Sinclair Community College

INFORMATION SECURITY POLICY

Approved: April 11, 2006
By: Sinclair Board of Trustees
Revised: October 11, 2019

Sinclair College Information Security Policy

Sinclair College recognizes that all information assets created, collected, used, and maintained by the college in the course of conducting our teaching, learning, and public service mission are subject to varying degrees of concern regarding security and privacy. All information assets and supporting infrastructure provided by the college are the property of Sinclair College; however, the college recognizes that intellectual property and copyright laws may supersede college ownership of specific file content. This policy strives to optimally balance the principles of academic freedom and freedom of speech with the precepts of effective information security—confidentiality, integrity, and availability.

Purpose

The purpose of this policy is to formally establish an information security program within the college. Most of Sinclair College's financial, administrative, and student systems are accessible through the campus network. As such, they are vulnerable to security breaches that may compromise sensitive information and expose the college to asset losses and other risks. An information security program is necessary to ensure that the college:

- Establishes a college-wide approach to information security, including appropriate security awareness training and education for constituents.
- Complies with federal and state statutes and regulations regarding the collection, maintenance, use, and security of information assets.
- Establishes and implements prudent, reasonable and effective practices for the protection and security of information assets, including protection of sensitive and confidential information against accidental or deliberate unauthorized disclosure, modification or destruction.
- Develops effective mechanisms for responding to real or perceived incidents involving breaches of information security.

This policy establishes a program charged with ensuring the college meets or exceeds its legal and ethical responsibilities for securing its critical and sensitive information assets.

Policy Statement

It is the policy of Sinclair College to protect its information assets in accordance with all applicable federal and state statutes and regulations, as well as with effective information security practices and principles generally accepted as 'due diligence' within the higher education community.

The college specifically prohibits unauthorized access to, tampering with, deliberately introducing inaccuracies to, or causing loss of Sinclair's information assets. It also prohibits using information assets to violate any law, commit an intentional breach of confidentiality or privacy, compromise the performance of systems, damage software, physical devices or networks, or otherwise sabotage college information assets.

Sinclair College protects its information assets from threats and exploits, whether internal or external, deliberate or accidental. The degree of protection is based on the nature of the resource and its intended use. The college recognizes that no single office, policy, or procedure provides absolute security, therefore, all college employees and other stakeholders share responsibility to minimize risks and to secure the information assets within their control.

A formal information security program, guided by the Chief Information Security Officer (CISO), has been established within the college. Individuals within the information security organizational structure of the program are empowered to research, develop, implement, and disseminate operational policies, procedures, standards, guidelines, and other processes to support effective information security practices.

The vice president of each division shall be responsible for ensuring appropriate and auditable information security controls are practiced within their division. Each division shall appoint an information security officer to partner with the CISO to develop, implement, and maintain appropriate and effective information security practices.

Campus-wide security awareness, training, and education are vital to information security. Therefore, each division shall develop and document methods for ensuring that information security responsibilities regarding to applicable laws, regulations, guidelines and policies is distributed and readily available to stakeholders.

The college shall take appropriate action in response to misuse of college information assets. Any violation of this policy may result in legal action and/or college disciplinary action under applicable college and administrative policies and procedures. Distribution of specific procedures implementing this policy includes, but is not limited to, web pages, email, and printed documentation.

The Chief Information Security Officer will review the Information Security Program annually and report the result of this review to the President.

Information Security Program

Table of Contents

1. Information Security Program Overview:

Sinclair College recognizes that all information assets created, collected, used, and maintained by the college in the course of conducting our learning, research, and community/public service mission are subject to varying degrees of concern regarding security and privacy. Information assets include all data and all methods and devices used to create, store, and manage the data. Examples include information stored on computers, transmitted across networks or telecommunication devices, printed or written on paper, or stored on removable media. All information assets and supporting infrastructure provided by the college are the property of Sinclair College. Accordingly, the college reserves the right, and may be obligated by statutes, to manage and protect these assets. However, the college recognizes that intellectual property and copyright laws may supersede college ownership of specific file content. The college encourages the use of its information assets to share information, to improve communication, and to exchange ideas in support of the learning mission. This policy strives to promote a balance between the principles of academic freedom and freedom of speech, and the requirements for information security.

To protect critical information and information systems, and to comply with applicable legislation, the Sinclair College Board of Trustees formally adopted Sinclair's Information Security Policy. This policy serves as a charter and establishes a comprehensive Information Security Program. The primary function of the program is to establish a framework to assist in formalizing the implementation of the most current effective practices in the college information environment and institutional information security procedures. While these practices mostly affect the IT Department, some of them impact diverse areas of the college, including but not limited to: Admissions; Bursar; Business Services; Financial Aid; General Accounting; Research, Analytics and Reporting; Registration and Student Records; and many third party contractors.

2. Program Purpose and Objective

The purpose of the information security program is to ensure the confidentiality, integrity, and availability of student and other stakeholder information and the systems housing this information. The objective is to protect the college's information assets from threats and exploits, whether internal or external, deliberate or accidental.

The college maintains its information resources to fulfill its mission. The overall objectives of this program are to:

- Define, establish, and maintain an organizational structure for protecting Sinclair's information assets;
- Implement a risk-based approach to protect information assets against anticipated threats, particularly to protect against loss of, unauthorized access to, or improper use of, information that could result in substantial harm or inconvenience to the college or any stakeholder;
- Provide college stakeholders with the highest level of service while protecting information assets and integrating information security across all essential activities.
- Identify issues that have resulted or may result in a breach of information assets, to respond to, mitigate damages resulting from, and prevent recurrence of information security issues.
- Maintain all Federal, State, International, and industry-specific compliance obligations.
- Develop processes college stakeholders use to foster security of information assets.

3. Program Elements

The program consists of four fundamental elements: (3.1) Establishing information security organization, roles & responsibilities; (3.2) Defining information security standards and principles (3.3) Specifying baseline security program controls and (3.4) Continual evaluation and adjustment of the program.

3.1. Information Security Organization — Roles and Responsibilities

Effective and efficient information security programs require clear direction and commitment from top management and administration. Information security is an integrated function that requires effective organization and collaboration throughout the college.

The Sinclair Board of Trustees is ultimately accountable for governance as a whole. The management and control of information security risks is an integral part of governance. In practice, however, the Board explicitly delegates executive responsibilities for most governance matters to Sinclair's President. Sinclair's President gives overall strategic direction by approving and mandating the information security principles and policy, but generally delegates operational responsibilities for the information security program to individual staff members as deemed appropriate. The formally defined and delegated organizational roles and responsibilities include:

3.1.1. Division Vice Presidents

Division Vice-Presidents are the offices of primary responsibility (OPR) for information collected, maintained, and/or that has been identified as primarily utilized or "owned" by their respective divisions. Vice-Presidents may delegate operational management of these responsibilities by designation of an Information Security Officer (ISO) within their respective divisions. Vice Presidents may also designate other responsible party(ies) to work with the ISO to assist in implementing this program. These designated individuals ensure information assets within their span of control have designated responsible parties (owners), that risk assessments are carried out for the division, and that mitigation processes based upon those risks take place. The designated responsible party reports the status of the Information Security Program within the division as appropriate.

3.1.2. Deans, Directors, Chairs, Managers, and other Supervisors:

Deans, Directors, Chairs, Managers, and other supervisors responsible for managing employees with access to information and information systems are responsible for specifying, implementing and enforcing the specific information security controls applicable to their respective areas. This includes ensuring all employees understand their individual responsibilities related to information security, particularly when accessing, processing, or transmitting sensitive or confidential information. Supervisors are responsible for ensuring employees have the access required, and only the access required, to perform their jobs. Supervisors should periodically review their employees' access levels to ensure they are still appropriate, and take appropriate action to correct discrepancies/deficiencies. Supervisors must proactively notify Human Resources and the IT Help Desk of any change in employment status that impacts access requirements. Supervisors are also responsible for reporting suspected misuse or other information security incidents to the CISO or other appropriate party.

3.1.3. Chief Information Security Officer (CISO)

The Sinclair College Chief Information Security Officer (CISO) is designated as the Program Officer responsible for coordinating and overseeing the Information Security Program. The CISO must work closely with the various divisions and departments throughout the campus. The CISO may recommend that Vice-Presidents of specific divisions delegate other representatives of the Institution to oversee and coordinate particular elements of the Program. The CISO also assists individuals who have the responsibility and authority for information (owners) with information security best practices relating to issues such as: establishing and disseminating enforceable rules regarding access to and acceptable use of information resources; conducting/coordinating information security risk assessment and analysis; establishing reasonable and effective security guidelines and measures to protect data and systems; assisting with monitoring and management of systems security vulnerabilities; conducting/coordinating information security audits; and assisting with investigations/resolution of problems and/or alleged violations of college policies. Questions/issues regarding the information security program or interpretation of this document should be initially directed to the CISO.

3.1.4. Administrative System Information Security Team

The primary repository for information covered by this policy is Sinclair's Administrative and Student Information System, the (Ellucian) Colleague System. The Administrative System Information Security Team authorizes and/or approves all access to Colleague. The team is charged to develop and implement proactive measures to ensure administrative application security controls provide sufficient granularity to allow appropriate access to the information stakeholders required to successfully perform their duties, while meeting the college's legal and ethical obligations to protect private, sensitive, and critical information. The team's primary responsibility is to develop processes and standards to provide optimal availability, integrity, and confidentiality of administrative system information, including processes for:

(1) users to request initial access;
(2) users to request access changes;
(3) documentation of user access authorized, as well as user/supervisor rights and responsibilities; and
(4) resolution of security-related conflicts and issues.

Primary/authoritative members of the team include the Division Information Security Officers and the Chief Information Security Officer. Associate/advisory members of the team are Department Information Security Officers and Enterprise Application Administrators. Specific responsibilities and procedures are detailed in the college's Administrative System Security Standards.

3.1.5. Computer Security Incident Response Team (CSIRT)

The Computer Security Incident Response Team is responsible for providing information and assistance to stakeholders in implementing proactive measures to reduce the risks of computer security incidents, investigating, responding to and minimizing damage from such incidents when they occur. The team is also responsible for determining/recommending required follow-up actions resulting from incidents. The CSIRT is essentially a two-layer team: 1) An operational team is charged with initial identification, response, triage, and determining escalation requirements. The operational team consists of the CISO and delegated IT staff members from the Information Technology Department, and Campus Police if criminal activity is suspected. 2) A management team is charged with college response to major or significant incidents. Primary management team members include the Chief Information Officer (CIO), CISO, Chief of Campus Police, Assistant Director of IT Operations, Assistant Director of IT Applications, Assistant Director of IT Systems, Director of Public Affairs, a Business Services Advisor, a Legal Advisor, a Human Resources Advisor, and delegates with technical or business expertise specifically appointed by the Vice Presidents of the college. Associate members of the team include the information "owner" and may also include any stakeholder involved in the specific incident handling or notification process on an as-needed basis. Specific responsibilities and procedures are detailed in Sinclair's Computer Security Incident Response Standards.

3.1.6. Information Technology (IT) Department

The IT Department is led by the CIO, who is responsible for the college's information technology capabilities, including information security. The CIO is supported by the Information Technology

Management Team which includes the CISO, Assistant Director of IT Operations, Assistant Director of IT Applications, and Assistant Director of IT Systems.

The IT Department is primarily responsible for all technical information security controls. IT is primarily responsible for integration of technical information security tools, controls, and practices in the network environment, and is also often the end-users initial contact for reporting suspected information security failure or incidents. IT staff must follow information security best practices for managing infrastructure and services. IT is also primarily responsible for developing, practicing, integrating, and implementing security best practices for the college's applications such as the administrative system and Web systems/applications, and is responsible for training (Web) application administrators and developers in using application security principles to make existing and new applications more secure.

3.1.7. Employees with Access to information:

Employees (including Student employees) with access to information and information systems must abide by applicable college policies and procedures, as well as any additional practices or procedures established by their unit heads or directors. Employees must use and safeguard covered information as governed by the regulations and the duties and responsibilities of their position. This includes understanding the classification of the information used to perform their duties and securely accessing, processing, or transmitting sensitive or confidential information. Employee responsibility includes protection of their account password and any other protection the account has, as well as reporting suspected misuse or information security incidents to the appropriate party (usually their supervisor).

3.1.8. Temporary staff, consultants, service providers

Temporary staff members (including student workers) are considered employees and have the same responsibilities as regular full- or part-time employees with access to information and information systems. Supervisors of temporary employees have the responsibilities outlined in paragraph 2 of this section.

Consultants, service providers, and other contracted third parties may be granted access to information on a 'need to know' basis. If a third party requires a network account, a Sinclair employee must 'sponsor' the third party by submitting a Service Request to the IT Help Desk. These accounts require a dean or director equivalent (or higher administration member) approval. It is the sponsor's responsibility to ensure the third party user understands the individual responsibilities related to the network account. The user is responsible for the security of his/her password(s) and accountable for any activity resulting from the use of his/her user ID(s) within reasonable scope of his/her control. Third party network accounts will be active for a maximum of one year. If account access is no longer required before a year's time has elapsed, it is the sponsor's responsibility to notify IT to cancel the network account. If the account is needed for more than one year, it is the sponsor's responsibility to renew the account prior to the expiration date by submitting an updated request.

Third parties shall implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentially, integrity, and availability of all electronically managed information. Upon termination of services, third parties will also return all information or certify destruction of information according to the agreement and/or specific terms of the contract. Third party providers are also responsible for protection of account and password(s) and any other protection the account has, as well as reporting suspected misuse or information security incidents to the appropriate party. In the event of an information security incident caused by a third party provider, the third party may be held liable for legal repercussions and expenses related to recovery/disclosure activities.

3.1.10. Students, community members

Students and community members are primarily responsible for the integrity of their own information and for reporting discrepancies to the appropriate office. All students and community members who are granted IT accounts must comply with Sinclair's Acceptable Use of Information Technology Policy. This includes being responsible for all activity conducted via their college IT accounts within reasonable control, including protection of their passwords and any other protection the accounts have, as well as reporting suspected misuse or information security incidents.

3.2. Key Information Security Concepts & Principles

3.2.1. Confidentiality

Confidentiality is the principle that information and information systems are only available to authorized users, that that they are only used for authorized purposes, and they are only accessed in an authorized manner. Confidentiality also determines information disclosure authority and conditions; unauthorized disclosure or use of confidential information could be harmful or prejudicial. The 'official' definition of confidentiality is: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]

3.2.2. Integrity

Integrity is the principle that safeguards reliability, accuracy, and completeness of information assets. Integrity safeguards ensure modifications are not made by unauthorized users and that unauthorized modifications are not made by authorized users. Integrity controls also ensure information is current and has not been altered or damaged. The 'official' definition of integrity is: Guarding against improper information modification or destruction, including ensuring information non–repudiation and authenticity. [44 U.S.C., SEC. 3542]

3.2.3. Availability

Availability is the principle that means that information assets are available and usable by authorized users when and where they need them. It is primarily used in the context of system availability. The 'official' definition of availability is: Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]

3.2.4. Identification

Identification is the means by which a user claims their identity to a system—who is the user? The most common example is the UserID. This identification entity is commonly used for access control; identification is necessary for authentication and authorization

3.2.5. Authentication

Authentication is the testing or reconciliation of evidence of users' identities. It establishes the user's identity and ensures that the user proves he, she, or it is who they claim they are. The most common example of an authentication entity is a password. Single factor authentication (requiring a single challenge to validate identity) is commonly used for routine access control; multifactor authentication should be considered for sensitive or critical assets.

3.2.6. Authorization

Authorization is the granting of rights and permissions to an individual (or process) that enables access to an information resource. Once a user's identity and authentication are established, authorization levels determine the extent of system rights that an operator can hold. Examples of authorization entities are access control lists and security classes.

3.2.7. Accountability

Accountability refers to a system's capability to determine and track the actions and behaviors of a single individual within a system, and to identify that particular individual; accountability is also sometimes referred to as non-repudiation. Audit trails and system logs support accountability.

3.2.8. Privacy

Privacy relates to the level of confidentiality and control granted to the user or individual subject of the information within a system. Privacy measures protect an individual's ability to determine what information is collected about them, who can access the information, how it may be used, and how it may be maintained. Loosely, privacy is to individual information (personal) what confidentiality is to corporate information (trade secret).

3.3 Security Program Baseline Controls

Sinclair's Information Security Program is multi-faceted and includes controls designed to address the confidentiality, integrity, and availability of information assets. Where deemed necessary, the college has established operational policies and procedures to facilitate support of these controls. Baseline controls addressed by the security policy include, but are not limited to:

3.3.1. Access Control

- Sinclair controls information asset access to authorized users, to processes acting on behalf of authorized users, or to authorized devices (including other information systems).
- Sinclair controls information asset access to transactions and functions that authorized users are permitted to execute in accordance with their role supporting the college.

3.3.2. Awareness and Training

- Sinclair ensures that managers, systems administrators, and users of organizational information assets are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information assets.
- Security Awareness Training is provided to all employees to ensure they are adequately trained to carry out their assigned information asset protection related duties and responsibilities.

3.3.3. Audit and Accountability

- Sinclair creates, protects, and retains information system audit records to the extent needed to support monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information asset activity.
- Sinclair takes reasonable effort to ensure the actions of individual information system users can be uniquely traced to those users, and administrative and technical policy is used to ensure they can be held accountable for their actions.

3.3.4. Configuration Management

- Configuration baselines and inventories are established and maintained for organizational information assets (including hardware, software, firmware, and documentation) throughout the respective system development lifecycles.
- Sinclair establishes and enforces security configuration settings for information technology products employed in organizational information systems.

3.3.5. Identification and Authentication

- Information asset users, processes acting on behalf of users, or devices are identified.
- Sinclair authenticates (or verifies) the identities of those users, processes, or devices as a prerequisite to allowing access to organizational information assets.

3.3.6. Incident Response

- An operational incident-handling capability has been developed and implemented for information assets that house or access Sinclair controlled information. The incident response capability includes a defined plan that addresses the seven stages of incident response:
    - Preparation/Preliminary Activities
    - Detection
    - Reporting & Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Activity
- Incidents will be tracked, documented, and reported to appropriate personnel and/or authorities both internal and external to the college IAW Sinclair policies and compliance requirements.

3.3.7. Maintenance

- Sinclair routinely maintains its information assets using effective industry-wide standards based on the nature of the information system or asset.
- All tools, techniques, mechanisms, and personnel used to conduct information system maintenance are used IAW vendor and/or other appropriate specifications and guidelines. Controls are in place and enforced for all systems involving non-public information.

3.3.8. Media Protection

- All sensitive/non-public information is required to be protected by appropriate media protection mechanisms (i.e. encryption) to ensure the highest levels of security when stored out of non-IT managed assets.
- Non-public information is required to be protected to ensure the highest levels of confidentiality, integrity and availability in all media formats.
- Sinclair policy restricts access to non-public information on any media to authorized users.
- Information system media containing non-public information is required to be sanitized or destroyed before disposal or release for reuse.

3.3.9. Personnel Security

- Nearly every Sinclair employee requires access to college information assets to support the college mission. The college has implemented multiple personnel security controls.
    - Prior to Employment:
        - All candidates for employment undergo background checks IAW college policy and appropriate laws.
        - Contractual agreements with employees and contractors outline responsibilities of the individual/contractor to information security.
    - During Employment:
        - Management is responsible for ensuring all employees and contractors adhere to applicable information policies and procedures within the organization.
        - All employees must undergo awareness training based on their roles, as well as review of policies and procedures applicable to their jobs.
        - There is a formal, communicated process to take action against employee(s) or contractor(s) when a failure to comply with security requirements occurs.
    - Termination or Change of Employment:

        - Sinclair processes ensure that appropriate access changes to information assets are addressed during and after personnel actions such as terminations and transfers.
        - Human Resources termination process includes exit interviews and appropriate handling of Sinclair property in possession or control of the affected personnel.
- Sinclair ensures that appropriate access to information assets containing non-public and/or sensitive information is specifically prioritized and addressed during and after personnel actions such as terminations and transfers.

3.3.10. Physical Protection

- As a Public institution, Sinclair employs a layered and flexible approach to protection and monitoring of the physical facility and support infrastructure for information assets.
    - Physical Access and Security:
        - Sinclair limits physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals based on role of the individual and classification of the asset.
        - Sinclair maintains a list of personnel with authorized access to facility areas where sensitive information systems (such as server rooms, network closets) are physically located.
        - Sinclair has established access control and credentialing processes for sensitive locations.
        - Audit logs of physical access are be maintained and reviewed as appropriate.
        - Sinclair policy requires escort of visitors and monitoring of visitor activity in physically sensitive areas.
    - Environmental Security:
        - The college has developed a Disaster Recovery and Business Continuity Plan to address protection against natural disasters or other malicious attacks, as well as accidental incidents.
        - Whenever feasible, Sinclair situates power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction.
        - Sinclair Facilities Management has implemented standards and processes addressing security measures for offices, conference rooms, classrooms, etc., including considerations for temperature, protection against water damage, and emergency lighting.
    - Asset Security:
        - All college assets are required to be appropriately maintained.
        - Physical removal of assets requires appropriate authorization and follows established procedures.

3.3.11. Risk Management

- Sinclair will periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the college's information assets and the associated processing, storage, or transmission of information.
    - Risk Assessment and Mitigation:
        - Security risk tolerance level should be defined, documented, and communicated across the college via a "risk register".
        - Security risk assessment criteria should be defined in order to produce consistent assessment results.

        - Risk assessments shall be performed upon initial acquisition of Sinclair-owned information asset and prior to establishment of service agreements with third parties. The risk assessment shall be reviewed and updated as appropriate, either at a specified time interval or when significant change is made to the information asset.
        - Routine vulnerability scans of information assets should be conducted prior to implementation and periodically. Detected vulnerabilities should be mitigated based IAW risk and classification of the asset
    - Third-Party Risk Management:
        - Prior to engaging a third party information services provider, risk assessment must be conducted IAW the IT checklist and other related Sinclair contracting policies.
        - Where appropriate, third parties must provide documentation around their own risk management procedures, staffing requirements, recordkeeping, and security processes.
    - Security Performance and Metrics:
        - The CISO should determine what needs to be monitored and measured to demonstrate effectiveness of security and overall risk management processes (e.g. incident reporting, and decrease in overall incidents).

3.3.12. Security Assessment

- The college periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
- Security and vulnerability assessments are routinely performed by internal staff. A periodic assessment should be performed by third-party provider at periodic intervals to ensure appropriate levels of coverage and oversight.
- Sinclair will develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.
- Information system security controls with be monitored on an ongoing basis to ensure the continued effectiveness of the controls.

3.3.13. System and Communications Protection

- Sinclair will monitor, control, and protect organizational communications (i.e. information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- Architectural designs, software development techniques, and systems engineering principles will be employed to promote effective information security within organizational information systems.
    - Information Transfer:
        - Unauthorized and unintended information transfer via shared system resources should be prevented.
        - Sinclair should prevent remote devices from simultaneously establishing local connections with the information system and communicating via some other connection to resources in external networks (i.e. proxy local access).
        - Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
        - Network communications traffic will be denied by default and network communications traffic will be allowed by exception (i.e. deny all, permit by exception).
        - External parties must agree to securely transfer data.

- Cryptographic Controls:
    - Cryptographic mechanisms are implemented to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical safeguards.
    - Sinclair will establishes and manages keys for cryptography employed in the information system. Cryptographic keys should be protected through their whole lifecycle.
    - Cryptography is used to protect the confidentiality of sensitive/non-public information in all systems that support cryptography.
    - All cryptographic keys should be protected against modification and loss; secret/private keys must be protected against unauthorized use/disclosure.
    - Equipment used to generate, store, and archive keys should be physically protected.

3.3.14. System and Information Integrity

- Sinclair will identify, report, and correct information and information system flaws in a timely manner.
- Sinclair will provide protection from malicious code at appropriate locations within organizational information systems.
- Information system security alerts and advisories will be monitored and appropriate actions will be taken in response.

3.4. Continual evaluation and adjustment of the program

The CISO, working with responsible units and offices, will evaluate and adjust the Information Security Program in light of the results of risk identification and assessment activities undertaken pursuant to the Program, testing and monitoring, as well as any material changes to operations or business arrangements, and any other circumstances which may reasonably have an impact on the Information Security Program.

The CISO will prepare an annual report on the status of the Information Security Program and provide that to the CIO. The CISO may prepare more frequent reports as necessary or requested. These reports may include copies of any unit-specific security plans, current risk assessments for each unit with access to covered data, a statement on the controls in place to mitigate those risks and the effectiveness of those controls, summaries of monitoring activities, actions taken or to be taken to correct any security concerns identified through monitoring, and such other information as required to provide assurance that this Information Security Program is implemented and maintained.

4. Related references

Sinclair College Board Approved Policies
Acceptable Use of Information Technology Policy

Operational Policies, Procedures, Standards, and Guidelines
Sinclair Policies Library
Human Resources Policies
Student Conduct and Safety
Public Safety Website
Privacy Statement
Information Technology Department Website
Sinclair Information Security Website

-HEOA Compliance
-Data Classification
-Computer Security Incident Response
-Risk identification and assessment