Niagara County Community College

Information Security Policy

Document: Information Security Policy
Owner: Chief Information Officer
Version: 1.0

Table of Contents:

Revision History:

January 18, 2012 Initial adoption

Purpose

The purpose of this Information Security Policy ("Policy") is to define a set of security requirements that will help protect all members of the campus community from information security threats that could compromise privacy, productivity, and reputation. The Policy recognizes the vital role of information in support of the mission of the college and the importance of protecting information in all forms in order to foster a secure environment for the gathering, retention, and dissemination of college information.

The following are the primary goals of the Policy:

- to communicate campus responsibilities for the protection of college information
- to increase awareness of the importance of information security within the college community
- to manage the risk of security threats to the information resources of the college
- to provide and protect a secure environment for the gathering, retention, and dissemination of college information
- to develop effective mechanisms for responding to real or perceived incidents involving breaches of information security
- through the above, to assure the College's compliance with all federal, state and local laws and regulations pertaining to information security

Scope

This Policy applies to all employees, students, consultants, contractors, vendors and other persons who have access to college information. Compliance with this Policy is mandatory for this constituency.

This Policy encompasses all information systems, computer-based and non-computer-based, automated and manual, physical and non-physical, for which the college has administrative responsibility. This includes systems managed or hosted by third parties on behalf of the College. This Policy addresses all information used in support of the business activities of the college, regardless of its form or format. This Policy must be communicated to all staff and all others who have access to or manage college information.

Policy

Part 1 - Responsibilities

Senior Executive: The President, along with the Executive Council, oversees the Policy's development, implementation and management, ensuring individual managers are assigned ownership and stewardship responsibilities for critical information assets and responding on behalf of the College.

Information Security Officer: The Chief Information Officer will serve as Information Security Officer and will have the following responsibilities:

- approve all external network connections to the college network
- establish an Information Security Committee to achieve the goals of this Policy and serve at its Chairperson

Information Security Committee: This committee will consist of key personnel from the Office of Information Technology Services, Security, Operations, Academic Affairs, Business Office, and Student Services. It will have responsibility for the following items:

- implement and maintain this Policy
- implement and maintain an information security training program
- implement and maintain an information security architecture to support this Policy
- approve implementation of new initiatives to maintain and enhance this Policy
- control the security of college information assets
- proactively monitor college information assets relative to potential security threats
- to investigate and respond to information security incidents
- to report information security incidents to senior administration
- to participate in the maintenance of a disaster recovery plan to insure the continuity of college business operations in the event that information systems become unavailable for an extended period of time
- to provide information security recommendations to senior administration relative to mitigating the risks associated with information security threats that could negatively affect college business operations

Information Experts: Information Experts will be identified for all information resources and will have responsibility for the following items:

- to classify the information resources within their area of expertise
- to determine the access rights and privileges for information resources within their area of expertise
- to communicate to the Information Security Officer the legal requirements for access and discloser for the information resources within their area of expertise

Information Technology Staff (IT Staff): The Office of Information Technology Services will have the responsibility for the following items:

- to implement access rights and privileges in pertinent digital environments as defined by Information Experts
- to maintain digital user accounts and deactivate accounts upon separation from the college
- to provide computer network and server infrastructure necessary to support this Policy
- to implement back-up and recovery procedures for centrally-maintained digital information resources
- approve implementation of new digital information applications and services based on review of the compliance of these new applications and services with this Policy

Department Managers: to manage access to information resources under their control in accordance with this Policy and communicate deficiencies to the Information Security Officer.

Employees: All employees will have the responsibility to protect information resources and report any suspected information security incident to the appropriate manager and the Information Security Officer.

Non-Employees: All contractors, consultants, vendors, and other persons working under agreements with the college will have the responsibility to protect information resources and report any suspected information security incidents to the appropriate manager and the Information Security Officer.

Students: All students will have the responsibility to protect their own information resources and report any suspected information security incident to an appropriate manager or the Information Security Officer.

Part 2 Information Classification

Information Experts will be responsible for classifying information as Public or Private based on the consequences of loss, the legal or retention requirements, the sensitivity, and the value of the information. This classification process should include consideration of the confidentiality, integrity, availability, legality, privacy and retention properties of the information.

Public information is information that can be freely provided to anyone without any possible damage to the college.

Private information is categorized as the following:

- personal information as defined by the NYS Freedom of Information Law (FOIL)
- personally-identifying information as defined by the NYS Information Security Breach and Notification Act and the NYS Disposal of Personal Records Law
- personal information defined in the NYS Personal Privacy Protection Law

- personally-identifiable information on students in education records as defined in the Family Educational Rights and Privacy Act (FERPA)
- personal information defined in the NYS Electronic Signatures and Records Act (ESRA)
- personally-identifiable financial information on customers in financial lending records as defined in the Gramm-Leach-Bliley Act (GLBA) with its associated Federal Trade Commission Safeguards Rule
- payment card transaction information as defined by the Payment Card Industry Data Security Standard (PCI-DSS)
- Personal, Private, and Sensitive Information ("PPSI") as defined in New York State's Information Security Policy (NYS IS Policy)
- personally-identifiable medical information as defined by the Health Insurance Portability and Accountability Act of 1996
- information classified as structural, operational, or technical information (about electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure) as defined within "PPSI" in NYS IS Policy
- emergency and business continuity plans and operational documents
- information identified as private by this Policy

All information will have an Information Expert established within the responsible functional area of the college. The Information Expert will be responsible for assigning the initial information classification of public or private and for making decisions regarding user access rights, user access privileges, and procedures for daily management of the information. The Information Experts should conduct a periodic analysis of the value of the information based on the above criteria in order to confirm the current classification or to reclassify the information.

Privacy of Information

Private information must be maintained consistent with federal and state laws and regulations and with college policies. All college employees with access to private information must protect that information in accordance with federal and state laws and regulations and college policy. The college must maintain the following characteristics for private information:

- must be accessible only by authorized individuals
- must be corrected if incorrect information is known to exist
- must be removed or made inaccessible, if appropriate and if the individual makes this request consistent with federal and state laws and regulations and with college policies
- must be gathered in a manner consistent with federal and state laws and regulations and with college policies
- must be protected using computer based and non-computer based access controls
- must be retained for the longer amount of time as required by federal and state laws and regulations or as required by college policies and then, unless there is a pending

court order, must be disposed of by physical destruction of the media on which the information resides or by erasing the information from the media in a manner that results in the information being totally unrecoverable
- must not be disclosed unless authorized or required by federal and state laws and regulations and by college policies

Part 3 Information Security

Information in any form or format that is created, acquired, or used in support of the business activities of the college is to be considered an asset. Information assets must only be used in relationship to the business activities of the college and must be protected from the time of creation, through useful life, and to the time of authorized disposal. Information assets must be maintained in a reliable and secure manner and must be readily available for authorized use. Information assets must be classified and protected based on the sensitivity of the information.

Information is among the most valuable assets of the college. The availability and reliability of information assets are keys to supporting the business activities of the college. The security of information assets is the responsibility of all employees, students, consultants, contractors, vendors and other persons who have access to these information assets.

Each authorized user is obligated to preserve and protect college information assets in a manner consistent with this Policy. Information security controls described within this Policy provide the necessary physical and procedural safeguards to achieve this goal. Information security management enables both the sharing and protection of college information assets. The Information Security Officer, the Information Security Committee, the Information Technology Staff, and Department Managers have the responsibility for insuring that appropriate controls are in place to preserve the security of these information assets.

Individual Accountability
Individual accountability is the cornerstone of this Policy and is required when accessing all college information resources. The following are requirements for accessing information on college computer systems and networks.

- access must be provided through the use of individually assigned unique identifiers know as usernames
- associated with each username is a token known as a password that must be used in combination to authenticate the individual requesting access
- an individual must access only information for which he or she has a legitimate business interest
- an individual must be provided access to authorized information only after proper authentication with his or her username and password

- an individual must not share his or her username and password as each individual is responsible for protecting information against unauthorized access through the use of his or her username and password
- no individual should ever communicate a password using email or any other insecure means of communication

Department/Office/Division Accountability

Each department, office and/or division will maintain a Workforce Inventory listing of which workers are active and have access to private information. This information will be updated annually and when needed by the Information Security Officer to conduct risk analysis and design information security education.

Security in Job Responsibilities

The security responsibilities of employees and third parties must be documented. For employees, these security responsibilities should be included in job descriptions and for third parties these security responsibilities should be included in contracts. These security responsibilities will include general and specific responsibilities for protecting information and for performing tasks related to security procedures or processes.

Whenever an employee leaves employment, changes departments, or otherwise has changes in job function that makes obsolete access to private material, his or her supervisor will notify the Office of Information Technology Services of the change, specifically noting that the change requires a removal or review of the worker's authorizations.

Personnel Security Training

Personnel with access to private information must be provided with specific information security training to insure knowledge of their security responsibilities to protect information and knowledge of college security policies and procedures to minimize information security risks. These same persons must additionally be provided with specific refresher training to maintain knowledge of current college security policies and procedures.

All employees must be provided with general information security training to insure knowledge of current college security policies and procedures.

Confidentiality/Integrity/Availability

All information must be protected from unauthorized access to help ensure the confidentiality and integrity of all information assets. Appropriate processes will be defined in the college's recovery plan and implemented to ensure the reasonable and timely recovery of all information, applications, systems and security regardless of computing platform, should that information become corrupted, destroyed, or unavailable for a defined period of time.

Part 4 Reporting and Responding to Security Incidents

Actual or suspected breaches of information security must be immediately reported by the involved person to the Chief Information Officer. Persons must not attempt to prove a suspected security weakness or threat unless authorized to do so by the Information Security Officer, as testing a suspected security weakness or threat may have serious, although unintended, consequences. The Chief Information Officer will immediately conduct an investigation to determine whether there has been a breach of private information, to determine the nature and extent of such breach, and to correct the circumstances that that allowed or caused the breach of private data. During this process, all persons will be made aware of the procedures that should be followed to prevent any further dissemination of private information. The Chief Information Officer will work with the President, Senior Staff and college counsel to determine an appropriate and timely notification of potentially affected individuals and the agencies to which any such breaches are to be reported. At a minimum, the Information Security Officer will notify the involved person and his/her supervisor of the results of the investigation after the incident has been resolved and closed.

Actual or suspected information security software malfunctions, such as a virus not being detected, must be reported by the involved person to the Office of Information Technology. The event should be thoroughly described by the involved person when reporting this type of information security incident.

Tracking of Security Incidents

A formal system for tracking security incidents will be established. This system will include recording the description and resolution of the security incident. This information will be used to identify recurring or high-impact incidents in order to focus resources on decreasing or eliminating such types of incidents.

Part 5 Physical and Environmental Security

Information processing and storage facilities for critical or sensitive information must be located in areas protected by a defined security perimeter with security control systems for accessing the facilities. These physical security mechanisms are intended to protect the facilities from unauthorized access, damage or interference and should be periodically tested to insure such protection. The college will review these and other locations on an ongoing basis to determine the need for additional physical mechanisms to reduce overall information security risks.

Physical Security

A breach of physical security threatens the integrity of college information assets. Physical security is achieved by creating physical barriers around the assets with each barrier establishing a security perimeter that requires a method of access to control entry. This security perimeter may be created with a staffed reception area, with a secured door, or with some other form of a physical barrier.

The college will perform analyses to determine the extent of the security perimeter necessary for each information processing and storage facility. The physical barriers necessary to create this security perimeter will then be implemented and maintained. A physical security perimeter will be established for information processing and storage facilities for critical or sensitive information, including the college data center and network wiring closets for data, security and telephone equipment and cabling.

Private information which is scheduled to be destroyed is to be stored in a locked container till which time the information is to be destroyed.

The protection of critical or private information contained on storage devices such as hard disk drives, either in personal machines or digital copiers, removable drives, thumb drives, magnetic tape media, or other digital storage devices is another important element of physical security. The disposal or reallocation of these storage devices must include a process to destroy or securely overwrite the device in order to prevent unauthorized disclosure of information.

Proper management of critical or private information stored on/in non-digital media (e.g., paper, microfiche, etc.) is another important element of physical security. Such media must be protected from loss, theft or other inadvertent disclosure by storing in physically-secure locations that are accessible by only those individuals who have a valid college business need for the information. Once the information's retention period has expired, the media must be disposed of in a manner that will prevent inadvertent disclosure of its content.

Environmental Security

Computer, data security and telephone equipment protection within physical security perimeters will require a level of environmental security. Special environmental systems for air conditioning and humidity control and for uninterruptable electrical power distribution will be maintained for information processing and storage facilities for critical or private information, including the college data center and major network wiring closets for data security and telephone equipment and cabling. Special environmental systems for backup electrical power distribution will be maintained for the college data center and major network wiring closets for data, security, and telephone equipment and cabling.

The protection of critical or private information visible on computer screens is another important element of environmental security. In public areas, computer screens should be faced so as to be visible only to the authorized user of the computer. In public and in all other areas, computer screens should use a screen saver with a screen saver password to insure that information is not displayed after a specified period of inactivity.

Computer equipment which has access to private information is only to be used by the authorized individual assigned to the computer.

Part 6 Communications and Network Management

The college network will implement appropriate security controls to ensure the integrity of data flowing across these networks. If there is a business need, additional measures to ensure the confidentiality of the data will also be implemented. If the college decides to outsource an application to a third-party vendor, the Information Security Officer will ensure that measures are in place to mitigate any new security risks created by connecting the college network to a third party network and will have periodic security reviews performed to ensure compliance with this standard. All connections to the college network must be authorized by the Information Security Officer.

Network Management
Minimally the below controls to prevent unauthorized access and use of the college network will be implemented:

- separate operational responsibility for networks and computer systems
- establish responsibilities and procedures for remote access
- implement special controls, when necessary, to safeguard the integrity and confidentiality of data passing over public networks

Vulnerability Scanning
Computer systems that provide information through a public network will be subjected to vulnerability scanning. These systems will be scanned for vulnerabilities before being installed on the network and after any software or significant configuration changes have been made to the systems. Network components that are, or will be, part of the college network will be scanned for vulnerabilities when installed on the network and after any software or significant configuration changes have been made to the components.

The output of the scans will be reviewed in a timely manner by the Information Security Officer and any detected vulnerabilities will be evaluated and mitigated based on the level of risk.

The tools used for scanning of computer systems and network components will be updated periodically to ensure that recently discovered vulnerabilities are included in any scans. Scans of computer systems and network components will be performed at least annually to ensure that no major vulnerabilities have been introduced into the environment. The frequency of additional scans will be determined by the Information Security Committee, taking into account the level of previously detected computer system or network vulnerabilities.

Vulnerability scanning must only be performed by Information Technology Staff or by a third-party vendor authorized to perform vulnerability scanning by the Information Security Officer.

Penetration and Intrusion Testing
Computer systems that provide information through a public network must be subjected to penetration and intrusion testing. The testing will minimally be used to determine the following

- if a user can make an unauthorized change to an application

- if a user can access an application and cause it to perform unauthorized tasks
- if an unauthorized individual can access an application and destroy or change data

Network systems that are directly connected to the public network must be subjected to the penetration and intrusion testing. The testing will minimally be used to determine the following:

- firmware and software are patched to prevent breaches
- hardware is properly configured to only allow approved connections

The output of the testing will be reviewed in a timely manner by Information Security Officer and any detected vulnerabilities will be evaluated and mitigated based on the level of risk.

The tools used for the testing will be updated periodically to ensure that recently discovered vulnerabilities are included in any testing. Testing of computer systems must be performed at least annually to ensure that no major vulnerabilities have been introduced into the environment. The frequency of additional tests will be determined by the Information Security Officer taking into account the level of previously detected computer system vulnerabilities.

Penetration and intrusion testing must only be performed by Information Technology Staff or by a third-party vendor authorized to perform vulnerability scanning by the Information Security Officer.

Acceptable use of Computer Systems and Networks
Employees, non-employees and students must adhere to acceptable use of computer systems and networks as defined in the NCCCnet Use Policy.

External Connections
Connections from the college network to external networks must be approved by the Information Security Officer after a risk analysis has been performed to ensure that the connection to the external network will not compromise the college network. Connections will only be allowed when the external networks have acceptable security controls and procedures or when the college has implemented appropriate security measures to protect the network resources of the college. Firewalls and access control lists will be implemented between the third-party and the college to achieve an appropriate level of protection. Any connections between college firewalls over external networks that involve sensitive information must use encryption to ensure the confidentiality and integrity of the data passing over the external network.

External connections will be periodically reviewed by the college to ensure that the security controls in place are functioning properly and that the business case for the external connection is still valid. Only authorized IT Staff and authorized third-party staff will be permitted to use tools to monitor network activity on external connections. Authorized IT Staff will regularly monitor external connections for abuses and anomalies.

Internal Connections
Wired connections from devices that are not maintained by the college's IT staff to the college network must be approved by the Information Security Officer after a risk analysis has been

performed to ensure that the connection from the device will not compromise the college network. Connections will only be allowed when the devices that are not maintained by IT staff have acceptable security controls and procedures to protect network resources of the college. These controls and procedures are to include, but are not limited to, firewalls and properly updating operating system and virus protection software. In addition to requiring the necessary controls in place, the devices will be segmented from the college's network segment.

Internal connections will be periodically reviewed by the college to ensure that the security controls in place are functioning properly and that the business case for the internal connection is still valid. Only authorized IT Staff and authorized third-party staff will be permitted to use tools to monitor network activity on internal connections. Authorized IT Staff will regularly monitor internal connections for abuses and anomalies.

Portable Devices

Portable computing resources and information media must be secured to protect the integrity of private information. The use of portable computing resources such as laptops, notebooks, PDAs, mobile smart phones, removable hard drives, flash drives, etc. must involve special care to protect private information. The following requirements, as applicable, must be followed when using such devices:

- when using portable computing resources in public and other unprotected locations external to the college, the use of encryption to protect the transmission of private information must be implemented and special care must be taken to protect against unauthorized persons viewing private information
- protection against malicious software on portable computing resources must be implemented and maintained at current levels
- private information is not to be stored on portable computing resources without whole disc encryption in place
- portable computing devices are not to be left unattended in public places
- when not in use, portable computing devices containing private information are to be physically secured, including, but not limited to, placing the device in an automobile's locked trunk instead of leaving the device in plain sight
- portable computing devices on which private information is stored must not be checked into transportation luggage systems and must remain in the possession of the traveler as hand luggage unless other arrangements are required by federal or state authorities

Telephones and Multifunction Devices

Employees must adhere to the following guidelines when using telephones and multifunction devices both internal and external to the college to mitigate potential information security risks:

- care should be taken to prevent conversations involving private matters from being overheard
- avoid the use of mobile phones when discussing private information
- avoid leaving messages involving private matters on voicemail
- contact the recipient to ensure protection of a fax and verify the destination fax phone number when sending private information
- avoid using third-party, internet or wireless fax services to send or receive private information

- avoid using third-party copiers to duplicate material containing private information
- confirm that all attendees are authorized participants before starting any private discussions when chairing a teleconference

Wireless Networks

Wireless devices and technology create new and innovative opportunities for providing instruction and conducting business functions of the college. However, everything that is transmitted on a wireless network could be intercepted by a person within the coverage area of a wireless transmitter. The following guidelines must be followed when implementing and using wireless networks:

- wireless network access points must not be installed without approval of the Information Security Officer and the installation must be done by an IT staff member
- suitable security controls, such as authentication, encryption and MAC address restriction must be implemented to ensure that wireless network access point cannot be exploited to disrupt college services or gain unauthorized access to college information
- private information must not be transmitted on a wireless network unless suitable security controls have been implemented and approved by the Information Security Officer

Public Web Servers and Public Web Sites

The internet provides an opportunity for the college to disseminate information and provide interactive services quickly and cost effectively. However, because a public web server is accessible globally and provides a potential connection path to the college network, care must be exercised in the deployment of public web servers. An insecure public web server may be used to obtain private college information, disrupt college services, or assist in an illegal activity such as an attack on the web site of some other organization.

Public web site content must be approved by the Office of Public Relations. Content will be reviewed with consideration for copyright issues, for confidentiality, privacy and sensitivity, for accuracy and for any potential legal implications associated with providing the information.

If faculty, staff and students have the ability to create personal web pages, while the content of personal web pages not reviewed prior to posting on the college web site, the content of personal web pages is subject to compliance with the college's Web Policy, with federal and state laws regarding use of computers and electronic communications and with the NYS Office of Technology Policy 99-3 titled Universal Accessibility for NYS Web Sites. No material included on personal web pages may violate any laws, including but not limited to, those regarding obscenity, harassment of others, and copyright infringement.

Part 7 Operations Management

Operating instructions and incident response procedures will be established and documented for the management and operation of all information processing facilities. Procedures will also be established and documented for activities associated with information processing and

communications facilities such as computer startup and shutdown, data backup and equipment maintenance.

Separation of Development, Test and Production Environments
Development, test/train, and production computing environments must be separated either logically or physically. Procedures will be established and documented to implement the transfer of software from a development environment, through a test environment, and to a production environment. The following controls must be considered when establishing these separations:

- software and tools for development will be maintained in development environments isolated from production environments
- when not required, access to compilers, editors and other system utilities will be removed from production environments
- login procedures and environmental identification will be sufficiently unique between development, test, and production environments
- short term access controls will be in place to allow necessary staff access to correct problems

Developing and testing software could potentially cause serious problems to production environments if these environments are not appropriately separated. The degree of separation must be considered by the college to ensure adequate protection of production environments. The college must also consider a stable testing environment where user acceptance testing may be conducted without changes being made to the software being tested.

System Planning and Acceptance
Planning for systems must be a comprehensive process to ensure the implementation of appropriate security measures and the availability of adequate resource capacity. The security requirements of new systems will be documented, implemented, and tested prior to acceptance of systems and will be regularly reviewed during use of systems. The processor, memory and storage requirements of systems will be monitored in order to maintain adequate resource capacity for current workload and to project requirements for future workload so that any potential system bottlenecks and related disruptions to the delivery of user services are avoided.

IT Staff and the Information Security Officer will ensure that the criteria for acceptance of security requirements are clearly defined, documented, and tested prior to new systems being migrated to a production environment and prior to existing systems being upgraded in a production environment.

Protection against Malicious Code
All systems must be protected with appropriate controls to prevent and detect the introduction of malicious code that could cause serious damage to networks, servers, workstations and data and that could significantly disrupt the operations of the college. Employees and Non-Employees must follow NCCCnet Use Policy and report any suspected malicious code incident.

Software Maintenance

All vendor software must be maintained at supported levels to ensure accuracy, integrity and supportability unless otherwise approved by the Information Security Officer. All college developed software must have appropriate change management procedures to ensure that changes are authorized, tested and accepted prior to deployment in a production environment. All software security patches must be reviewed, evaluated and, as appropriate, applied in a timely manner to reduce the risk of security incidents that could affect the availability, confidentiality and integrity of systems, software or business data.

Information Back-Up

Critical college data and software must be backed-up regularly. A risk assessment will be performed for all systems on which college data is stored to determine the criticality of each system and the appropriate amount of time for recovery of each system. In this process, the criticality of services provided by the system and the sensitivity of information on the system will be considered. Systems to be analyzed will include networks, servers, and workstations for critical systems. Processes will be developed to back-up and fully restore the data and software, including full restoration at an alternate location should that be necessary. Disaster recovery plans will be developed, implemented and periodically tested for all critical college systems. The results of testing will be documented and any detected deficiencies will be corrected in a timely manner.

System Security Checking

Systems that provide critical services or store private information will undergo annual security reviews to ensure compliance with implementation standards and to identify security vulnerabilities to subsequently discovered threats. Any identified security vulnerabilities must be reported to the Information Security Officer and must be corrected by IT Staff. The appropriate Information Expert will be informed of the vulnerability and will initiate an investigation to determine if any private information has been compromised.

Part 8 Access Control

Digital and physical access control mechanisms must be implemented in order to protect the availability, confidentiality and integrity of college information assets. The level of security provided by these mechanisms for each information asset should be commensurate with the criticality, sensitivity and privacy properties of the asset. Information Experts will be responsible for making decisions regarding user access rights and privileges based on job responsibilities of the user.

User Registration Management

The college will establish a user registration management process to control the generation, distribution, modification and deletion of user accounts for access to information resources. The purpose of the process is to ensure that only authorized individuals have access to college applications and the information required in the performance of their job responsibilities. The user registration management process will include sub-processes for the following components:

- creating user accounts
- granting user account privileges
- removing user account privileges

- periodic reviewing of user accounts
- periodic reviewing of user account privileges
- assigning of new authentication tokens (password reset processing)
- removing user accounts

Information Experts must approve access rights (who should have access) and privileges (what access should be provided) for information resources within their area of expertise.

Privileged Accounts Management
The issuance of privileged accounts for performing systems administration functions will be restricted and controlled because the inappropriate use of privileged accounts may significantly contribute to breaches of information security on systems. Processes will be developed to ensure that usage of privileged accounts is regularly monitored and that any suspected misuse of privileged accounts is promptly investigated. The passwords of privileged accounts used by more than one person will be changed on a regular basis.

User Password Management
Passwords are a common means of authenticating the identity of a user to provide access to information systems. Password standards will be developed and implemented to ensure that authorized individuals accessing college resources are following proven password practices or rules. Whenever possible, these password practices or rules will be automatically required by system controls and will include, but not be limited to, following:

- passwords must not be stored in clear text
- passwords should not be subject to disclosure through dictionary attack or easily guessed
- passwords must be confidential and not shared with any other person
- passwords should be changed at regular intervals
- temporary passwords should be changed at the time of first logon
- initial passwords should be randomly assigned with a prompt for users to change them immediately upon login; ideally they should contain a mix of alphabetic, numeric, special and upper/lower case characters
- passwords should not be automatically included in any logon process

Network Access Control
Access to the college internal network will require that users authenticate themselves through use of an individually assigned username and a password constructed to meet established standards. Network controls will be developed and implemented to ensure that authorized users can access only those systems and services necessary to perform their assigned job responsibilities.

Remote Access Control (User Authentication for External Connections)
The college requires that individual accounts be maintained by Employees and Non-employees at all times, including during remote access, in order to maintain information security. Any access from an external connection to the college network is a remote access. Remote access to any on-campus college computer system must be authorized by the Information Security Officer. External connections to the college network will be established in a secure manner in

order to preserve the integrity and availability of the network including the integrity of data transmitted over the network. Security mechanisms will be in place to control access to college systems and networks from fixed and mobile locations.

Connections from the college network to external networks must be approved by the Information Security Officer after a risk analysis has been performed to ensure that the connection to the external network will not compromise the college network. Connections will only be allowed when the external networks have acceptable security controls and procedures or when the college has implemented appropriate security measures to protect the network resources of the college from the external network.

The Information Security Officer must approve any external connection to the college network to ensure that the connection does not compromise the college network. This includes the use of a college computing device to establish an external connection and automatically report a problem or suspected problem.

Employees and Non-Employees must be authorized by college management to work from a remote location. Appropriate arrangements will be made through written policy and procedures to ensure that the remote work environment provides adequate security for college data and computing resources, including protection against theft of college equipment, misuse of college equipment, unauthorized disclosure of college information, and unauthorized access to the college network or other facilities by anyone other than the authorized Employee or Non-Employee.

Segregation of Networks

When the college network is connected to another network, or becomes a segment on a larger network, appropriate controls will be in place to prevent users from other connected networks access to sensitive areas of the college private network. Routers or other technologies must be implemented to control access to secured resources on the college private network.

Operating System Access Control

Access to operating system code, commands and services must be restricted to those Employees who need this access in the normal performance of their job responsibilities. When possible, each individual will have a unique privileged account for their personal and sole use so that operating system activities are able to be traced back to a responsible person. When there is a clear business requirement or system limitation, a single privileged account for more than one individual may be used. In these cases, approval of the Information Security Officer is required and additional controls must be implemented to ensure that individual accountability is maintained.

When possible, the username of a privileged account should not reflect the privileged status of the account. Individuals with privileged accounts must have a second account for performing normal business functions such as use of the college email system.

Application Access Control

Access to college applications and systems must be restricted to those Employees needing such access to perform their job responsibilities. Access to source code for applications and systems

must be further restricted to those Employees and Non-Employees whose job responsibilities include direct support for the applications.

Monitoring Application Access and Use
Applications and systems will be monitored to detect deviation from access control policies and to record events for evidence and use when reconstructing lost or damaged data. Depending on the nature of events, continuous or periodic monitoring may be appropriate. Audit logs recording exceptions and other security-relevant events that represent security incidents or deviations from policies will be produced and maintained to assist in future investigations and access control monitoring. When technically possible, audit logs will include the following

- usernames
- dates and times for logon and logoff
- workstation location

Part 9 Systems Development and Maintenance

The software for information systems is acquired or developed to support the business and instructional needs of the college. These information systems are critical to the operation of the college and must be protected from unauthorized access in order to prevent disruptions with their usage or tampering with their data.

Security must be built into all information systems used by the college. Security issues will be identified during the requirements phase of an implementation project and must be justified, agreed to, documented and presented as part of the overall business case for the implementation project. The Information Security Officer must be kept informed of all security issues during the entire implementation project.

Security requirements and controls must reflect the value to the college of the involved information and the potential damage that could result from an absence or failure of security mechanisms. This is especially critical for web and other online applications. The process of analyzing security requirements and identifying appropriate security controls must be performed by IT Staff and Information Experts, reviewed by the Information Security Committee, and approved by the Information Security Officer.

For information systems that are critical to college operations this process to assess threat and manage risk will include the following:

- development of a data profile to understand the risks
- identification of security measures based on data protection requirements
- implementation of security controls based on the identified security measures and the technical architecture of the system
- implementation of a process for testing the effectiveness of the security controls
- development of processes and standards to support system changes to support system administration and to measure compliance with established security requirements

Data Validation

Data entered into an information system must be validated in order to detect data input errors and to ensure accuracy and correctness. When possible the data validation should be applied by the information system to ensure consistent and complete implementation of the rules for determining data accuracy and correctness. When not possible, college personnel must be identified to perform the data validation.

Information system design must ensure that controls are implemented to minimize the risk of processing failures leading to a loss of data or system integrity. When possible, programs to recover from data failures that access, add, change and delete data functions will be developed as part of the information system.

Strict controls must be implemented for changes to information systems to minimize the possible corruption of these systems and the resulting disruption to the operations to the college. Formal change control procedures will be developed, implemented and enforced to ensure that information security is not compromised. These change control procedures will apply to college information systems including computer hardware, computer application software, computer system software, network hardware and network software.

Access to source code libraries for college information systems must be tightly controlled to ensure that only authorized individuals have access to these libraries and will be logged to ensure that all access to these libraries can be monitored.

Part 10 Compliance

Compliance with this Information Security Policy is mandatory. Each Employee and Non-Employee must understand their roles and responsibilities regarding information security issues and the protection of college information assets. Failure to comply with this Policy or any other security policy that results in the compromise of college information may result in appropriate action as permitted by negotiated agreement, regulation, rule or law. The Information Security Officer will facilitate all matters relative to compliance with this Policy and the college will take all administrative and legal steps necessary to protect college information assets.

Monitoring

The college reserves the right to inspect, monitor and search all college information systems consistent with applicable law, employee contracts and college policies. College computers and networks are provided for business purposes and, therefore, staff members should have no expectation of privacy for information stored on college computers or transmitted across college networks. The College additionally reserves the right to remove any unauthorized material from college information systems.

Responding to a Suspected Breach of Private Data Procedure

New York State recently enacted the Information Security Breach and Notification Act to provide people with notice that their private information was acquired due to a security breach. A rationale is provided in the below Legislative Intent section of the law.

Legislative Intent
The legislature finds that identity theft and security breaches have affected thousands statewide and millions of people nationwide. The legislature also finds that affected persons are hindered by a lack of information regarding breaches, and that the impact of exposing information that should be held private can be far-reaching. In addition, the Legislature finds that state residents deserve a right to know when they have been exposed to identity theft.

The legislature further finds that affected state residents deserve an advocate who can speak and take action on their behalf because recovering from identity theft; can, and sometimes does, take many years. Therefore, the legislature enacts the information security breach and notification act which will guarantee state residents the right to know what information was exposed during a breach, so that they can take the necessary steps to both prevent and repair any damage they may incur because of a public or private sector entity's failure to make proper notification.

The law requires any state agency or business that owns or licenses a computerized database which includes vulnerable personal information to disclose any breach of security of such system to any resident of NYS whose personal information may have been acquired by an unauthorized person. The CSCIC (NYS Office of Cyber Security and Critical Infrastructure Coordination) has added a component to the NYS Information Security policy that also requires notification to nonresidents of NYS.

The law additionally requires notification to three NYS Offices (Attorney General, CSCIC and Consumer Protection Board) in the event of a security breach that results in personal information being acquired by an authorized person. The form and process to be used for notifications to these NYS Offices is published on the CSCIC website at: http://www.cscic.state.ny.us/security/securitybreach/ReportForm11_07.doc

College Compliance
The college will comply with this law by following the procedures outlined in Part 4. If the breach involved student private information, all potentially affected students will be provided with the following information:

- A summary of what occurred
- Advice to monitor any suspicious activity involving possible misuse of information to establish unauthorized credit.
- The U.S. government's central web site maintained by the Federal Trade Commission (FTC) for information about identity theft - www.ftc.gov/IDTheft
- Social Security Administration fraud telephone number, if applicable *(800.1269-0271)*
- Credit Bureau numbers, if applicable (Equifax 800/525-6285; Experian 888/397-3742; Trans Union 800/680-7289)

SUNY Cyber Incident Reporting Procedure

All state agencies, including SUNY and its campuses, have to report unusual or serious cyber security incidents using two State forms: *Initial Report* and *Final Report.* Based on incidents reported to the Information Security Officer, that Officer will assure compliance with these reporting requirements, which are outlined below.

The *Initial Report* describes the nature of the incident, how, when and where it was found, and its impact on services and information – information that management (e.g. CIOs) on campus would want to know about anyway within an hour or two of an incident.

The *Final Report* is filed after the incident has been understood and resolved. It reports the details of the compromised systems, source of the attack, steps taken to investigate and fix the problem and an assessment of its impact on services and costs.

An initial working definition of a cyber-incident is provided in the next paragraph. To understand what is being requested, we must be clear about the purpose. The purpose is to strengthen ourselves through communication prior to and during exposure to unusual or highly damaging information security incidents. Our incident reporting enables the State to provide coordination against cyber-attacks and for legal actions against intruders, to facilitate warnings and share preventative information, and to collect statewide information on the frequency, impact and cost of attacks. The goal is to help all of us recover from cyber incidents in a timely and secure manner to minimize impact on other state entities.

Types of incidents that should be reported*

- Unauthorized access
- Infections by malicious code
- Denials of service
- Reconnaissance scans and probes

*Do not report malicious cyber activity that is considered normal in today's networked environment. The purpose of the policy is to provide *helpful* information to each other; we should report only incidents that are unusual and have significant impact.

Report incidents that are unusually:

- Damaging or impending
- Threatening to life or sensitive information
- Persistent
- Wide-spread
- Resistant to defenses
- Valuable for other IT managers to know about

Type of Activity	***Report/ Do Not Report***	**Description of Activity**
Access	*Report*	Access to a person's electronic HR file from unknown intruders from the internet
	Do Not Report	Unauthorized reading of another person's electronic HR file by an employee who had read access but no job requirement to access it
Congestion	*Report*	A sustained denial-of-service attack on a campus resource
	Do Not Report	Serious network congestion caused by peer-to-peer traffic used by students
Intrusion	*Report*	Intrusion (e.g. via root) to a campus email server
	Do Not Report	Intrusion on a PC in a public lab
Virus Activity	*Report*	An outbreak of a new virus that was spreading rapidly
	Do Not Report	Normal level of virus activity, or an outbreak of a known virus in a department or college

Procedure:

1. Call (518) 320-1800 (System Administration Customer Services Help Desk)
   - to alert the SUNY ISO and briefly describe the incident
   - to receive possible updated details on the procedures
   - if necessary, to receive a new copy of the CSCIC *Initial Report*
   - to receive instructions for password protecting the *Initial Report*
2. Fax (518) 443-5273 the completed *Initial Report*
3. Email: Customer.Services@suny.edu the password protected *Initial Report*
4. Contingencies:
   - if you get voicemail, leave a message and call (518) 443-5179 or (518) 443-5596
   - if you still get voicemail or the phones are out of service, email **Customer.Services@suny.edu** stating that you have a cyber-incident
   - if it is off-hours (nights, weekends, holidays) or two hours have passed without response, and you need assistance in dealing with your incident (technically, forensically) or your incident is urgently important for others in the State to know about, call or email the State Office of Cyber Security and Critical Information Coordination at (866) 767-4722/(866)STS-ISAC; IRT@CSCIC.STATE.NY.US