctions

ITS is responsible for the appropriate enforcement of this policy.

Individuals who violate the provisions of the policy are subject to disciplinary action pursuant to applicable disciplinary policies, as well as loss of access to applicable information systems. They may also be subject to criminal and/or civil proceedings.

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

RELATED POLICIES

Access Control Policy
Acquisition and Disposal Policy
Audit and Accountability Policy
Cloud Computing Policy
Confidentiality of Employee Records Policy
Confidentiality of Student Records Policy
PURPOSE
The purpose of this policy is to provide guidance in developing and implementing appropriate training regarding the protective policies and associated controls in place at the college that support the confidentiality, integrity, and availability of applicable information systems and College Data.

POLICY
It is the policy of Canisius College to provide information security awareness education to all Authorized Users of College Information Systems that collect, process, maintain, use, share, disseminate or dispose of College Data.

Authorized Users granted access to Private College Data are adequately trained to perform their information security-related duties and responsibilities consistent with related college policies, legal requirements, regulations, and agreements. The chief information officer, ITS, and the SSC work in cooperation with Human Resources to develop training and education programs for all employees who have access to Private College Data, reviews the information security awareness program annually and appropriate updates are applied based on the findings of the annual reviews. Directors and supervisors are ultimately responsible for ensuring compliance with information security policies and associated control.

DEFINITIONS

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

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

College Employees—including Canisius College executive officers, administrators, faculty, staff, student employees, contractors, and others who act on behalf of the college.
**College Information System**—a set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The term system is used throughout this policy to represent all types of computing platforms that can process, store, or transmit College Data.

**Covered Data and Information**—means all Non-Public Personnel Information of customers required to be protected under the Title V of the Gramm Leach Bliley Act of 1999 ("GLBA"), including Student Financial Information. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the Data Classification Policy.

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

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

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

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

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

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

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

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

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

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

**PROCEDURES/GUIDELINES**

I. **General Training**

A. **Employee Training**

During employee orientation, each new employee to be granted authenticated access to Private College Data receives general training on the importance of confidentiality of Private College Data, actions needed to be taken to maintain security, information on how to respond to suspected security incidents, and the need for physical operations security.

Specific topics addressed include, but are not limited to:

1. The proper use of College Data and passwords;
2. A review of policies and associated controls in place at the college to prevent employees from providing College Data to an unauthorized individual, (i.e., training on appropriate use of encryption use, etc.);
3. A review of physical security policies and controls to protect Private College Data;
4. How to properly dispose of documents that contain College Data in accordance with the Record Retention Policy and Schedule; and
5. Protecting College Data from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

General training will be conducted when required by system changes.

As a supplement to the training programs listed above, general employee education is also attained through regular electronic mails sent by ITS, as well as Social Media postings that highlight relevant information technology security topics. ITS also provides one-on-one training upon request. Users of the administrative information systems of the college who do not participate in any required training are subject to loss of their access privileges.

Collectively, the above general training efforts help minimize risk and safeguard College Data.
2. **Student Training**

ITS provides students with general information security education. This material is made available on the ITS Website.

II. **Administrator Account Training**

The end user department delivers specific role-based training for individuals authorized to use administrator access accounts prior to them receiving privileged access. ITS resources are available to assist in this end user training as needed. This training is documented and archived by the end user department and includes, but is not limited to the following topics:

1. Each individual that uses administrator access accounts is trained to use the account or access privilege most appropriate for the requirements of the work being performed (e.g., Authorized User account vs. administrator account);
2. Each individual that uses administrator access accounts will receive training regarding abuse of privilege:
   a. Investigations conducted by individuals that uses administrator access accounts shall be conducted as directed by the chief information officer, after consultation with the area vice president of the college.
   b. In those cases where law enforcement agencies request access in conjunction with an investigation, the request must be presented in writing (e.g., subpoena, court order). All individuals that use administrator access accounts that receive such a written request must report the matter to the chief information officer, who will consult with the area vice president of the college before any action is taken.
3. The password for a shared administrator access account must change under the following conditions:
   a. An individual knowing the password leaves the college or department;
   b. Job duties change such that the individual no longer performs functions requiring administrator access; and
   c. A third-party contractor or vendor with role account access leaves or completes the contracted work.
4. A password escrow must be in place for all administrative accounts to enable someone other than the custodian to gain access to the system in an emergency.

Administrative access training is reviewed by the end user department supervisor, upon necessary system changes, and updated accordingly.

III. **Special Account Training**

Third-parties, such as suppliers, contractors, vendors, and partners, granted special account access by ITS are required to understand their roles and responsibilities regarding information system security requirements. See the Information Security Program document.

Depending upon the nature of the third-party relationship, the roles and responsibilities may vary greatly. If a third-party is granted access privileges to Private College Data, the third-party will be required to have in place a training program that meets the same level of requirements as the college’s information security training and awareness program. In the event the third-party does not have an adequate information security awareness and training program, the college, at its discretion, may administer its training and awareness program for the third-party.

**RELATED POLICIES**

- Acceptable Use of College Computer and Network Systems Policy
- Access Control Policy
- Acquisition and Disposal Policy
- Audit and Accountability Control Policy
- Configuration Management Policy
- Data Classification Policy
- Email Retention Policy
- Identification and Authentication Policy
- Incident Response Policy
- Information Security Program
- Information Technology Personnel Security Policy
- Information Technology Physical and Environmental Protection Policy
- Identity Theft Prevention Policy
- Mass Email Policy
- Media Protection Policy
- Mobile Device Use and Support Policy
- Password Policy
- Record Retention Policy and Schedule
- Wireless Access Points Policy
2.4.24. Payment Card Information Security Policy

PAYMENT CARD INFORMATION SECURITY POLICY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>May 3, 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Number:</td>
<td>2.4.24</td>
</tr>
<tr>
<td>Supersedes:</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Issuing Authority:</td>
<td>President</td>
</tr>
<tr>
<td>Responsible Officer:</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Applicability:</td>
<td>All College Information Systems that store, process, or transmit Cardholder Data, as well as all Authorized Users who access, use, or handle those resources.</td>
</tr>
</tbody>
</table>

History:

PURPOSE

The purpose of this policy is to prescribe a comprehensive set of standards and associated controls for protecting the confidentiality, integrity, and availability of the college’s Cardholder Data Environment and related College Information Systems (“applicable information systems”) as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. This policy is intended to be used in conjunction with the complete PCI-DSS Program requirements as established and revised by the PCI Security Standards Council.

POLICY

It is the policy of Canisius College to comply with the Payment Card Industry Data Security Standard (PCI-DSS) Program. The college is committed to PCI-DSS standards to protect credit and payment card Account Data (Cardholder Data and/or Sensitive Authentication Data) that is stored, processed, or transmitted by the college in conducting its business operations.

This policy incorporates, by reference, college policies and associated controls that address the security and confidentiality of Private College Data. These policies include:

- Acceptable Use of College Computer and Network Systems Policy
- Access Control Policy
- Audit and Accountability Control Policy
- Computer Assess Disposal Policy
- Computer Asset Replacement Policy
- Configuration Management Policy
- Data Classification Policy
- Identification and Authentication Policy
- Information Security Program
- Information Technology Configuration Management Policy
- Information Technology Personnel Security Policy
- Information Technology Security Awareness and Training Policy
- Media Protection Policy
- Password Policy
- System and Information Integrity Policy
- Wireless Access Point Policy

College departments that have received formal approval from the vice president for business and finance (or his/her designee) to accept payment for goods or services on behalf of the college via credit or payment cards must meet the PCI-DSS requirements and associated controls set forth in this policy and the policies referenced above. Moreover, vendors and service providers involved in payment and credit card transactions on behalf of the college must contractually agree to comply with PCI-DSS and provide evidence of compliance annually to the college.

All Authorized Users in units approved to accept and/or access Cardholder Data or utilize devices or systems that store or access Cardholder Data must be properly trained and agree to adhere to the standards and controls set forth in this policy, as well as applicable college information technology security policies and associated controls. Any suspected security breach must be immediately reported and addressed in accordance with the ITS contingency plan, which includes incident response procedures for actual or attempted unauthorized access to Private College Data, including but not limited to Cardholder Data.

Failure to comply with the terms of this policy may result in disciplinary action up to and including termination and the possibility of civil and/or criminal liability. Additionally, an employee’s violation may also result in the loss of a department’s credit card acceptance privileges as determined by the vice president for business and finance (or his/her designee).

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

Cardholder - a person/agency to whom a card is issued, or any individual authorized to use a card.

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

Cardholder Data Environment (“CDE”)—is a college computer system or networked group of information systems that processes, stores and/or transmits Cardholder Data or Sensitive Authentication Payment Data. A CDE also includes any component that directly connects to or supports this network.

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. In addition to this coverage, which is required under federal law, the college chooses as a matter of policy to also include in this definition any Cardholder Data received in the course of business by the college, whether or not such Cardholder Data is covered by GLBA. Covered Data and Information includes both paper and electronic records. Covered Data and Information is classified as Private, Highly Restricted College Data pursuant to the College Data Classification Policy.

Credit Card Processing—the act of storing, processing, or transmitting credit card data.

E-commerce Application—any network-enabled financial transaction application.

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.

Payment Card—includes credit and debit cards bearing the logo of Visa, MasterCard, American Express, Discover, etc. used to make a payment.

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS is a standard that all organizations, including online retailers, must follow when storing, processing and transmitting their customers’ credit card data. The standard was developed by the PCI Security Standards Council to increase control of cardholder data to reduce payment card fraud and exposure. (See https://www.pcissecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1503420035332).

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, 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.

POS Device—point-of-sale (POS) - computer or payment card terminals either running as stand-alone systems or connecting to a server which are approved by the Controller’s Office.

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

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

Untrusted Network—is any network that is external to a college network(s) and/or which is out of the college’s ability to control or manage.

Virtual Payment Terminal—a web-browser-based access to a third-party service provider website to authorize payment card transactions when the merchant manually enters payment card data via a securely connected web browser.

PROCEDURES/GUIDELINES

I. Responsibilities

PCI-DSS compliance at Canisius College is a joint effort among all units associated with collecting payments to the college by means of credit and payment cards. The chief information officer is responsible for PCI compliance, with support from the vice president for business and finance (or his/her designee). These officers work jointly to ensure that units that process Cardholder Data are PCI-compliant. They also attest to merchant bank(s) regarding the college’s PCI compliance.

General roles and responsibilities as it pertains to the college’s Cardholder Data Environment are set forth below:

A. Chief Information Officer

The Chief Information Officer (“CIO”) is responsible for recommending and implementing prudent information technology security policies and associated controls, subject to the approval of the ITS Systems and Security Committee (SSC) and college president.

Role of the CIO:

1. Ensure an appropriate level of protection for the college’s Cardholder Data Environment; whether retained in-house or under the control of outsourced contractors;
2. Recommend the PCI DSS Information Security Policy policies and controls;
3. Identify Cardholder Data protection goals, objectives and metrics consistent with the college’s mission and strategic plan;
4. Ensure appropriate procedures are in place for security testing and risk assessment for all applicable information systems; and monitor, evaluate, and report to the SSC and college president on the status of information security within the college;
5. Ensure that college employees working in an information security role are properly trained, and supported with the appropriate resources;
6. Assist in compliance reviews and other reporting requirements;
7. Provide feedback to the SSC and president on the status of the college’s Information Security Program, and suggest improvements or areas of concern in the program or any other security-related activity;
8. Promote best practices in information security management;
9. Monitor and evaluate the status of the college’s information security posture by performing annual compliance reviews of the Payment Card Information Security Policy and associated controls (including reviews of security plans, risk assessments, security testing processes, and others);
10. Provide security-related guidance and technical assistance to all operating units;
11. Act as the college’s central point of contact for incident response handling in accordance with the ITS contingency plan;
12. Maintain liaison with external organizations on information security-related issues;
13. Identify resource requirements, including funds, personnel, and contractors, needed to manage the Information Security Program; and
14. Assign ownership of resources.
15. Regularly monitoring and testing the Information Security Program, including the Payment Card Information Security Policy.

B. Vice President for Business and Finance

Role of Vice President for Business and Finance:

1. Approve departments that may accept payment for goods or services on behalf of the college via credit or payment cards;
2. Obtain merchant numbers for each approved unit;
3. Maintain a registry of all Merchant ID holders and authorized users;
4. Obtain approved credit card swipe terminals for each approved unit not using ecommerce for credit and debit card transactions;
5. Oversee credit card accounting for each approved unit;
6. Review unit compliance with payment card receipt transactions procedures; and
7. Provide general supervision of unit credit and payment card operations.

C. 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 data. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. Data Owners have responsibility for:

1. Knowing the College Data for which she/he is responsible;
2. Determining a data retention period for the information, relying on advice from the college’s legal counsel and the Record Retention Policy and Schedule;
3. Ensuring that the college’s policies, controls, and procedures are followed to protect the integrity, confidentiality, and availability of the College Data used or created within the department;
4. Authorizing access and assigning custodianship in accordance with the Access Control Policy;
   a. Ensuring that access to Private College Data is limited to those with a “need to know” or “need to use”;
5. Specifying controls and communicating the control requirements to the custodian and users of the College Data;
6. Ensuring Authorized Users have proper information security training (relevant to the system);
7. Reporting promptly to the CIO all security incidents, including the loss or misuse of College Data;
8. Initiating corrective actions when problems are identified;
9. Promoting employee education and awareness by utilizing programs approved by the CIO, where appropriate;
10. Following existing approval processes for the selection, budgeting, purchase, and implementation of any computer system/software to manage College Data;
11. Following existing approval processes for the disposition of any computer system/software to manage College Data;
12. Participating in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies;
13. Participating in self-assessments of system safeguards and program elements and in certification and accreditation of the system;
14. Attending security awareness training and programs;
15. Maintaining a cooperative relationship with business partners or other interconnected systems;
16. Maintaining an inventory of unit hardware and software; and
17. Investigating security incidents in cooperation with and under direction of CIO.

D. Data Custodians

Data Custodians are generally responsible for the processing and storage of the College Data. The custodian is responsible for the administration of controls as specified by the Data Owner.

Responsibilities include:
1. Following information security policies, procedures and controls;
2. Promoting employee education and awareness by utilizing programs approved by the college;
3. Reporting promptly to the CIO the loss or misuse of Private College Data;
4. Identifying and responding to security incidents and initiating appropriate actions when problems are identified;
5. Reading and understanding all applicable training and awareness materials;
6. Participating in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies;
7. Following existing approval processes for the disposition of any computer system/software to manage College Data;
8. Complying with information security-related policies and with all controls established by the college and department.

E. Supervisors

Employees who supervise Authorized Users are responsible for overseeing their employees’ use of College Data.

Responsibilities include:
1. Reviewing and approving, in collaboration with the applicable Data Owner, all requests for department employee’s access authorizations;
2. Promptly informing ITS of employee terminations and transfers;
3. Revoking physical access to terminated employees, i.e., collecting keys, computers, etc.;
4. Providing employees with the opportunity for training needed to properly use the computer systems;
5. Reporting promptly to the CIO the loss or misuse of Private College Data;
6. Initiating corrective actions when problems are identified;
7. Following existing approval processes within their department for the selection, budgeting, purchase, and implementation of any computer system/software to manage College Data;
8. Following existing approval processes for the disposition of any computer system/software to manage College Data;
9. Comply with information security-related policies, procedures, and controls established by the college.

F. Authorized Users

An Authorized User is any person who has been authorized to read, enter, or update College Data.

Responsibilities include:
1. Accessing College Data only in support of the user’s authorized job responsibilities;
2. Complying with information security-related policies, including but not limited to the Payment Card Information Security Policy, and with all information security-related policies, procedures, and controls established by the college;
3. Knowing which systems or parts of systems for which they are directly responsible (printer, desktop, browser, etc.);
4. Completing all required user training and awareness programs;
5. Keeping personal authenticators (e.g., passwords, PINs, etc.) confidential;
6. Reporting all incidents to the Data Owner in a timely manner;
7. Following labeling, handling, sharing, storage and destruction requirements based on appropriate classification level;
8. Complying with the Record Retention Policy and Schedule before disposing of College Data; and
9. Reporting promptly to the Data Owner the loss or misuse of Private College Data.

II. PCI-DSS Standards

Section 1. Build and Maintain a Secure Network

It is the policy of Canisius College to protect the college’s Cardholder Data Environment by implementing formal, documented baseline firewall and router configurations that are consistent with industry-recognized best practices as follows:

Requirement 1. Firewall Configuration

Information Technology Services (“ITS”) establishes firewall and router configurations in accordance with the System and Communications best practices and Configuration Management policies. (PCI Requirement 1)
Firewall configuration requirements specific to the Cardholder Data Environment are summarized below:

1. All connections from an applicable information system (including a Cardholder Data Environment) to the Internet or other external networks or information system are authorized by the chief information officer (or his/her designee), documented by ITS, occur through controlled interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, encrypted tunnels), and are continuously monitored by ITS.
   a. To allow ITS to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection, ITS installs firewalls at each Internet connection and between any Demilitarized Zone (DMZ) and the college’s internal network(s) as applicable. (PCI Requirement 1.1)
   b. All new firewalls, as well as changes to firewall configuration settings, enabled services, and permitted connectivity are authorized by the chief information officer (or his/her designee) and tested and documented in accordance with the change control policies and procedures set forth in the Configuration Management Policy. (PCI Requirement 1.1.1)
   c. ITS establishes and maintains detailed network diagrams. The college’s network diagrams; (PCI Requirement 1.1.2)
      i. Document all connections to the Internet, or other external networks or information systems, including all wireless networks;
      ii. Are reviewed annually by ITS as part of the risk assessment process (see the Information Technology Policies); and
      iii. Are updated by ITS as the college’s network changes to reflect the current architecture in place.
   d. ITS establishes and maintains detailed data flow diagrams that shows all Cardholder Data flows across college systems and networks. (PCI Requirement 1.1.3).
   e. Privileges to modify the functionality, connectivity, configuration, and services supported by firewalls are restricted to authorized ITS staff. (PCI Requirement 1.1.5)
   f. All services that are permitted to pass through a college firewall, whether inbound or outbound, are documented by ITS as to:
      i. Service allowed;
      ii. Description of the service;
      iii. Business case necessitating the service;
      iv. Internal management and security controls associated with the service; and
      v. System interconnection agreements and service level agreements, as applicable. (PCI Requirement 1.1.6)
   g. Firewall and router rules are reviewed at least every six months in accordance with the vulnerability scanning process set forth in the Information Technology Policies. (PCI Requirement 1.1.7)

2. Approved firewalls are implemented by ITS to restrict connections between untrusted networks and any system in the Cardholder Data Environment. Access to the Internet must be through a firewall, as must any direct connection to a third-party vendor, processor, or service provider. (PCI Requirement 1.2)
   a. Firewalls are configured by ITS to deny all traffic by default, and only enable those services that are needed for the Cardholder Data Environment. Only services that are required and approved are activated by ITS. Any service that is not needed is turned off or deactivated. (PCI Requirement 1.2.1)
   b. ITS secures and synchronizes router and firewall configuration files. (PCI Requirement 1.2.2)
      i. Running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted) are configured to have the same, secure configurations.
   c. Perimeter firewalls are installed by ITS between any wireless networks and the Cardholder Data Environment. These firewalls are configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the Cardholder Data Environment. (PCI Requirement 1.2.3)

3. Firewalls are configured by ITS to prohibit direct public access between the Internet and any system component in the Cardholder Data Environment as follows:
   a. Where feasible, boundary perimeters (i.e., a DMZ) are established to limit inbound and outbound traffic to only protocols that are necessary for the Cardholder Data Environment. (PCI Requirement 1.3.1)
   b. Inbound Internet traffic is limited to IP addresses within the perimeter (i.e., a DMZ). (PCI Requirement 1.3.2)
   c. Denial of Service protection measures (e.g., anti-spoofing techniques) are implemented to detect and block forged source IP addresses from entering the network. (PCI Requirement 1.3.3)
   d. Unauthorized outbound traffic from the Cardholder Data Environment to the Internet is prohibited. (PCI Requirement 1.3.4)
   e. Where feasible, dynamic packet filtering is implemented. (PCI Requirement 1.3.5)
   f. System components that store cardholder data are placed within an internal network zone, segregated from the DMZ and other untrusted networks. (PCI Requirement 1.3.6)
   g. Firewall and routers are configured by ITS to prevent Private IP addresses and routing information from being disclosed to unauthorized parties. (PCI Requirement 1.3.7)
      i. Non-routable IP addresses specified in RFC 1918 (Private Network Addresses) will be dropped.

4. Any Mobile Device, regardless of ownership, with direct connectivity to the Internet and the ability to access the Cardholder Data Environment are required to have firewall software or equivalent functionality installed on the device. (PCI Requirement 1.4)
   a. Firewall software must be audited and approved by ITS;
   b. Configuration settings of the firewall software must not be alterable by the user of the Mobile Device; and
   c. The access controls and security configuration requirements set forth in the Mobile Device Use and Support Policy must be adhered to.

5. Training regarding the management of firewalls is conducted annually pursuant to the Security Awareness and Training Policy. In addition, the college’s information security-related policies are published at https://wiki.canisius.edu/x/VJ4Ag (PCI Requirement 1.5)

Refer to the Information Technology Policies for additional information regarding boundary protection mechanisms utilized by ITS to protect Private College Data.

Requirement 2. Change Vendor-Supplied Defaults

In accordance with the Information Technology Policies, ITS changes vendor default passwords and other vendor default settings prior to system implementation on a college network in order to prevent a system from being compromised by malicious individuals making use of standard configuration parameters.

1. ITS changes all vendor-supplied defaults prior to the resource being installed on the network. This hardening process for both wired and wireless information systems includes, but is not limited to changing the following vendor defaults as applicable: (PCI Requirement 2.1 and 2.1.1)
   a. Passwords: including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.;
   b. Simple Network Management Protocol (SNMP) community strings;
   c. Encryption keys;
   d. Default passwords/passphrases on access points;
e. Other security-related wireless vendor defaults as applicable; and
f. Firmware on wireless devices must be updated to support strong encryption (such as WPA or WPA2) for authentication and transmission of data over wireless networks. See the Information Technology Policies.

2. ITS configures system components in accordance with the hardening standards set forth in the Information Technology Policies. ITS’s process of pre-installation hardening includes, but is not limited to: (PCI Requirement 2.2)
a. Verifying that the college’s system configurations are:
   i. Updated as new vulnerability issues are identified via the risk assessment process (see the Information Technology Policies);
   ii. Applied when new systems are configured (see the Configuration Management Policy); and
   iii. Consistent with industry-accepted hardening best practices.
   b. In accordance with the System and Communications Protection Policy, ITS implements only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers, and Domain Name Systems (DNS) are implemented on separate servers). (PCI Requirement 2.2.1)
   c. In accordance with the Information Technology Policies, ITS employs principals of least privilege and least functionality, which includes:
      i. Enabling only necessary and secure services, protocols, daemons, etc., as required for the function of the system. (PCI Requirement 2.2.2)
      ii. Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (PCI Requirement 2.2.5)
   d. Implementing additional security features for any required services, protocols or daemons that are considered by ITS to be insecure. This may include using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Transport Layer Security (TLS), or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, and (PCI Requirement 2.2.3)
   e. Configuring system security parameters to prevent misuse. (PCI Requirement 2.2.5)
   f. Documenting the functionality present on the Information Technology Resource.

3. In accordance with the Information Technology Policies, ITS ensures that strong cryptography (i.e., encryption) is utilized to protect Private College Data, which includes Cardholder Data and/or Sensitive Authorization Data, transmitted by Authorized Users over the college networks to protect against risks of interception.
   a. This includes the encryption of authorization credentials for non-console (i.e., wireless) administrative access using technologies such as SSH, VPN, or TLS. (PCI Requirement 2.3)

4. In accordance with the Information Technology Policies, ITS maintains an inventory of information systems and updates the inventory as necessary. (PCI Requirement 2.4)
   a. Maintaining a current list of all system components enables ITS to accurately and efficiently define the scope of its Cardholder Data Environment for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from applicable configuration standards.

Refer to the Information Technology Policies for additional information regarding the changing of vendor default passwords and settings to prevent a system from being compromised by malicious individuals making use of standard configuration parameters.

Section 2. Protect Cardholder Data

In accordance with the Information Technology Policies, the college protects Cardholder Data by implementing protection methods such as encryption and other boundary protection actions.

Requirement 3. Protect Stored Cardholder Data

1. It is the responsibility of Data Owners and Data Custodians to maintain and ensure the secure disposal of Cardholder Data in accordance with the Data Retention Policy and Schedule and the Media Protection Policy. (PCI Requirement 3.1) Specific responsibilities include:
   a. Overseeing unit compliance with the retention periods set forth in the College Data Retention Policy and Schedule;
   b. Conducting a quarterly process (automatic or manual) to identify and securely delete stored Cardholder Data that exceeds defined retention requirements;
   c. Ensuring that electronic-based Cardholder Data is securely deleted of at the conclusion of the retention period; and
   d. Ensuring that physical-based Cardholder Data is shredded at the conclusion of the retention period.

2. ITS configures, examines, and confirms system settings and system components to preclude the storing of Sensitive Authorization Data after authorization. (PCI Requirement 3.2) Specifically, ITS:
   a. Appropriately configures, examines, and confirms system settings and all necessary configurations for system components to ensure that:
      i. Any contents of any track from the magnetic stripe on the back of a card or equivalent data on a chip are not stored after authorization; (PCI Requirement 3.2.1)
      ii. That the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CA2 data) is not stored after authorization; and (PCI Requirement 3.2.2)
   b. Appropriately configures, examines, and confirms system settings and all necessary configurations for system components to ensure that PANs and encrypted PIN blocks are not stored after authorization. (PCI Requirement 3.2.3)
   c. Appropriately configures, examines, and confirms system settings and all necessary configurations for system components to ensure that PANs are masked when displaying Cardholder Data, and that only those with a legitimate business need are able to see full PAN. This may include using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Transport Layer Security (TLS), or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, and (PCI Requirement 3.2.4)
   d. If disk encryption is used, preventing decryption keys from being tied to Authorized User accounts, rather than file- or column-level database encryption: (PCI Requirement 3.4.1)
i. Logical access must be managed independently of native operating system access control mechanisms (e.g., by not using local user account databases).
ii. Decryption keys are not tied to operating system-level Authorized User accounts.

5. ITS
a. Encryption keys are protected primarily through the use of standard certificate authorities, so to restrict access to the fewest number of custodians; and are stored in the fewest possible locations.
b. Cryptographic key access is restricted to the fewest number of Authorized Users. (PCI Requirement 3.5.2)
c. Cryptographic key access is securely stored at all times using one of the following methods: (PCI Requirement 3.5.3)
   i. Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data encrypting key;
   ii. Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device); or
   iii. As at least two full-length key components or key shares, in accordance with an industry-accepted method; and

d. Encryption keys are securely stored in the fewest possible locations and forms in accordance with the Information Technology Policies. (PCI Requirement 3.5.4)

6. Encryption keys are established and managed by ITS in accordance with the Information Technology Policies. (PCI Requirements 3.6).

7. Training regarding the protection of Cardholder Data is conducted annually pursuant to the Security Awareness and Training Policy. In addition, the college’s information security-related policies are published at https://wiki.canisius.edu/x/VIJ4Ag (PCI Requirement 3.7)

Refer to the Information Technology Policies for additional information regarding the use of encryption and other boundary protection actions utilized by ITS to protect Cardholder Data.

**Requirement 4. Encrypt Transmission of Cardholder Data Across Open, Public Networks**

In accordance with the System and Communications Protection Policy, ITS safeguards Cardholder Data during transmission over open, public networks by utilizing strong encryption and security protocols. (PCI Requirement 4.1)

Encryption requirements specific to the Cardholder Data Environment are set forth below:

1. Point of Sale Devices at the college are configured by ITS to use built-in certificates for transmitting Cardholder Data over the college network; applications use industry-accepted protocols like TLS V1.2 or above to transmit any Cardholder Data.
2. Industry best practices (for example, IEEE 802.11i) are used by ITS to implement strong encryption for authentication and transmission for wireless networks transmitting Cardholder Data or connected to the Cardholder Data Environment. (PCI Requirement 4.1.1)
3. Authorized Users may not transmit unencrypted Cardholder Data via texting messages, instant messages, emails, or voicemail. (PCI Requirement 4.2)
   a. It is strongly recommended to never send Cardholder Data through these protocols, even with added encryption.
4. Training regarding the encryption of Cardholder Data prior to transmission over open, public networks is conducted annually pursuant to the Security Awareness and Training Policy. In addition, the college’s information security-related policies are published at https://wiki.canisius.edu/x/VIJ4Ag (PCI Requirement 4.3)

Refer to the Information Technology Policies, Electronic Mail, and Use of Mobile Devices policies for additional information.

**Section 3: Maintain a Vulnerability Management Program**

**Requirement 5. Use and Regularly Update Anti-Virus Software or Programs**

In accordance with the Canisius College System and Data Integrity best practices, ITS provides protection from malicious code at appropriate locations within the Cardholder Data Environment, as well as monitors security alerts/advisories and takes appropriate actions in response.

Below is a summary of malicious code protection mechanisms utilized by ITS to protect the Cardholder Data Environment:

1. ITS employs malicious code protection mechanisms at system entry and exit points within the Cardholder Data Environment (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or college-owned/leased mobile computing devices on the college network(s). (PCI Requirement 5.1, 5.1.1)
2. For systems considered to be not commonly affected by malicious software, ITS performs periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require malicious code protection. (PCI Requirement 5.1.2)
3. The college’s anti-virus software programs are kept current through automatic updates, are required to be actively running, are configured to run periodic scans, and are configured to generate audit logs. The audit logs of protection activities are included in the backups and are retained in accordance with the Record Retention Policy and Schedule. (PCI Requirement 5.2)
4. Malicious code protection mechanisms are required to be actively running and Authorized Users are prohibited from disabling or altering such mechanisms, unless specifically authorized by ITS on a case-by-case basis for a limited time period. (PCI Requirement 5.3)
5. Training regarding protecting systems against malware is conducted annually pursuant to the Information Technology Security Awareness and Training Policy. In addition, the System and Data Integrity best practices are published at https://wiki.canisius.edu/x/VIJ4Ag (PCI Requirement 5.4)

Refer to the Information Technology Policies for additional information regarding the mechanisms utilized by the college to manage risks from malicious code.

**Requirement 6: Develop and Maintain Secure Systems and Applications**

In accordance with the Information Technology Policies, ITS scans for vulnerabilities in Cardholder Data Environment systems and applications. ITS analyzes vulnerability scan reports, assigns a risk rating for identified vulnerabilities, and remedies legitimate vulnerabilities in accordance with its assessment of risk and corresponding risk management strategy. (PCI Requirement 6)

Below is a summary of the college’s vulnerability scan processes as it applies to the Cardholder Data Environment:

1. ITS ranks identified system vulnerabilities as either Critical, High, Medium, Low and Minimal in accordance with the definitions set forth in the Information Technology Policies. (PCI Requirement 6.1)
2. Patches are applied for the highest risk vulnerabilities first:
   a. Security patches will be installed within one month of release for all vulnerabilities ranked as “Critical”; and
3. ITS tests and validates changes to Cardholder Data Environment systems introduced as a result of vulnerability scans before implementing the change in accordance with the procedures set forth in the Configuration Management Policy. (PCI Requirement 6.4)

   b. All non-critical security patches will be installed within an appropriate time frame determined by ITS (for example, within three months). (PCI Requirement 6.2)

4. ITS documents changes to Cardholder Data Environment systems introduced as a result of vulnerability scans in accordance with the procedures set forth in the Configuration Management Policy. (PCI Requirement 6.4.5) ITS documents:
   a. The impact of the change (PCI Requirement 6.4.5.1);
   b. The administrator(s) who approved the change (PCI Requirement 6.4.5.2);
   c. The results of functionality testing (PCI Requirement 6.4.5.3); and
   d. Back-out procedures (PCI Requirement 6.4.5.4).

5. Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. (PCI Requirement 6.4.6)

6. In accordance with the Information Technology Policies, ITS locates public access servers outside of the college’s Intranet. In addition, these servers are protected by firewalls on the public side of the college network and have their own intrusion detection systems. As part of the risk assessment process (see the Information Technology Policies), ITS reviews public-facing web application intrusion detection systems as follows: (PCI Requirement 6.4.7)
   a. At least annually; and
   b. After any changes to the public facing website.

7. Training regarding maintaining secure systems and applications is conducted annually pursuant to the Security Awareness and Training Policy. In addition, the System and Data Integrity best practices are published at https://wiki.canisius.edu/x/VIU4Ag (PCI Requirement 6.8)

Refer to the Configuration Management policies for additional vulnerability scanning procedures utilized by the college.

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

In accordance with the Access Control Policy, ITS limits access to cardholder system components and Cardholder Data to only those individuals whose jobs require such access. (PCI Requirement 7)

Below is a summary of the college’s access controls applicable to the Cardholder Data Environment:

1. In accordance with the Access Control Policy, access to college cardholder system components and Cardholder Data is limited to only those Authorized Users whose jobs require such access. (PCI Requirement 7.1)
   a. Administrator and special access account IDs are restricted based on the principle of least privilege. (PCI Requirement 7.1.2)
   b. Privileges are assigned by Data Owners to Authorized Users based on job classification and function (also called “role-based access control”). (PCI Requirement 7.1.3)

2. College cardholder system components and Cardholder Data are configured by ITS to have a default “deny-all” setting, which ensures no one is granted access without a login ID associated with an authorized account. (PCI Requirement 7.2)

3. Training regarding access controls is conducted annually pursuant to the Security Awareness and Training Policy. In addition, this policy, as well as the Access Control Policy and other applicable information technology security related policies are published at https://wiki.canisius.edu/x/VIU4Ag (PCI Requirement 7.3)

Refer to the Access Control Policy for additional access control procedures utilized by the college.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

In accordance with the Access Control, Identification and Authentication, Password, and Information Technology Personnel Security policies, ITS ensures proper user identification management for non-consumer Authorized Users and administrators on all Cardholder Data Environment system components. (PCI Requirement 8)

Below is a summary of the college’s identification and authentication controls applicable to the Cardholder Data Environment:

1. ITS assigns a unique Login ID to all Authorized Users as appropriately authorized by applicable Data Owners and supervisors upon hiring or transfer. (PCI Requirement 8.1.1)
   a. Authorized User Login IDs are added, deleted, and modified in accordance with the procedures set forth in the Personnel Security Policy; (PCI Requirement 8.1.2)
   b. Access authorization to information systems are revoked immediately by ITS upon notification of the termination in accordance with the procedures set forth in the Personnel Security Policy; (PCI Requirement 8.1.3)
   c. Inactive User Accounts are removed or disabled by ITS within ninety (90) days in accordance with the procedures set forth in the Access Control Policy. Exceptions can be made at the request of the Data Owner; (PCI Requirement 8.1.4)
   d. Special access accounts (e.g., guest or visitor) are to be used in very limited situations and must provide individual accountability, which also includes wireless. (PCI Requirement 8.1.5) In accordance with the procedures set forth in the Access Control Policy, special access accounts must be:
      i. Requested in writing by a Data Owner (or his/her authorized designee) and authorized by the chief information officer, or designee.
      ii. Created with a specific expiration date;
      iii. Monitoring the account when in use; and
      iv. Removed when the task or project is complete.
   e. In accordance with the Access Control Policy, ITS enforces, through the baseline configuration, a limit of than attempts to login to the account within a 15-minute timeframe by a user; (PCI Requirement 8.1.6)
   f. In accordance with the Access Control Policy, if a user has unsuccessfully attempted more than three (3) attempts to login to the account within a 15-minute timeframe, the account will be locked for a minimum of thirty (30) minutes (or until an administrator enables the user ID) and the user may try again after that time; and (PCI Requirement 8.1.7)
g. In accordance with the Access Control Policy, ITS, through a baseline configuration, enforces a session lock as a temporary action taken when an Authorized User stops work, and the resource is idle. The session lock will be set to initiate after fifteen (15) minutes of idle time. (PCI Requirement 8.1.8)

2. ITS ensures the proper management of user-authentication for non-consumer Authorized Users and administrators on all system components in accordance with the controls set forth in the Identification and Authentication and Password policies. (PCI Requirement 8.2)
   a. In accordance with the Identification and Authentication Policy, ITS authenticates all Authorized User through the use of passwords, PINS, or biometrics in addition to assigning a unique ID: (PCI Requirement 8.2)
   b. The Password Policy requires the use of strong cryptography to render all passwords unreadable during transmission and storage; (PCI Requirement 8.2.1)
   c. In accordance with the Identification and Authentication Policy, ITS verifies user identity before performing password resets, provisioning new tokens, or generating new keys; (PCI Requirement 8.2.2)
   d. In accordance with the Password Policy, system software must require passwords to contain: (PCI Requirement 8.2.3)
      i. A minimum length of at least seven (7) characters; and
      ii. Both numeric and alphabetic characters;
   e. In accordance with the Password Policy, system software must require password changes at least once every ninety (90) days; and (PCI Requirement 8.2.4)
   f. In accordance with the Password Policy, system software must prohibit Authorized Users from submitting a new password that is the same as any of the last four (4) passwords he or she has used; and (PCI Requirement 8.2.5)
   g. In accordance with the Identification and Authentication Policy, system software must set passwords for first-time use and upon reset to a unique value for each Authorized User. Authorized Users must then change the password immediately after the first use. (PCI Requirement 8.2.6)

3. ITS secures all non-console administrative access and all remote access to the Cardholder Data Environment using multifactor authentication. (PCI Requirement 8.3)
   a. ITS incorporates multi-factor authentication for all non-console access into the Cardholder Data Environment for personnel with administrative access Login ID credentials. (PCI Requirement 8.3.1)
   b. ITS incorporates multi-factor authentication for all remote network access (both user, administrator, and special access for support or maintenance) originating from outside the college network. (PCI Requirement 8.3.2)

4. In accordance with this Credit Card Security and the Password Policy, supervisors are required to provide applicable staff with: (PCI Requirement 8.4)
   a. Guidance on selecting strong authentication credentials;
   b. Guidance for how users should protect their authentication credentials;
   c. Instructions not to reuse previously used passwords; and
   d. Instructions to change passwords if there is any suspicion the password could be compromised.

5. Data Custodians and Data Owners are prohibited from using group, shared, or generic IDs, passwords, or other authentication methods as follows: (PCI Requirement 8.5)
   a. Generic user IDs must be disabled or removed;
   b. Shared user IDs must not exist for system administration and other critical functions (see the Access Control Policy); and
   c. Shared and generic user IDs must not be used to administer any system components.

6. ITS restricts all access to any database containing Cardholder Data (including access by applications, administrators, and all other Authorized Users) as follows: (PCI Requirement 8.7)
   a. ITS configures, examines, and confirms system settings and all necessary configurations for system components to ensure that all users are authenticated prior to access.
   b. ITS configures, examines, and confirms system settings and all necessary configurations for system components to ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete) the database are through programmatic methods only (for example, through stored procedures).
   c. ITS configures, examines, and confirms system settings and all necessary configurations for system components to ensure that user direct access to or queries of databases are restricted to database administrators.
   d. ITS configures, examines, and confirms system settings and all necessary configurations for system components to ensure that application Login IDs can only be used by the applications (and not by individual users or other processes).

7. Training regarding identification and authentication controls are conducted annually pursuant to the Security Awareness and Training Policy. In addition, this policy, as well as the Access Control, Identification and Authentication, Password, Information Technology Personnel Security, and other applicable information technology security related policies are published at https://wiki.canisius.edu/x/VIJ4Ag (PCI Requirement 8.8)

Refer to the Access Control, Identification and Authentication, Password, and Information Technology Personnel Security policies for additional identification and authentication control policies and procedures utilized by the college.

Requirement 9: Restrict Physical Access to Cardholder Data

In accordance with the Physical and Environmental Protection and Media Protection policies, ITS implements appropriate controls to limit and monitor physical access to systems and media in the Cardholder Data Environment (CDE). (PCI Requirement 9)

Below is a summary of the college’s physical access controls applicable to the Cardholder Data Environment:

1. In accordance with the Physical and Environmental Protection Policy, ITS implements appropriate facility entry controls to limit and monitor physical access to sensitive areas in the Cardholder Data Environment. (PCI Requirement 9.1)
   a. The use of to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries: (PCI Requirement 9.1.1)
      i. Video surveillance footage must be readily accessible for at least three (3) months, unless otherwise restricted by law; and
      ii. Access control mechanisms (e.g., sign-in sheets) must be readily accessible for at least three (3) months;
   b. Restricting physical access to publicly accessible network jacks, by either: (PCI Requirement 9.1.2)
      i. Preventing physical access to the network jack; or
      ii. Disconnecting unused or publicly accessible network jacks at the patch panel;
   c. Restricting physical access to Wireless Access Points (WAPs), gateways, handheld devices, networking/communications hardware, and telecommunication lines. (PCI Requirement 9.1.3)

2. In accordance with the Physical and Environmental Protection Policy, ITS implements the following procedures to easily distinguish between college personnel and visitors, including third-party support services personnel, in sensitive areas in the Cardholder Data Environment: (PCI Requirement 9.2)
   a. ITS issues visitors a badge or other identification that expires and that visibly distinguishes them from members of the college community; and
b. Visitors must turn in their badge or identification before leaving the sensitive area.

3. In accordance with the Physical and Environmental Protection Policy, ITS controls physical access for college personnel to sensitive areas in the Cardholder Data Environment as follows: (PCI Requirement 9.3)
   a. Access must be authorized by the CIO (or designee) and based on individual job function; and
   b. Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.

4. In accordance with the Physical and Environmental Protection Policy, visitors, including third-party support services personnel, are granted access to sensitive areas only when required, authorized, and monitored by ITS or other appropriate college staff: (PCI Requirement 9.4)
   a. ITS must authorize visitors before entering specific controlled sensitive areas; (PCI Requirement 9.4.1)
   b. Visitors must sign in and out of the sensitive area logbook, documenting their name, company if any, purpose of visit, time of entry and departure, and the name of the college employee authorizing the access; (PCI Requirement 9.4.4)
   * ;
   c. Visitors must be escorted by authorized ITS personnel or other appropriate college staff;
   d. ITS issues visitors a badge or other identification that expires and that visibly distinguishes them from members of the college community; and (PCI Requirement 9.4.2)
   e. Visitors must turn in their badge or identification before leaving the sensitive area. (PCI Requirement 9.4.3)

5. In accordance with the Media Protection Policy, Data Owners, in conjunction with Data Custodians, supervisors, and Authorized Users, are required to physically secure all media, as follows: (PCI Requirement 9.5)
   a. Store media back-ups in a secure location designated by ITS, such as: (PCI Requirement 9.5.1)
      i. An alternate or back-up site on campus; or
      ii. A commercial storage facility; and
   b. ITS reviews the backup facility’s security at least annually as part of the risk assessment process.

6. In accordance with the Media Protection Policy, the college maintains strict control over the transmission of media, including the following: (PCI Requirement 9.6)
   a. Data Owners are responsible for evaluating and classifying College Data for which they are responsible according to the classification system adopted by the college and described in the Data Classification Policy; (PCI Requirement 9.6.1)
   b. Authorized Users must transmit media classified as Private by secured courier or other delivery method that can be accurately tracked; (PCI Requirement 9.6.2)
   c. Authorized Users must ensure they have their supervisor’s approval prior to transmitting media (including when media is distributed to individuals) classified as Private. (PCI Requirement 9.6.3)

7. In accordance with the Media Protection Policy, the college maintains strict control over the storage and accessibility of media: (PCI Requirement 9.7)
   a. Data Owners, Data Custodians, and supervisors ensure that Authorized Users in their respective units physically and logically protect media containing Private College Data while at rest, stored, or actively being accessed in accordance with the media storage guidelines set forth in the Media Protection Policy; (PCI Requirement 9.7.1)
   b. Data Owners, in conjunction with Data Custodians and supervisors, maintain inventory logs of all media classified as Private; and (PCI Requirement 9.7.1)
   c. ITS oversees the inventorying of media classified as Private at least annually. (PCI Requirement 9.7.1)

8. In accordance with the Media Protection Policy, the college sanitizes applicable media when it is no longer needed for business or legal reasons. Data custodians are required to destroy media that cannot be sanitized, as follows: (PCI Requirement 9.8)
   a. Hardcopy materials are shredded, incinerated, or appropriately recycled (i.e., pulped) so that Cardholder Data cannot be reconstructed; (PCI Requirement 9.8.1)
      i. Cardholder Data that is awaiting to be destroyed is securely stored;
   b. Electronic media is rendered unrecoverable so that Cardholder Data cannot be reconstructed. (PCI Requirement 9.8.2)

9. The college prohibits unauthorized physical access to devices that capture credit and payment card data (e.g., Point of Sale (PoS) devices) as follows: (PCI Requirement 9.9)
   a. Student Records and Financial Services maintains an up-to-date list of devices that includes the following: (PCI Requirement 9.9.1)
      i. Make, model of device;
      ii. Location of device (e.g., the address of the site or facility where the device is located); and
      iii. Device serial number or other method of unique identification;
   b. Authorized Users are required to periodically inspect device surfaces to detect tampering (e.g., addition of card skimmers to devices), or substitution (e.g., by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device); and (PCI Requirement 9.9.2)
   c. The Student Records and Financial Services office trains for personnel to be aware of attempted tampering or replacement of devices that includes the following: (PCI Requirement 9.9.3)
      i. Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices;
      ii. Prohibiting the installation, replacement, or return devices without verification;
      iii. Awareness for suspicious behavior around devices (e.g., attempts by unknown persons to unplug or open devices); and
      iv. Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (e.g., to a supervisor or security officer).

10. Training regarding media protection controls is conducted annually pursuant to the Security Awareness and Training Policy. In addition, this policy, as well as the Physical and Environmental Protection, Media Protection, and other applicable information technology security related policies are published at https://wiki.canisius.edu/vUJ4Ag (PCI Requirement 9.10)

Refer to the Physical and Environmental Protection, Media Protection, and Acceptable Use of College Computer and Network Systems policies for additional physical security and media protection control policies and procedures utilized by the college.

Requirement 10: Regularly Monitor and Test Networks

In accordance with the Audit and Accountability Policy, ITS utilizes logging mechanisms and system activity to track Authorized User activities. (PCI Requirement 10)

Below is a summary of the college’s monitoring and testing controls applicable to the Cardholder Data Environment:

1. In accordance with the Audit and Accountability Policy, ITS links all access to Cardholder Data system components (especially access done with administrative privileges such as root) to each Authorized User; (PCI Requirement 10.1)
2. In accordance with the Audit and Accountability Policy, ITS implements automated audit trails for all Cardholder Data system components accessing to reconstruct the following events: (PCI Requirement 10.2)
   a. All Authorized User accesses to Cardholder Data; (PCI Requirement 10.2.1)
b. All actions taken by any individual administrator access privileges; (PCI Requirement 10.2.2)
c. Access to all audit trails; (PCI Requirement 10.2.3)
d. Invalid logical access attempts; (PCI Requirement 10.2.4)
e. Use of and changes to Identification and Authentication mechanisms, including but not limited to: (PCI Requirement 10.2.5)
   i. Creation of new accounts and elevation of privileges; and
   ii. All changes, additions, or deletions to accounts with root or administrative privileges;
f. Initialization, stopping, or pausing of the audit logs; and (PCI Requirement 10.2.6)
g. Creation and deletion of system-level objects. (PCI Requirement 10.2.7)

3. In accordance with the Audit and Accountability Policy, ITS configures systems to record at least the following audit trail entries for all Cardholder Data system components for each event: (PCI Requirement 10.3)
   a. User identification; (PCI Requirement 10.3.1)
   b. Type of event; (PCI Requirement 10.3.2)
   c. Date and time; (PCI Requirement 10.3.3)
   d. Success or failure indication; (PCI Requirement 10.3.4)
   e. Origination of event; and (PCI Requirement 10.3.5)
   f. Identity or name of affected data, system component, or resource. (PCI Requirement 10.3.6)

4. In accordance with the Audit and Accountability Policy, ITS configures internal system clocks to generate time stamps for audit records. (PCI Requirement 10.4)
   a. Time stamps generated by the system must include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. (PCI Requirement 10.4.3)
   b. Data Owners are responsible for ensuring that the time stamps on their systems are configured properly and validate the following:
      i. Systems are configured to synchronize time with college servers; (PCI Requirement 10.4)
      ii. Information systems have the correct and consistent time; and (PCI Requirement 10.4.1)
      iii. Time data is protected from unauthorized modification. (PCI Requirement 10.4.2)

5. In accordance with the Audit and Accountability Policy, ITS secures audit trails, so the logs cannot be altered. Securing audit trails includes the following: (PCI Requirement 10.5)
   a. Only authorized Data Owners and Custodians, as well as select staff from ITS, with a legitimate business need are permitted access to audit logs and audit tools; (PCI Requirement 10.5.1)
   b. Audit files are protected from unauthorized modifications via the use of Login ID and authentication; (PCI Requirement 10.5.2)
   c. Systems are configured to allow real-time backup or the transfer audit of trail files to a centralized log server or media that is difficult to alter; (PCI Requirement 10.5.3)
   d. Systems are configured to write logs for external-facing technologies onto a secure, centralized, internal log server or media device; (PCI Requirement 10.5.4)
   e. Audit logs containing Private College Data must be encrypted in accordance with the Information Technology Policies; and
   f. Where feasible, ITS implements File Integrity Monitoring (FIM) or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. (PCI Requirement 10.5.5)

6. In accordance with the Audit and Accountability Policy, ITS review logs and security events for all system components to identify anomalies or suspicious activity as follows: (PCI Requirement 10.6)
   a. The following logs are reviewed by ITS Staff at least daily: (PCI Requirement 10.6.1)
      i. All security events;
      ii. Logs of all system components that store, process, or transmit cardholder data, or that could impact the security of Private College Data, including Cardholder Data;
      iii. Logs of all critical system components; and
      iv. Logs of all servers and system components that perform security functions. This includes, but is not limited to:
         1. Firewalls
         2. Intrusion Detection Systems (IDS)
         3. Intrusion Prevention Systems (IPS)
         4. Authentication servers (e.g., Active Directory domain controllers); and
         5. E-commerce redirection servers;
   b. ITS staff reviewing logs of all other system components in accordance with the college’s annual risk assessment (see the Information Technology Policies); (PCI Requirement 10.6.2) and
   c. ITS staff report exceptions and anomalies identified during the review process to the chief information officer (or his/her designee) and follow up as appropriate. (PCI Requirement 10.6.3)

7. The college retains Cardholder Data Environment related audit records for at least one (1) year, with a minimum of three (3) months immediately available for analysis. (PCI Requirement 10.7)

8. The college timely detects and reports failures of critical security control systems through the use of the following: (PCI Requirement 10.8)
   a. Firewalls (see the Information Technology Policies);
   b. IDS/IPS (see the Information Technology Policies);
   c. Anti-malware (see the Information Technology Policies s);
   d. Physical access controls (see the Information Technology Policies);
   e. Logical access controls (see the Identification and Authentication, Password and Access Control policies);
   f. Audit logging mechanisms (see the Audit and Accountability Policy); and
   g. Segmentation controls (if used) (see the Information Technology Policies).

9. Training regarding the monitoring of applicable college networks is conducted annually pursuant to the Information Technology Security Awareness and Training Policy. In addition, this policy, as well as the all applicable information technology security related policies are published at https://wiki.canisius.edu/x/xIF4Ag (PCI Requirement 10.9)

Refer to the Information Technology Policies for additional monitoring control policies and procedures utilized by the college.

Requirement 11: Regularly Test Security Systems and Processes

In accordance with the Information Technology Policies, ITS implements security system testing strategies to manage risks from system flaws /vulnerabilities, malicious code, unauthorized code changes, and inadequate error handling. (PCI Requirement 11)

Below is a summary of the college’s security system testing controls applicable to the Cardholder Data Environment:

1. ITS employs a wireless intrusion detection system (IDS) to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to applicable resource systems in the Cardholder Data Environment: (PCI Requirement 11.1)
   a. ITS conducts testing to detect and identify all authorized and unauthorized wireless access points on campus at least once every ninety (90) days;
b. ITS maintains an inventory of authorized wireless access points, including a documented business justification; and

c. ITS implements incident response procedures in the event unauthorized wireless access points are detected.

2. In accordance with the Information Technology Policies, ITS scans for vulnerabilities in applicable systems and applications as follows: (PCI Requirement 11.2)

a. External and internal scans are conducted by qualified ITS staff quarterly (i.e., every ninety (90) days), as well as whenever there is a security incident, new information on potential vulnerabilities, or a major system change; (PCI Requirement 11.2.1) and

b. External vulnerability scans are conducted at least every quarter by a Payment Card Industry Security Standards Council (PCI SSC) Approved Scanning Vendor (ASV). (PCI Requirement 11.2.2)

3. In accordance with the Information Technology Policies, the college performs external and internal penetration testing against its Cardholder Data Environment to identify security weaknesses.

a. The Information Technology Policies set forth a methodology for penetration testing that: (PCI Requirement 11.3)


ii. Includes coverage for the entire Cardholder Data Environment perimeter and critical systems;

iii. Includes testing from both inside and outside the network;

iv. Includes testing to validate any segmentation and scope-reduction controls (as applicable);

v. Defines network-layer penetration tests to include components that support network functions as well as operating systems (i.e., wireless);

vi. Includes review and consideration of threats and vulnerabilities experienced in the last 12 months; and

vii. Specifies retention of penetration testing results and remediation activities results.

b. In accordance with the Information Technology Policies, the college performs external and internal penetration testing annually and after any significant infrastructure or application changes to the Cardholder Data Environment; (PCI Requirements 11.3.1 and 11.3.2)

1. Testing is performed by qualified internal personnel or an external ASV approved by the chief information officer (or his/her designee)

2. In accordance with the Information Technology Policies, exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections; (PCI Requirements 11.3.3)

d. In accordance with the Information Technology Policies, if segmentation has been used by ITS to isolate the Cardholder Data Environment from other college networks, penetration tests will also be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the Cardholder Data Environment; (PCI Requirements 11.3.4)

4. In accordance with the Information Technology Policies, ITS utilizes Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) to: (PCI Requirements 11.4)

a. Prevent intrusions into the Cardholder Data Environment;

b. Monitor all traffic at the perimeter of the CDE, as well as at critical points in the Cardholder Data Environment;

c. Alert personnel to suspected compromises within the Cardholder Data Environment; and

d. Keeps all intrusion-detection and prevention engines, baselines, and signatures up-to-date.

5. In accordance with the Information Technology Policies, ITS deploys change-detection mechanisms (for example, file-integrity monitoring tools) to alert ITS staff to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configures the software to perform critical file comparisons at least weekly. (PCI Requirements 11.5)

6. Training regarding the testing of applicable systems is conducted annually pursuant to the Security Awareness and Training Policy. In addition, this policy, as well as other Information Technology Policies, and other applicable information technology security related policies are published at https://wiki.canisius.edu/xxIF4Ag (PCI Requirement 11.6)

Refer to the Information Technology Policies for additional system security testing control policies and procedures utilized by the college.

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment. (PCI Requirement 12)

1. This Payment Card Information Security Policy, as well as the college’s information technology security related policies, are published by the college at https://wiki.canisius.edu/vi4Ag and distributed to all appropriate college employees, contractors, vendors, service providers, and business partners. (PCI Requirement 12.1)

2. In accordance with the Information Technology Policies, ITS. (PCI Requirement 12.2)

a. Reviews all information security policies and where necessary updates the policies on at least an annual basis, or upon significant change to the Cardholder Data Environment (whichever happens first). The review process ensures that:

i. PCI DSS required policies in place are still required;

ii. Perceived threats facing are identified and consideration included in policy and associated control documentation;

iii. Any new legal issues are identified that require changes in current policy or associated controls;

iv. The college meets current PCI compliance standards;

v. Any changes to network configuration or new applications are included in the college’s security policy; and

b. Annually conducts a formal documented risk assessment process to identify key information systems that store, process, or transmit Cardholder Data, and potential threats and vulnerabilities which could impact on the security of those resources.

i. ITS develops a report that outlines strategies to efficiently and effectively mitigate the risks identified in the risk assessment process.

3. In addition to the requirements set forth in the Acceptable Use of College Computer and Network Systems Policy, the following acceptable use controls must be followed by all Authorized Users of applicable information systems that collect, process, maintain, use, share, disseminate or dispose of Cardholder Data and/or Sensitive Authentication Data to ensure proper usage of the Cardholder Data Environment: (PCI Requirement 12.3): a. Access to the systems and resources in the Cardholder Data Environment require explicit approval and authorization by a supervisor. Such authorization must be in accordance with the individual’s job responsibilities, and the individual must complete the appropriate training administered by ITS. Refer to Section 7 above, as well as the Access Control and Information Technology Personnel Security policies.

b. All Authorized Users accessing systems within the Cardholder Data Environment must use their own uniquely assigned Login ID and password. No individual is permitted to access the Cardholder Data Environment through the use of a shared or generic ID. Passwords or active sessions to any system must never be shared with another individual, as set forth in Section 8 above, as well as the Identification and Authentication and Password policies.
c. Student Records and Financial Services maintains an inventory of all assigned credit card swipe devices and other electronic payment systems in use at various units. All deployed devices are tagged in the college’s asset management system.

d. All Authorized Users with access to the Cardholder Data Environment must be maintained in a centralized repository maintained by the applicable Data Owner and ITS.

e. Any deployment of new products for the use of processing credit card transactions must be reviewed, assessed, and approved by the chief information officer.

f. Cardholder Data may not be copied or removed from the Cardholder Data Environment (all data must be contained within the secure environment). Access controls set forth in Sections 8 and 9 above must be in place to prohibit such action by any authorized individual, including access from a remote location. Refer also to the Information Technology Policies.

4. Cardholder Data security roles and responsibilities are defined in Section I above.

5. ITS, under the leadership of the CIO, performs the following Cardholder Data security management responsibilities: (PCI Requirement 12.5)

a. Develops and recommends to the CIO and president security policies and procedures;

i. Approved security policies and procedures are published at https://wiki.canisius.edu/x/VIJ4Ag;

b. Monitors and analyzes security alerts and information;

c. Distributes and escalates security alerts to appropriate college staff;

d. Develops and recommends to the CIO and president security incident response and escalation procedures to ensure timely and effective handling of all situations;

e. Administers administrative and authorized user accounts, including additions, deletions, and modifications; and

f. Monitors and controls all electronic access to Cardholder Data.

6. In accordance with the Information Technology Security Awareness and Training Policy, applicable staff are trained upon hire and at least annually regarding this Policy and its associated controls. (PCI Requirement 12.6)

a. Cardholder Data Environment security awareness training includes, but is not limited to, a review of the following:

i. Pin Entry Device tampering;

ii. The Identification and Authentication and Password policies;

1. Guidance on selecting strong authentication credentials;

2. Guidance for how users should protect their authentication credentials, and why sharing passwords is a poor security choice;

3. Why it is important not to reuse previously used passwords;

4. How to change passwords if there is any suspicion the password could be compromised.

iii. Suspicious behavior awareness and reporting incidents of tampering or substitution of POS devices to ITS.

b. In addition, applicable staff are required to acknowledge in writing at least annually that they have read and understand this policy and its associated controls.

c. ITS shall also ensure that third-party vendors covered by this Policy are familiar with these requirements.

d. Once a new policy has been introduced, following significant changes, and at least annually, all staff must acknowledge in writing or electronically the policy. This ensures that they have read and understood the policy (or changes) and accept any consequences should they fail to adhere to them.

e. Data Owners, Data Custodians, supervisors, and other applicable staff granted administrator access are given extra training to ensure they are aware of the significance of the data being held and the repercussions of disclosing it to those who do not have the need to know.

7. In accordance with the Personnel Security Policy, Human Resources is responsible for screening potential personnel prior to hire to minimize the risk of attacks from internal sources; (PCI Requirement 12.7)

8. Third-party vendors that process, transmit or store Card Holder Data for the college must be PCI DSS compliant and approved by the vice president for business and finance and the chief information officer. (PCI Requirement 12.8)

a. 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.

b. Annually, the chief information officer, in conjunction with applicable Data Owners, will verify third-party vendor compliance with PCI DSS standards.

9. 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. (PCI Requirement 12.9)

10. The college’s incident response procedures are tested annually and includes reporting requirements in the event of a suspected incident or breach involving Cardholder Data. (PCI Requirement 12.10)

RELATED POLICIES

Acceptable Use of College Computer and Network Systems Policy

Access Control Policy

Computer Assess Disposal Policy

Computer Asset Replacement Policy

Configuration Management Policy

Data Classification Policy

Identification and Authentication Policy

Information Security Program

Information Technology Security Awareness and Training Policy

Media Protection Policy

Password Policy

System and Information Integrity Policy