Amarillo College®

Information Security Plan

In compliance with the Gramm Leach Bliley Act of 1999

Information Security Plan

This Information Security Plan describes Amarillo College's safeguards to protect data, information, and resources as required under the Gramm Leach Bliley Act. These safeguards are designed to:

- Make reasonable efforts to ensure the security and confidentiality of covered data, information, and resources;
- protect against anticipated threats or hazards to the security or integrity of such information; and
- protect against unauthorized access to or use of covered data, information, and resources that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten covered data, information, and resources maintained by the College;
- manage and control these risks;
- implement and review the plan; and
- adjust the plan to reflect changes in technology, the sensitivity of covered data, information and resources, and internal or external threats to information security.

Identification and Assessment of Risks to Customer Information

The College recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of covered data, information, and resources by someone other than the owner of the covered data, information, and resources;
- compromised system security as a result of system access by an unauthorized person;
- interception of data during transmission;
- loss of data integrity;
- physical loss of data in a disaster;
- errors introduced into the system;
- corruption of data or systems;
- unauthorized access or distribution of covered data, information, and resources by employees, students, affiliates, or other constituencies;
- unauthorized requests for covered data, information, and resources;
- unauthorized access through hardcopy files or reports; and
- unauthorized transfer of covered data, information, and resources through third parties.

The College recognizes that this may not be a complete list of the risks associated with the protection of covered data, information, and resources. Since technology is not static, new risks arise regularly.

The College believes current safeguards are reasonable and, in light of current risk assessments, are in line with common practices to provide security and confidentiality to covered data, information, and resources maintained by the College. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information. However, the College cannot guarantee the unequivocal security of covered data, information, and resources given the evolving and ever-changing state of IT environments and threats thereto.

Information Security Plan Coordinators

The CIO and the Registrar have been appointed as the current coordinators of this plan. They are responsible for assessing the risks associated with unauthorized transfers of covered data, information, and resources. They are also responsible for implementing procedures to minimize those risks to the College and/or conducting audits of this plan on a periodic basis.

Design and Implementation of Safeguards Program

Employee Management and Training

Each department responsible for maintaining covered data, information, and resources is instructed to take steps to protect the information from destruction, loss, or damage due to environmental hazards, such as fire and water damage or technical failures. Further, each department responsible for maintaining covered data, information, and resources should coordinate with the plan coordinator(s) on an annual basis for the review of additional privacy training appropriate to the department. These training efforts should help minimize risk and safeguard covered data, information, and resources security. All employees and students are required to acknowledge the ITS Acceptable Use Policy as well which outlines the technology and its guidelines for acceptable use.

Physical Security

The College has addressed physical security by placing access restrictions at buildings, computer facilities, and records storage facilities containing covered data, information, and resources to permit access only to authorized individuals. These locations are to be locked, and only authorized employees are permitted to possess keys or digital combinations. Paper documents that contain covered data and information are to be shred at time of disposal.

Information Systems

Access to covered data, information, and resources via the College’s IT Infrastructure is limited to those employees who have a business reason to know such information. Each employee is assigned a set of unique credentials. Databases containing personal covered data, information, and resources including, but not limited to, accounts, balances, and transactional information are available only to College employees in appropriate departments and positions.

The College will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data, information, and resources are secure and to safeguard the integrity of records in storage and transmission. The College requires that all servers must be registered before being implemented in a College data center or before access to them is allowed through data center firewalls, thereby allowing verification that the system meets necessary security requirements as defined by the ITS Department. These requirements include maintaining the operating system and associated applications, application of appropriate patches, and updates in a timely fashion. Authentication is also required of users before they can access College-protected data. In addition, security systems have been implemented to assist with detection and mitigation of threats, along with procedures to handle security incidents when they do occur.

When reasonable, encryption technology will be utilized for both storage and transmission. All covered data, information, and resources will be maintained on servers that are behind a firewall.

Management of System Failures and Compromises

The College has developed written plans and procedures the AC IT Disaster Recovery Plan in case there is an incident or a major failure of IT services.

Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, external resources may be needed to provide services the College determines it cannot provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data, information, and resources, the evaluation process shall include the ability of the service provider to safeguard confidential financial information. Contracts with service providers may include the following provisions:

- An explicit acknowledgement that the contract allows the contract partner access to confidential information;
- a specific definition or description of the confidential information being provided;
- a stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- an assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information;
- a provision requiring the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;
- an agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract that, in turn, would allow the College to terminate the contract without penalty; and
- a provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

Information Technology Services General Security Considerations

Computer Labs

1. Computing labs are provided for use by AC students, faculty, and staff. In cases that a computer lab does not have logon authentication, individuals should have a valid College photo ID at all times while using the labs. Lab staff have the right to deny access to the labs to anyone without proper identification. Most Lab and tutoring areas require ID scans for check-in purposes.
2. Guests are allowed to use computer labs for a limited period of time when access has been requested by an authorized faculty or staff. Guest accounts are password protected.
3. The ITS Department reserves the right to disable lab connections that negatively impact the College network or pose a security risk.
4. Lab machines are prohibited from engaging in port scanning, traffic spamming/flooding, and other similar activities that negatively impact the College network and/or non-College networks.
5. Labs must not advertise network services that may compromise College network integrity or put lab information at risk.
6. Network equipment such as hubs, switches, routers, and wireless access points may not be placed in College labs without written authorization from the AC ITS Department.

Anti-Virus

1. All AC PC-based computers must have AC's standard, supported anti-virus software installed.
2. The anti-virus software and the virus definitions must be kept up-to-date.
3. Virus-infected computers may be removed from the network until they are confirmed to be virus-free.
4. Any activities with the intention to create and/or distribute malicious programs into AC's networks (e.g., viruses, worms, Trojan horses, etc.) are prohibited.

Network Control and Access

1. Anyone who uses the campus computing environment must be properly authorized.
2. Users must not
    - perform acts that negatively impact the operation of computers, peripherals, or networks or that impedes the ability of someone else to do his/her work;
    - attempt to circumvent protection schemes for access to data or systems; or
    - gain or grant unauthorized access to computers, devices, software, or data.
3. Users may be held legally and financially responsible for actions resulting from unauthorized use of College network and system accounts.
4. AC has installed various network security devices, including account passwords and firewalls, to help ensure the safety and security of College information. Any attempt to disable, defeat or circumvent any security facility is considered inappropriate activity and is a violation of this network policy.

5. Expansion or manipulation of network hardware and/or software, except by designated individuals within the ITS Department, without prior approval from the ITS Department, is strictly prohibited.
6. Prior to connecting any server to the College network, approval must be obtained in writing from the AC ITS Department.
7. Attachment of any the following devices to the campus network, other than those provided or approved by the ITS Department, is strictly prohibited:
   - DHCP servers
   - DNS servers
   - NAT routers
   - Packet capturing technology
   - Any device that disrupts or negatively impacts network operations
8. Static assignment of IP addresses must be approved and obtained through the ITS Department.
9. Only ITS Department staff or authorized agents may move College-owned networking and communications equipment.
10. The owners of data stored on network accessible systems are responsible for managing and determining the appropriateness of information stored on these systems. This includes both private storage areas and "shared" folder areas.
11. Only authorized merchants may use College networks, wired or wireless, to accept credit card payments. Merchants must also notify and receive approval from the ITS Department before using AC networks to accept payments and must comply with current Payment Card Industry Data Security Standards (PCI DSS).
12. DHCP and DNS Services – the ITS Department provides centralized and redundant DHCP and DNS services for the College. Due to the nature of these services, and because of the potential disruption of service and possible security breaches resulting from incorrect setup of additional systems, attachment of unauthorized DHCP or DNS servers is prohibited. The following guidelines must be followed when requesting or using any DHCP or DNS services:

   - By default, systems requiring an IP address must support DHCP and be capable of obtaining DHCP address information from one of the centrally administered College DHCP servers.
   - Using DHCP, devices requesting an IP address will be assigned a dynamic pool address from the subnet to which the device is attached. Devices with dynamically assigned IP addresses may have their address changed.
   - Reserved IP addresses needed for devices functioning as servers must be requested from the ITS Department. Once assigned, the IP address must be obtained by the machine via DHCP. The MAC address for any reserved IP address must be provided prior to assignment.
   - Static IP addresses to be hard-coded for specialized equipment incapable of using DHCP may be requested from the ITS Department. The MAC address for any statically assigned IP address must be provided prior to assignment.
   - The ITS Department must be informed of any changes to equipment utilizing reserved

or static IP addresses.

DNS Guidelines

- Any domain that is to be associated with AC's Class-B IP network must be registered with the ITS Department.
- Requests for assignment of DNS names must be for valid College purposes.
- DNS names ending in actx.edu are made available upon request at no charge for College approved services.
- DNS names for domains other than actx.edu and which are to be hosted on College systems, must be requested from the ITS Department. Any charges for initial or ongoing registration of the requested name are the responsibility of the requestor.
- The ITS Department will work with any user requesting a domain name to identify an appropriate and available name; however, the ITS Department has final approval for all DNS name assignments.
- DNS names, not in the actx.edu domain, will not be approved for use without justification. For any other domain name to be approved for use, it must be demonstrated that equivalent functionality cannot be provided under the existing actx.edu domain.

Security Assessment

1. Network and system security will be assessed on a periodic basis.
2. If a security concern is found, then the responsible party will be notified so the problem can be addressed. Depending on the severity of the concern, the device may be removed from the network.

End-User Devices (Workstations, Laptops, Tablets, Mobile Devices, etc.)

1. Users are responsible for the security and integrity of College information stored on their end-user devices, which includes controlling physical and network access to the equipment. This includes personally owned devices to the extent they access College IT services or contain College data of any kind. Storage of sensitive or personal covered data on mobile devices is strictly prohibited.
2. Users may not run or otherwise configure software or hardware that may allow access by unauthorized users.
3. Employees must not access College-owned end-user devices that have not been provided to them for their work without the express permission of their department head.
4. Employees accessing College IT services and systems with their own personal devices must adhere to all IT polices
5. Anti-virus software must be installed on all workstations/laptops that connect to the College network.

Software Licenses

1. Virtually all commercially developed software is copyrighted; and the users may use it only according to the terms of the license the College obtains.
2. Duplicating such software with the intent to redistribute or installing multiple instances of such

software without authorization is prohibited.

3. All users are legally liable to the license issuer or copyright holder.
4. Placing unlicensed or illegally obtained software, music, movies, or documents on College computers is strictly prohibited.

Physical Access

1. Access should only be granted to any person with proper authorization to access the corresponding area.
2. We comply with the College’s least required access for distribution of keys.
3. Unauthorized access to areas where personally identifiable information is stored is prohibited.
4. Supervisors must ensure that staff who (voluntarily) terminate or suspend their employment with the department return their physical access keys and cards on their last day of work in that unit.
5. Employees who are (involuntarily) dismissed from the institution must return their keys and other access control devices/cards at the time they are notified of their dismissal. Any access granted to access control devices/cards must be removed immediately.
6. If an employee does not return his/her keys, then areas controlled by the outstanding keys must be rekeyed.
7. College information or records may not be removed (or copied) from the office where they are kept except in performance of job responsibilities.
8. Access to AC IT Infrastructure operations areas shall be restricted to those responsible for operation and maintenance.
9. Access to AC’s Information Technology Services data center by non-ITS personnel is not permitted unless they are escorted by an authorized ITS staff member.
10. Key access is granted on an individual basis and in no case should be lent or given to others. Some units leverage electronic key cabinets to allows the physical keys to be a shared resource but under auditable conditions.
11. Computer installations should provide reasonable security measures to protect the computer system against natural disasters, accidents, loss or fluctuation of electrical power, and sabotage.
12. Adequate disaster recovery plans and procedures are required for critical systems data.

Servers

1. Administrative access to servers containing or processing protected data must be password protected.
2. Servers should be physically located in an access-controlled environment.
3. All servers deployed at AC must be approved by the ITS Department. Server maintenance plans must be established and maintained.
4. Network Services should be kept up-to-date with any changes to server information.
5. Operating system configuration should be in accordance with approved security best practices.
6. Services and applications that will not be used must be disabled where possible.
7. Access to services should be logged and/or protected through access-control methods if possible.
8. The most recent patches must be installed on the system as soon as practical.
9. Do not use accounts with elevated privileges (such as administrator or root) access when a non-

privileged account can be used.

10. Privileged access must be performed via an encrypted network protocol (such as SSH, HTTPS, RDP) and/or over an encrypted VPN tunnel).
11. Security-related events will be reported to the IT Department, who will review logs and prescribe corrective measures as needed. Security-related events include, but are not limited to:
    - Port-scanning or Distributed Denial of Service attacks.
    - Evidence of unauthorized access to privileged accounts.
    - Evidence of access to information by an unauthorized viewer.
    - Anomalous occurrences that are not related to specific applications on the host.

Passwords

1. Passwords are designed to prevent unauthorized access to information. Users are responsible for safeguarding passwords along with other authentication mechanisms (such as user names, PINs, etc.) and are accountable for negligent disclosure of passwords.
2. Passwords should be a minimum of 7 characters long and constructed of a combination of alpha and numeric characters. Must contain at least 1 number.
3. Passwords changes are required every 90 days at a minimum or immediately if compromised. Systems should automatically expire passwords at regular intervals and require the user to reset the password in accordance with the requirements for that system.
4. Passwords should be memorized and never written down.
5. AC accounts or passwords should not be shared with anyone. All passwords are to be treated as sensitive, confidential information.

Wireless Access

1. Wireless access points not sanctioned by the AC ITS Department are prohibited.

Destruction and Disposal of Information and Devices

1. Confidential information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons. Physical documents must be shredded.
2. When donating, selling, transferring, surplusing, or disposing of computers or removable media, care must be taken to ensure that confidential data is rendered unreadable. Any restricted information that is stored must be thoroughly destroyed. In general, it is insufficient to "delete" the information, as it may remain on the medium. The data should be properly removed from the drive either by software that meets U.S. Department of Defense specifications or the drive may be physically destroyed.

Employee Training and Management

1. Each department is responsible for ensuring its employees are trained to take steps to maintain security, confidentiality, and integrity of personal information, such as:
    - securing rooms and cabinets where records are kept;
    - using strong passwords and not posting, sharing, or releasing passwords;
    - recognizing any fraudulent attempt to obtain student information and reporting it to appropriate department or law enforcement agencies; and

- reviewing all ITS Policies.

Sensitive Data Protection

Special care and awareness is required with regard to “sensitive data.” Sensitive data are any data that the unwarranted and/or unauthorized disclosure of such would have an adverse effect on the institution or individuals to which it pertains. Unauthorized disclosure or mishandling of sensitive data can be a violation of federal and state law and the College and its employees can be held personally liable for damages or remediation costs.

Data related to identity theft such as social security numbers (SSN), credit card numbers, bank account information, driver’s license, name, address, birthdate, passwords, Personal Identification Numbers (PINs), and ID pictures are of particular concern as all or most of this information is collected in the course of College business. Other types of data such as medical information, tax returns, donor information, mailing lists, scholarship information, financial information, and bidding information are examples of data that could require confidential handling or restricted access. These examples are not exhaustive or all inclusive. It is the responsibility of College employees handling any College data to understand what data are sensitive and confidential and to adhere to the following guidelines and any applicable regulations. Employees should contact College legal counsel if they are unsure whether or not data is considered sensitive.

1. Employees must not collect and/or store SSNs unless it is required by a federal or state agency and there is no other option in terms of unique identifier. If collection and storage of SSNs are required for operations in a given unit, the ITS Department must work with and approve and understand why the SSNs must be utilized and how and where they are being collected/stored.
2. Data should be stored in as few places as possible and duplicated only when necessary. Unless absolutely necessary, data should be stored on central administrative systems only.
3. Employees must never upload, post, or otherwise make available any kind of sensitive data on a web server even for short periods of time. Individuals responsible for maintaining web site content must be particularly cognizant and vigilant regarding this matter.
4. Employees must inventory and identify the data under their control that is external to central administrative systems. Additionally, they must know what data they have and in what form (electronic, paper, etc.) it exists. Data files should be purged or deleted in a timely manner to minimize risk.
5. Employees must not use shared network drives to share or exchange data unless they are certain that access to those shared drive resources is restricted to individuals authorized to handle such data.
6. Transmission of any sensitive data should be encrypted. Websites should use HTTPS encryption if they collect data. Unencrypted protocols should be abandoned in favor of their encrypted counterparts (i.e. abandon Telnet in favor of SSH, or abandon FTP in favor of SFTP). Employees who have doubts or concerns should contact the ITS Service Desk.
7. Employees must not release AC data of any kind to 3rd party (non- AC) entities for any reason unless such entities have agreed in writing to restrict the use of such data to the specific and intended purposes authorized by the AC department or unit enlisting the services of the 3rd

party entity. Any AC department or unit releasing data to a non-AC 3rd party entity is responsible for how the data are used (misused). Release of highly sensitive and confidential data (beyond FERPA allowed "directory information") is prohibited.

8. Employees must not send, receive, or store any sensitive data using email under any circumstances. Email is not secure unless using the ITS approved secure methods.
9. Under no circumstances should credit card numbers be collected and stored on standalone devices, digital media, or paper media. Processing credit card numbers should be done via secure methods that authorize or deny the transaction in real time but do not retain or store the credit card number. Collecting credit card numbers via phone calls, websites, or email and retaining such numbers on paper or in electronic files for periodic processing is bad practice and insecure. Employees who need help processing credit cards securely should contact the ITS Service Desk.

Privacy Notices

Web Privacy Statement

Amarillo College is committed to ensuring the privacy of personal information. We do not actively share personal information gathered from our web servers. However, because Amarillo College is a public institution, some information collected from the Amarillo College website, including summary server log information, emails, and information collected from web-based forms, may be subject to release. This means that while we do not share or sell information unless solicited, in some cases we may be compelled by the Texas Open Records Act to release information.

Student directory information for both resident and distance students is routinely requested by vendors through the Texas Public Information Act. If a student does not wish for this public information to be released, he/she is responsible for notifying the Registrar’s Office, located in the Student Service Center, in writing by the 12th class day each regular semester and by the 4th class day of the summer term.

Employees (faculty and staff) can restrict access to public information by completing the appropriate documents in the Human Resources office.

Amarillo College complies with the Family Educational Rights and Privacy Act (FERPA), which prohibits the release of education records without student permission.

The Amarillo College web consists of several web servers. Some servers hosted by Amarillo College may adopt different privacy statements as their specific needs require. If another Amarillo College web server has a privacy statement that is different from this notice, that statement will be posted on their site.

The Amarillo College website contains links to external websites. The College is not responsible for the privacy practices or content of external web links.

Information We Gather

The following information may be collected and stored automatically from all users accessing the Amarillo College website to browse or download information:

- Internet address of computer being used
- Web pages requested
- Referring web page
- Date and time
- Type of web browser being used

This information is used to occasionally create summary statistics which are used for purposes such as assessing what information is of most interest to users, determining technical design specifications, and identifying system performance or problem areas. This information is not reported or used in any manner that would reveal personally identifiable information, and will not be released to outside (third) parties unless legally required.

Personal Information

Amarillo College does not retain personally identifiable information about you when you visit our web sites unless you choose to provide such information to us (i.e. sending an email, participating in a survey, responding to a request for information or "contact us" form, etc.). We consider any information that could reasonably be used to identify you as "personally identifying information." This includes, but is not limited to:

- name
- address
- email address
- Social Security Number
- Any combination of data that could be used to identify you such as your birth date, your zip code and your gender.

If you provide personal information in an email or by completing a form and submitting it through our website, we may use that information to respond to your message and to help us get you the information you have requested. We do not collect personal information from such communications for any purpose other than to respond to you. We do not collect information for commercial marketing.

Security and Accuracy of Personal and Confidential Information
Although no computer system is 100 percent secure, Amarillo College has deployed extensive security measures to protect against the loss, misuse, or alteration of the information under our control.
If you are concerned about the accuracy of information contained in your personal records, you should refer to the appropriate custodian of record. The Registrar is custodian of all records for currently enrolled students and for all official academic records. The Vice President of Student Affairs is custodian of all other student records. Vice President for Human Resources is the custodian of all employee records (faculty and staff).

Off-Site Links
Links to non-Amarillo College organizations are provided solely as a service to our users. These links do not constitute an endorsement of these organizations or their programs by Amarillo College, and none should be inferred. Amarillo College is not responsible for the content found at these links.

Questions
If you have questions about this privacy statement or you believe that your personal information has been

released without your consent, send email to humanresources@actx.edu

Notification of Rights Under FERPA

The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their education records, including:

1. The right to inspect and review the student's education records within 45 days of the day the College receives a request for access. Students should submit to the registrar, dean, head of the academic department, or other appropriate official, a written request that identifies the record(s) they wish to inspect. The College official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the College official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.
2. The right to request that inaccurate or misleading information in the student's record be amended. Students may ask the College to amend a record that they believe is inaccurate or misleading. They should write the College official responsible for the record, clearly identify the part of the record they want changed, and specify why it is inaccurate or misleading. If the College decides not to amend the record as requested by the student, the College will notify the student of the decision and advise the student of his or her right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.
3. The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent, including:
    a. Disclosure without the student's consent is permissible to school officials with legitimate educational interests. A school official is a person employed by the College in an administrative, supervisory, academic, research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the College has contracted (such as an attorney, auditor, or collection agent); a person serving on the Board of Regents; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.
    b. FERPA allows the institution to routinely release information defined as "directory information." The following student information is included in the definition: the student's name, address, e-mail address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, enrollment status (including full-time, part-time, not enrolled, withdrawn and date of withdrawal), degree and awards received, and the most recent previous education agency or institution attended by the student. When a student wants any part of the directory information to remain confidential, an official request form must be completed in the Office of the Registrar within the first five days of class of each school term.

4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by Amarillo College to comply with the requirements of FERPA. The name and address of the Office that administers FERPA is:

   Family Policy Compliance Office
   U.S. Department of Education
   400 Maryland Avenue, S.W.
   Washington, DC 20202-5920

Incident Reporting

AC employees must immediately report the following to their managers or Office of Human Resources

- Any actual or suspected security incident that involves unauthorized access to electronic systems owned or operated by AC;
- malicious alteration or destruction of data, information, or communications;
- unauthorized interception or monitoring of communications;
- any deliberate and unauthorized destruction or damage of IT resources; and unauthorized disclosure or modification of electronic institutional or personal information.

Incident reports will be treated as confidential unless there is a need to release specific information. All incident reports will be investigated and handled appropriately.

Continuous Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within the ITS Department where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation, and maintenance of the plan will be the responsibility of the designated Information Security Plan Coordinators who will assign specific responsibility for implementation and administration as appropriate. The Coordinators, in consultation with the Office of General Counsel, will review the standards set forth in this plan and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security. The CIO for Information Technology Services will be responsible for maintaining the most current version of this plan and keeping it updated.

Revision History

- July, 2019: created and approved.
- Reviewed August 21, 2019
- Reviewed/Edited November 19, 2019