Sinclair Community College

POLICY MANUAL

Policy:		Policy No. X3.1	Page: 1 of 1
Information Security Policy		Issue No. 3.1.1	Issue Date: 4/11/06
Scope:	Effective Date: 4/11/06	Approved By: Sinclair Board of Trustees	
Global	Expiration Date: N/A	Title:	

Sinclair Community College Information Security Policy

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

Sinclair Community College

POLICY MANUAL

Policy:		Policy No. X3.1	Page: 1 of 1
Information Security Policy		Issue No. 3.1.1	Issue Date: 4/11/06
Scope:	Effective Date: 4/11/06	Approved By: Sinclair Board of Trustees	
Global	Expiration Date: N/A	Title:	

Information Security Program

Table of Contents

1. Overview:

Sinclair Community 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 Community 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, Sinclair Community College has established a comprehensive Information Security Program 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 Division, some of them impact diverse areas of the College, including but not limited to, Accounting Services, Admissions/Outreach Services, Bursar, Business Services, Financial Aid, Institutional Planning and Research, Registration and Student Records, and many third party contractors.

2. 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 plan are: to protect information 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; to identify incidents that have resulted or may result in a breach of this information; and to develop processes to respond to, mitigate damages resulting from, and prevent recurrence of information security incidents.

3. Program Elements

The program consists of five fundamental elements: (3.1) Information security organization, roles & responsibilities; (3.2) Defining information security standards and principles (3.3) Identification and assessment of information assets and risks; (3.4) Safeguards to mitigate identified risks; and (3.5) 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.

3.1.1. Division Vice Presidents

Division Vice-Presidents are the offices of primary responsibility 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, and ensuring employees have the access required, and only the access required, to perform their jobs. Supervisors should periodically review all users' access levels to ensure they are still appropriate, and take appropriate action to correct discrepancies/deficiencies. Supervisors have to 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 other appropriate party.

3.1.3. Chief Information Security Officer (CISO)

The Sinclair Community 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 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 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 information security 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 (Datatel) 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 Administrative Systems 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. An operational team is charged with initial identification, response, triage, and determining escalation requirements. A management team is charged with College response to major or significant incidents. The operational team consists of the CISO and delegated IT staff members from Information Technology Services and Systems Development and Maintenance. Primary management team members include the CIO, Chief of Campus Police, Director of Public Information, Director of ITS, Director, Systems Development and Maintenance, CISO, Manager of Systems and Network Administration, 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 Services (ITS) Department

The ITS Department staff members include systems and network administrators and engineers as well as technical services providers such as the IT Help Desk, User Support Technicians, and Voice communications administrators. ITS 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. ITS staff must follow information security best practices for managing infrastructure and services.

3.1.7. Systems Development & Maintenance (SDM)

The Systems Development & Maintenance staff members include developers and database administrators who know and understand the technical and operational intricacies of the College information systems. SDM is 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. It is also responsible for training (Web) application developers in using application security principles, to make existing and new applications more secure.

3.1.8. Employees with Access to information:

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 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).

3.1.9. 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 will 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 written request signed by the third party requestor and the sponsor, and approved by the appropriate vice-president, dean, or director. 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 ITS 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 (written) 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. Identification and Assessment of Assets and Risk

The College, as part of this Program, must identify and assess reasonably foreseeable external and internal risks to the confidentiality, integrity, and availability of its information and information systems. The IT Division will assist with developing tools and establishing procedures for identifying and assessing such risks to relevant information and systems. Major risk identification and assessment areas include identification and classification of information and information systems, assessment of employee training and management practices, information processing/systems risk analysis, and system failure and incident management identification processes.

3.3.1. Information/Information Systems Classification and "Ownership"

Information assets owned by the College must be identified, classified, and assigned an "owner" for information security purposes. The owner is responsible for identification of the assets, assigning a classification level based on the confidentiality, integrity, and/or availability needs of the College, and assigning an individual or department primarily responsible for each asset. Identification and classification of assets facilitates the decision making processes regarding the level of security required to protect each information asset.

3.3.1.1. Information asset identification

Virtually every piece of information about or collected by the College is considered an asset if used to conduct College business. Examples of information assets include, but are not limited to:

1). Data/Information collections such as databases, data files, policies, standards, procedures, information archives, disaster recovery/continuity plans, and other paper or digital records.

2). Software assets such as application software (Colleague modules, MS Office) and system software (Windows, Unix, Unidata) and custom software (locally developed programs).

3). Physical assets, including computers (desktops, servers, notebooks, PDAs), communication equipment (telephone systems, fax machines, modems), storage media (tapes, removable disks, CDs), and even some facility equipment (generators, power supplies, air conditioners, furniture).

4). Outsourced services such as vendor support, consulting, contingency services, communication infrastructure, and environmental services (electricity, heating, etc.)

3.3.1.2. Information asset "ownership" (responsibility & accountability)

Each identified information asset must have a responsible/accountable party designated as the asset "owner." While many of these assets have multiple uses and users, primary responsibility for the information or system must be determined. Examples of asset owners include network owners, hardware owners, application owners, and data owners. Any access to, addition to, or modification to the information asset should only be done with the consent of the asset owner. The asset owner is also responsible for classifying the criticality of the information to the College.

Every information technology device (hardware) connected to the Sinclair network must have an owner responsible for security of that device. The owner should maintain some type of inventory registry for of all their devices. This registry should include, where relevant, the device name, model, serial number, network ID, the IP address or subnet, MAC address, physical location, operating system, intended use (Web server, personal computer, lab server, PDA, T-Reg machine, etc.), and the department and person or persons primarily responsible for maintaining the device (owner and administrators). The registry should also record what classification of information (see "c." below) the device stores and/or provides access to.

Software must also have a designated owner. Data is typically owned by the department primarily responsible for collecting or using the data, but may also rely on the application or application module used to store or collect it. Information Technology Services is the primary owner of most of the standard application software supplied campus-wide via 'core' images. Lab coordinators and department heads are generally designated the owners of, and are accountable for, the security of lab- and department-specific applications distributed via non-core images. An owner must be determined and be accountable for non-imaged systems.

3.3.1.3. Information asset classification

To determine the measures required to adequately secure an information asset, the asset must be classified. The data owner is responsible for ensuring that each asset is evaluated against the below criteria and classified based on at least one of the three primary information security criteria, confidentiality, integrity, and availability. Criteria for classifying information include:

3.3.1.3.1. Confidentiality: For classification purposes, confidentiality refers to the sensitivity and the access controls required to protect the information. Does legislation or College policy require the information be protected, or is it freely distributable? Is the information time sensitive? Will its confidentiality status change after some time? Confidentiality is defined in terms of:

1) **Confidential:** Access is restricted to a specific list of people. Examples include human resources/payroll data such as salaries, garnishment orders, child support orders, and employee health information. Stored credit card numbers are also confidential.

2) **Sensitive:** Access and use of the information must be protected from routine disclosure and is restricted to specific uses only. This includes information required to be protected by legislation and/or generally recognized best practices. Examples include Social Security Numbers, Financial Aid Data, Student Records, and Personal Identifying Information (as defined by the Ohio Revised Code).

3) **Public:** Where the resources are publicly accessible. For example, the College Bulletin, the College Web Site, recruitment brochures.

Access control is a primary component of confidentiality. Who must have access to the asset? Who should have access to the asset? Who can manipulate/modify the information? How should the information be stored? This is controlled by assigning access rights for individuals,

groups, and the public. The asset owner determines these access rights. For data stored in the Colleague system, access is determined by security classes and defined in terms of:

1) **Never Do** – no access (to the particular role or security class);
2) **Privileged** – access to specified individuals/roles;
3) **Inquiry only** – access to read information only; and
4) **Do Only** – write access unless restricted by inquiry only or privileged.

3.3.1.3.2. Availability: This is a measure of criticality. How important is it that the information asset is accessible/available to the authorized constituent? Is it a single instance or is a backup available? Availability is measured based on reliability and timely access to the asset. In other words, is the system up and running when needed? How long can the asset be down or unavailable? For classification purposes, the availability hierarchy is:

1) **Vital**: The asset is essential to the College, even a brief outage is significant and may result in a serious negative impact, financial, legal, or otherwise, to Sinclair.
2) **Critical:** Necessary for routine operation of the College, must be available during normal working hours and/or during registration, reporting, or other business cycles. Brief outage other than during these periods is acceptable, outages during these periods are significant and result in serious negative impact.
3) **Important:** Significant to a small segment of the College such as a single department or committee. Should be available during normal working hours, outages of up to 24 hours do not significantly impact the College.
4) **Routine**: Has value to the college and should be routinely available, but extended outages (1-5 days) would not significantly impact Sinclair.

3.3.1.3.3. Integrity: Integrity is seldom used for primary information classification, but may be used as a 'tie-breaker' when determining priority during business continuity and contingency planning. How important is it that the information is 100% accurate and can be verified as tamper-free? How critical is the accuracy of information to the College or stakeholder? Can it be duplicated or replaced? Integrity is defined in terms of value: **high**, **medium** or **low**. As this is often a subjective valuation, justification may be required for assigning a value classification if the rationale is not obvious or is questionable.

3.3.2. Assessment of employee training and management.

Nearly everyone associated with the College has some degree of access to information and information systems, and consequently has the potential to cause harm. While technology can help mitigate risk to the College's information assets, the weakest link in the information protection chain is people. The College must continually assess the current state of each end-user's understanding of the importance of information security, including assessing the effectiveness of current training practices and management policies and procedures in this area.

3.3.2.1. Employee management policies and procedures

Employee management policies and procedures must be evaluated to identify and assess how well they enforce information security practices. Hiring practices should be reviewed to verify references and skill sets of potential employees. Existing employees must be familiar with applicable information security policies such as this policy, the Acceptable Use and Email policies, as well as other policies, procedures, and standards with information security implications. Procedures should be reviewed to ensure information systems/security administration is aware of employee actions such as termination, retirement, extended absence, or department transfer. Procedures and standards should outline actions that determine when and how a user account (and the access the account provides) is added, revoked, suspended, or

modified, and should also specify time-frames for the activity. Managers/supervisors should also understand their responsibilities relating to periodic review of employee access.

3.3.2.2. Security Awareness, Training, and Education (SATE)

Security awareness is the most effective and efficient method for protecting information assets. If employees view information security measures simply as a collection of burdensome rules and processes, rather than as a critical requirement for successful College business, they are likely to ignore or "shortcut" protective measures. Informed employees also improve information security by recognizing threats/vulnerabilities and recommending corrective actions.

Every vice-president, dean, director, chair, manager, or supervisor responsible for employees who use information assets should assess general and specific information handling practices within their area to identify current or potential vulnerabilities. This assessment should include determining who has access, what information they can access, where they can access the asset, and how it is used and protected. Supervisors must ensure their employees know, understand, and are accountable for fulfilling their information security responsibilities, and should implement training or education programs to correct identified deficiencies.

3.3.3. Information Systems Security Risk Analysis

The directors/managers of Information Technology departments, and directors/managers of other applicable departments owning information systems, must regularly identify and assess risks to these systems.

3.3.3.1. Risk Analysis Approach

The risk analysis of each system should as a minimum identify information systems threats and vulnerabilities, measure the likelihood and magnitude of compromise, recommend control measures to increase the security of the system in the most effective and efficient manner, and document and communicate the results of the analysis. Individual departments and divisions should initiate and conduct risk analysis of the systems under their control and should follow up/act on results. IT should assist with the technical controls, but systems risk originating with process must be addressed by the process owner. Current and planned internal operating polices, standards, and procedures relating to information systems must be evaluated. Areas for consideration during the analysis should include:

1. Network and software design and development
2. Change management (including patches and other software "fix" management)
3. Physical security
4. Access control
5. External vulnerability (including penetration testing, intrusion detection)
6. Internal vulnerability (including services running, "rogue" modems, wireless")
7. Storage and backup strategies
8. Contingency planning/testing (disaster recovery/business continuity)
9. Information transmission
10. Disposal of information assets
11. Systems audit practices.

Controls implemented to mitigate risk must also be regularly analyzed for currency, applicability, and effectiveness.

3.3.3.2. Risk Assessment Process

One recommended risk assessment process is:

1. Identify the asset/assets being evaluated, this includes hardware, applications, data, and connectivity. Complex assets may need to be broken into simpler components.

Determine a quantitative or qualitative (or combined) value of the asset to the College. How much would it cost to replace? How long can it be unavailable? What effect does it have when not available? Include the costs/effects of recovering the asset.

2. Identify as many practical potential threats as possible that could harm or otherwise adversely affect operation or efficacy of the asset. Both internal (disgruntled or untrained employees), and external (hackers/criminals, natural disasters, malicious code) threats should be identified and documented.
3. Estimate the likelihood of each threat occurring, and the frequency of the occurrence. This may be based on historical information, estimates of those with expertise, or other experience. This estimate is often subjective, and may require a team of knowledgeable individuals to reach consensus for a realistic estimate.
4. Estimate the effect of the loss of the asset. A quantitative method is to multiply the value of the asset (from step 1) by the frequency of incident occurrence (from step 3) for each potential threat identified (in step 2). This value may be used as a baseline to determine practicality and cost efficiency of protective controls.
5. Identify controls or actions that could mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls.
6. Finally, evaluate and select appropriate controls based on the cost of the control vs. the cost of the effect of the loss of the asset (from step 4).

3.3.4. Information Security Failure/Incident Management Assessment.

Information Security incidents must be properly identified, recorded, reported, investigated, and assessed. The Sinclair Computer Security Incident Response Team (CSIRT) is responsible for identifying, assessing, and responding to actual and potential system failures and information security incidents. The assessment responsibilities include: defining, identifying, and categorizing actual and potential "incidents;" determining the impact of such incidents; evaluating, recommending, and implementing appropriate response; and developing, leading, and implementing recovery and reporting procedures.

Incidents should be assessed for causative factors such as human error, natural disasters, system failures, malicious acts, malicious software, and collateral damage from other systems. Impact of incidents should be examined for results such as denial of service, theft of information, deletion of information, inappropriate disclosure of information, corruption of information, and collateral damage to other systems.

3.4. Controls/Safeguards to Mitigate Identified Risk

Controls and safeguards must be designed and implemented to mitigate the risks identified and assessed. The College must review current safeguards implemented to mitigate identified risks, and recommend/coordinate implementation of additional safeguards as required. Administration and management should regularly review implemented safeguards to control the risks identified through such assessments and ensure regular tests or other monitoring of the effectiveness of such safeguards is conducted. Primary safeguards include:

1. Employee Training and Management Processes
2. Information/Information Systems Controls
3. System Failure Management
4. Overseeing Service Providers

3.4.1. Employee training and management.

Safeguards for information security must include management and training of those individuals with authorized access to covered information. While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, Information Security personnel may assist with identifying categories of employees or others who have access to sensitive or confidential information. They may also recommend or require appropriate training and education for employees who have access to sensitive or confidential information. Such training may include education on relevant policies and procedures, specific safeguards in place, or specific minimum hardware/software requirements required to protect covered data. The two primary focus areas for information security related to employees are management practices and security awareness programs.

3.4.1.1. Management Practices

Appropriate management safeguards should be used such as: utilizing effective hiring screening practices (reference checks, skills verification); providing job-specific training on information systems and information security practices; ensuring no single individual controls a critical or sensitive process from start to finish or with no audit capability (principles of separation of duties); limiting access to sensitive data to those with a legitimate need for access to the information (need to know); reviewing and revalidating access (audit); requiring user identification and authentication such as individual login ID and strong passwords, and requiring periodic changes to those passwords (access control); requiring signed statements of understanding of responsibilities prior to authorizing access to systems housing sensitive information (confidentiality and non-disclosure); implementing job rotation or job backup assignments for critical processes (reduce single point of failure); establishing methods for prompt reporting of loss or theft of information, storage media, and/or information system failures or incidents (incident reporting); ensuring employee access to information is removed in a timely fashion at job change or termination; and other measures that provide reasonable safeguards to information accessible to employees.

3.4.1.2. Security Awareness, Training, and Education

The College must develop and implement a security awareness and training program focused on the entire user population, beginning with managers, directors, and administrators. Supervisors must ensure their employees know, understand, and are accountable for fulfilling their information security responsibilities, and implement appropriate awareness, training, or education programs to correct identified deficiencies. This is not traditionally an IT role, but it is crucial that IT staff members are included in the development and implementation process. The awareness program is the primary vehicle for disseminating information that users need to implement effective information security practices as they do their jobs. The security awareness program must be tailored to delineate the rules of behavior for acceptable use of College information assets, including communication of information security related policies and procedures. All employees should receive basic security awareness training. Employees with significant access to sensitive information should receive advanced training, and periodic refresher training should be available as warranted. An effective security awareness and training program minimizes sanctions resulting from non-compliance and fosters a fully informed, well-trained, and aware culture. The program should support a three-tiered approach; awareness, training, and education.

3.4.1.2.1. Awareness

Security awareness efforts are designed to change behavior or reinforce good security practices. Awareness is not training. The purpose of awareness efforts is simply to focus attention on security by getting individuals to recognize information security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with techniques such as newsletters, brochures, presentations or other broad-audience tools designed to increase awareness of the importance preserving the confidentiality, integrity, and availability of information. Training is more formal, having a goal of building knowledge and skills to improve performance of specific jobs or functions. Awareness is the foundation; when institutions successfully establish programs that increase the general level of security awareness, stakeholders generally integrate basic effective information security practices into their information handling activities. Information security awareness is targeted to all stakeholders.

3.4.1.2.2. Training

Training is an activity; it strives to produce relevant and needed security skills and competencies by practitioners of functional specialties (e.g., management, systems design and development, acquisition, auditing). The most significant difference between training and awareness is that training focuses on developing skills which allow a person to perform a specific function, while awareness focuses an individual's attention on general issues or a related class of issues. Awareness is the foundation; the skills acquired during training are built upon this foundation. Information security training is primarily geared towards users with access to sensitive information, supervisors of these users, information technology staff, and information security organization members. Employees should receive appropriate initial or refresher security awareness training as determined by their supervisor, and should be reminded of their responsibilities at least annually during their performance evaluation with their supervisor

3.4.1.2.3. Education

Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and strives to produce information security specialists and professionals capable of vision and proactive response. Information security education is primarily pursued by managers and information technology/information security professionals.

3.4.2. Information/Information Systems Safeguards

The College relies extensively on its information and information systems. It is essential that controls and safeguards are implemented to protect these assets.

3.4.2.1.. Information systems and devices

Every information technology system or device connected to the Sinclair network must have an owner responsible for security of the device. Before the device or system is connected to the Sinclair information technology infrastructure, the owner must as a minimum address information security issues related to planning, implementing, maintaining, and disposing of the asset. Some of the factors that should be considered and addressed include the following:

1. Physical Environment. Where is the asset located? How is it physically protected?
2. Interconnection/sharing. How is the asset connected to the network? Does it have external connection (ie. modem, wireless) capability?
3. Classification of information accessible through the asset. Does any of the information accessible via the asset require protection based on its classification?

4. IT Risk analysis. Has risk been assessed? How often should it be reassessed?
5. Access controls and audit. How do users access the system? How is access controlled? Is access audit required/performed? Who can read (view or inquiry only) information, who can write (maintain or modify) information?
6. Change Management: Who, what, when, how, are changes developed, tested, and implemented?
7. Support. Who supports the users? Who backs-up the data? Who performs maintenance or repairs?
8. Contingency planning. What happens if asset is lost or corrupted? Who, what, when is responsible for recovery?
9. Documentation. Who, what, where is the information documentation?

3.4.2.2. IT managed systems and devices

The IT Division is the primary "owner" of information systems infrastructure, and is responsible for ensuring network and software systems are reasonably designed and maintained to provide optimal confidentiality, integrity, and availability. IT is primarily responsible for network and operating software design and maintenance, standard software "image" configuration and maintenance, network storage, data transmission, information retrieval controls, and asset disposal. IT develops and implements controls and processes relating to access, systems performance, systems monitoring to detect intrusion and/or malicious code, and deploying security patches for these systems. IT also assures the physical security of all servers which contain or have access to sensitive data and information.

IT staff must implement safeguards for information processing, storage, transmission, retrieval and disposal. Examples of safeguards include: requiring that sensitive information is entered using only secure, password-protected systems; using secure connections (Citrix, VPN, SSH) to transmit data outside the College; using secure servers; ensuring server and desktop operating systems and application software is securely configured (e.g.. SANS/FBI top 20 vulnerabilities addressed, unneeded services turned off); ensuring confidential data is stored and backed-up properly; ensuring sensitive information is permanently and completely removed from computers, diskettes, magnetic tapes, hard drives, or other electronic media before re-selling, transferring, recycling, or disposing of them; storing physical records in a secure area and limiting access to that area; providing safeguards to protect sensitive data and systems from physical hazards such as fire or water damage; disposing of outdated records under a document disposal policy; shredding confidential paper records before disposal; maintaining an inventory of servers or computers used to access or store sensitive data; and other reasonable measures to secure sensitive information during its life cycle in the College's possession or control.

IT assumes the responsibility of assuring that patches for operating systems or software environments are reasonably up to date on all systems they "own" or are responsible for managing; IT tests and documents all patching activity. IT regularly reviews procedures for patches to operating systems and software, and keeps current on potential threats to the network and its data. Risk assessments are updated regularly. The following table lists some specific IT Managed services or devices requiring risk assessment and basic areas to address when conducting risk assessments for them.

Service/Device	Areas to Consider
Data Center	Auditing
Desktops	Authentication
Legacy Systems	Backups

Network Devices	Change Management
Network (Domain) Services	Content Filtering
Strategic Servers	Disaster Recovery
Telecommunication Systems	Intrusion Protection
Web Servers	Password Standards
	Physical Access
	Provisioning/Deprovisioning (Identity Management)
	Redundancy
	Remote Access
	Retention/destruction Policy
	Security Zones (VLAN)

3.4.2.3. Non-ITS managed systems and devices

All devices connecting to the college network must meet ITS standards and be approved by ITS. This applies to all device owners, employees, students, contractors, vendors, etc., who need to connect a non-ITS-managed device to the domain. Devices may include computers, PDAs, printers, network appliances, VOIP telephones, etc.

3.4.2.3.1. Authentication

As a minimum, any device permitting write, execute, or modify permissions shall support and permit authentication (e.g. password or multifactor system).

3.4.2.3.2. Software patches

All networked devices must have all available patches installed that address critical security vulnerabilities. Vulnerable systems face disconnection from the college network. Delaying installation until a convenient time, such as semester breaks, is unacceptable. Exceptions may be made for patches that compromise the usability of critical applications, provided additional security measures are taken. Computer overseers are responsible for creating and enforcing procedures to ensure that system software is kept current.

3.4.2.3.3. Anti-virus software

All systems connected to the college network must be running current anti-virus software, and must check for updates at least daily. The minimum standard for anti-virus software is to meet or exceed the effectiveness of the software products site-licensed by the college (McAfee). Non-compliant or infected systems are subject to removal from the network. System owners are responsible to ensure that anti-virus software is run at regular intervals and devices are verified to be free of viruses.

3.4.2.3.4. Anti-spyware software

Users are strongly encouraged to routinely scan their systems for potentially unwanted programs commonly referred to as spyware or adware. Users are strongly encouraged to read end-user license agreements before installing any software, and if they have any questions regarding technical language, or if they do not fully understand what the software claims to do, they should seek assistance of or evaluation from IT staff before installing the software.

3.4.2.3.5. Host-based firewall software

Host-based firewalls may be used to provide an additional level of security to individual computer systems. Computer users are encouraged to check the compatibility of and current issues regarding the use of host-based firewall software with Information Technology Services.

3.4.2.4. Administrative/Student system (Colleague)

The administrative system (Colleague database) is the primary repository of personally identifiable and other sensitive information and requires stringent safeguards. Electronic access to this information is protected by usernames and passwords. Division Vice Presidents (owners of the data) will appoint an information security officer from each division as primary members of the Administrative System Information Security Team; the information security officer is the steward of the data for that division and is the person responsible for the safeguarding of that data. The Administrative System Information Security Team authorizes and/or approves all access to the administrative system. The team's primary responsibility is to ensure processes and standards are developed and implemented to provide optimal access, integrity, and that confidentiality of administrative system information is maintained.

Sinclair administrative systems are for use by authorized Sinclair faculty, staff and other designated stakeholders. Restricted/controlled access is also granted (via WebAdvisor) to students and other stakeholders to view and maintain limited personal information. When any individual is to be given access to administrative systems (other than for restricted viewing/updating limited personal information), including part-time, student, temporary, or contract workers and SCC vendors, written authorization is required from the supervisor. All use of administrative systems and data must be consistent with the requirements specified by applicable laws and Sinclair polices and procedures.

Employees (including part-time and student workers) requesting access to the administrative system must, as a minimum, complete training on access, basic navigation, and data standards developed by the College. Supervisors are responsible and accountable for ensuring this training is completed, therefore, before any access is granted to the system, staff members must submit a request and statement(s) of understanding, endorsed by their supervisor, certifying that that they have read the manual and understand their specific responsibilities. Existing staff members should receive periodic access review and refresher training as determined by their supervisors, and should be reminded of their responsibilities at least once each year during the performance evaluation process. When an employee's access to the system (i.e. security class) is changed, IT will send a notification of the change to the user and supervisor reminding them of their responsibilities.

Vice-Presidents, Directors, Deans, Chairs, Managers, and other supervisors should regularly ensure (at least biannually) audits are conducted of their employees' access and activity, and must report any significant changes required or questionable access discovered. The Information Security staff will work with the relevant offices (Business Services, Human Resources, the Registrar, Financial Aid, Institutional Planning and Research, and the Bursar, among others) to develop and maintain a registry of the departments of the College community who have access to the system and any sensitive information and how this data is used/maintained. This registry includes access provided by each security class and the security classes assigned to each user.

3.4.3. System Failure/Incident management.

IT develops plans and procedures to detect any actual or attempted attacks on college systems and assists with development of incident response procedures for actual or attempted unauthorized access to covered data or information. IT must implement and maintain reasonable and effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such systems include maintaining and implementing current anti-virus software; checking with software vendors and others to regularly obtain and install patches to correct

software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting those with access to covered data of threats to security; backing up data regularly and storing back up information off site, as well as other reasonable measures to protect the integrity and safety of information systems.

Systems monitoring should be implemented to regularly test and monitor the effectiveness of information security safeguards. Monitoring is conducted to reasonably ensure that safeguards are being followed and to swiftly detect and correct breakdowns in security. The level of monitoring should be appropriate for the potential impact and probability of the risks identified, as well as the sensitivity of the information provided. Monitoring may include sampling, system checks, reports of access to systems, reviews of logs, audits, and any other reasonable measures adequate to verify that Information Security Program's controls, systems and procedures are working. The Information Security staff periodically review the safeguards and disaster recovery program and report to the Director of Information Technology Services on the status of the information safeguards and monitoring implemented for covered data.

The CSIRT is primarily responsible for system failure response and incident management. The operational component of the CSIRT should immediately take action when an incident has been reported or is in progress to contain damages to College systems; halt attacks if caught while in progress; and preserve and gather evidence that results from an incident that has occurred. The CSIRT will also consider the evidence and reports resulting from any incident and decide upon what, if any, escalating actions should be taken, as well as recommending appropriate reporting, sanction, or prosecution of individual(s) responsible for the security incident. The CSIRT will conduct a biannual review of procedures, incidents, and responses, and will publish all relevant materials except in those cases where publication may likely lead to breaches of security or privacy. The review will assure that procedures and responses are appropriately reflective of those widely practiced at other educational institutions. The following table lists some major components of the incident handling process.

Security Incident Handling
Preliminary Activities (Preparing and Planning)
Detection, Initial Reporting, Identifying
Containment and Escalation
Eradication
Recovery
Post-Incident/Follow-Up Activities
Reporting/Lessons Learned

In cases where college information assets are actively under significant threat or attack, the CSIRT is authorized to act in the best interest of the College by securing or delegating the securing of the assets as necessary. When possible, the CSIRT will work with the appropriate asset owner to mitigate the threat. In an urgent situation requiring immediate action and leaving no time for collaboration, the Director of ITS or the CISO is authorized to secure the asset without the owner's consent.

The CSIRT is also responsible for approving and coordinating IT assistance to law enforcement agencies conducting investigations. All requests for assistance must originate with the Sinclair Campus Police and be approved by an officer holding the rank of Sergeant or above unless a valid subpoena specifically dictates otherwise. In the event of any law enforcement

request for IT assistance, the Director of ITS should be notified as soon as practically possible. The Director of ITS will provide guidance for the action to be taken.

3.4.4. Overseeing Service Providers.

Those responsible for the third party service procurement activities among the Systems Development & Maintenance, ITS, and other affected departments must be aware of security implications of the service, and must institute methods for selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for the information to which they will have access. In addition, the CISO will work with the appropriate Business Operations departments to develop and incorporate standard, contractual obligations applicable to third party service providers. These obligations will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the President's Council. These standards shall apply to all existing contracts when renewed and future contracts entered into with such third party service providers.
Contracts with service providers should include the following provisions:

a. an explicit acknowledgment that the contract allows the contract partner access to confidential information;
b. a definition of the confidential information being provided;
c. a stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
d. a guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
e. a guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;
f. a stipulation that in the event of a security breach (within its control) covered under sections 1347 and 1349 of the Ohio Revised Code, the contractor shall bear all responsibility and expense for complying with the disclosure and notification requirements of the statute
g. a provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
h. a stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles Sinclair Community College to immediately terminate the contract without penalty;
i. a provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and
j. a provision ensuring that the contract's protective requirements shall survive any termination agreement.

3.5. Auditing, Monitoring, and Adjusting 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 documents

Sinclair Community College Board Approved Policies
Acceptable Use Policy
Email Policy

Operational Policies, Procedures, Standards, and Guidelines
Data standards manual
Administrative systems security standards (draft)
Risk identification and assessment standards (tbd)
Computer Security Incident Response Standards (draft)
Automatic Nighttime PC Shutdown
Connecting to Sinclair Network Resources
Firewall Procedures
Laptop Procedures
Network Change Methodology
Network Storage Procedures
Off-Campus File Access (Citrix)
Software Update Services
Generic Email Accounts
Non-Employee Network Accounts
Guidelines for the Use of 'All Sinclair Users'
One (1) MB Size for Email Attachments
Spam Assassin with Automated Spam Rejection Feature

Other related documentation
Colleague operator definition records
Colleague security class definition records
Network Security Architecture Model