COMMUNITY COLLEGE SYSTEM OF NEW HAMPSHIRE
INFORMATION SECURITY POLICY

I. Policy Statement

The CCSNH and its Colleges are committed to meeting administrative needs, complying with all applicable laws, and maintaining an information security program to help 1) ensure the individual privacy and confidentiality of educational, personnel, financial and other records containing sensitive information through systematic and consistent management of all records, 2) protect the integrity of information technology and storage systems, 3) minimize interruptions that affect productivity and 4) protect the reputation of CCSNH and its Colleges.

II. Policy Purpose

The purpose of this policy is to:

- Establish and communicate responsibilities for the security and protection of CCSNH information assets;
- Promote compliance with state and federal laws protecting confidential business and personally identifiable information;
- Strengthen safeguards against the inadvertent disclosure of confidential information;
- Provide a secure environment for the dissemination and retention of CCSNH information assets;
- Increase awareness of and the need for protecting security of information technology and storage systems;
- Reduce the risk of security threats to information technology and storage systems.

III. Scope of Policy

This policy applies to all CCSNH and College departments, offices, employees, students, contractors, and any other person who has access to CCSNH Information. This policy covers all information technology and storage systems, used for the creation, receipt, maintenance, storage, use, destruction, or preservation of CCSNH information assets in any format, computer-based and non-computer-based, automated and manual, including systems managed or hosted by third parties on behalf of CCSNH and its Colleges. Individual accountability is expected of all individuals when accessing CCSNH information technology and storage systems.

IV. Definitions

Authentication: A process of identifying an individual, based on a username and password.

Availability: The ability of a user to access information or resources in a specified location and in the correct format.

CCSNH Chief Information Officer: The individual at CCSNH who is responsible for the information technology and computer systems that support enterprise goals.

CCSNH Chief Information Security Officer: The individual at CCSNH who is responsible for overseeing the system vision, strategy, and program to ensure information assets and technologies are adequately protected. The individual identified as having responsibility for maintenance and delivery of CCSNH's Information Security and related policies and procedures, including Computer Use Policy, Process for Responding to a Suspected Breach of Private Data and Cyber Incident Reporting Procedures. The CISO is the point of contact for College Information Security Officers, external auditors or agencies for information security and privacy matters.

College Information Security Officer: The information technology staff member within the College responsible for overseeing the College vision, strategy, and program to ensure information assets and technologies are adequately protected.

Computer Information Security Committee: A committee comprised of the CCSNH Chief Information Security Officer, CCSNH Chief Information Officer and the College Information Security Officers. The Committee is charged with identifying computer information security risks and preventative initiatives and developing recommendations for policies, procedures, and standards to address those risks and preventative initiatives that enhance the security and protection of CCSNH and College networks, information, and information systems.

Encryption: Encryption is the conversion of electronic data into another format, which cannot be easily understood by anyone except authorized parties.

Firewall: A network appliance that controls incoming and outgoing network traffic based on a configured set of rules.

Information Asset: A body of information defined and managed as a single unit so it can be understood, shared, protected and utilized effectively. Information assets have recognizable and manageable value, risk, content and lifecycles. An information asset has one or more of the following characteristics: 1.) It has a value to the organization; 2.) It will cost money to reacquire the information; 3.) There may be legal, reputational or financial repercussions if the information cannot be produced on request; 4.) It will have an effect on operational efficiency if the information cannot be accessed easily; 5.) There would be consequences of not having the information; 6.) There is a risk associated with the information – a risk of losing the information, a risk that the information is not accurate, a risk that someone may try to tamper with it, a risk arising from inappropriate disclosure; 7.) The information has specific content and uses; 8.) The information has a manageable lifecycle; 8.) Information with similar content and uses is disposed of in the same way and according to the same rules.

Information Owners: Individuals identified as having specific responsibility within their general area of responsibility for: 1) classifying the information assets and resources; 2) determining the access rights and privileges for information assets and resources; 3) communicating to the Information Security Officer the requirements for access and disclosure.

Information Technology Staff: Individuals identified as having responsibility for, but not limited to, the following computer-based information: 1) implementing access rights and privileges, as defined by Information Owners; 2) implementing back-up and recovery procedures for centrally-maintained information technology and storage systems; 3) recommending back-up and recovery procedures for departmentally-maintained information technology and storage systems; 4) providing the information technology systems infrastructure necessary to support information security.

Information Security Incident: A real or suspicious event that may adversely affect the security of CCSNH's network or systems that process, store or transmit CCSNH information.

Integrity: Relative assurance that the data being accessed or read has neither been altered nor damaged through a system error since the time of the last authorized access.

Personally Identifiable Information (PII): Information protected by State or Federal privacy laws that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Sensitivity: The property of data that reflects a harmful and measurable impact resulting from disclosure, destruction or modification.

V. Information Security

A. General Principles

Information security management enables both the sharing and protection of Information Assets. Information Assets are among the most valuable assets of CCSNH and the Colleges. The availability and reliability of Information Assets are keys to supporting the educational and business activities of CCSNH and the Colleges.

All CCSNH and College departments, offices, employees, students, contractors, and any other person who has access to CCSNH Information Assets are responsible for protecting the security of Information Assets. Each authorized user is obligated to preserve and protect these Information Assets in a manner consistent with this policy.

Information Owners and Information Technology Staff have primary responsibility for assuring that appropriate controls are in place to preserve the security of these Information Assets. Information security controls described within this policy are intended to provide the essential physical and procedural safeguards to achieve this goal.

Information Assets must only be used in relationship to the educational and business activities of CCSNH and the Colleges and must be protected from the time of creation throughout the 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 upon the sensitivity of the information.

B. Individual Accountability

Individual accountability is the cornerstone of this policy and required whenever accessing Information Assets. The following requirements must be adhered to when accessing information on CCSNH computer systems and networks.

1. Access may only be provided to an authorized individual using an individually assigned unique identifier known as a computer username together with an associated computer password;

2. An individual may be provided access to authorized information only after proper Authentication;

3. An individual may only access information for which he or she has the appropriate authorization and may only use such information for the legitimate business purposes for which access is authorized;

4. An individual may not share his or her computer username and password as each individual is responsible for protection against unauthorized information access through the use of his or her computer username and password;

5. No individual should ever communicate a computer password using email or any other insecure means of communication;

C. Information Owners and Information Technology Staff Responsibility

All Information Assets must have an Information Owner established within the responsible functional area of CCSNH or each College. Information Assets must be protected from unauthorized access to maintain the confidentiality, integrity and availability of the information.

1. Information Owners are responsible for working with Information Technology Staff to implement access rights and privileges to provide access to computerized information for use by CCSNH and College employees, students, and other persons as needed for normal business activities.

2. Information Technology Staff are responsible for implementing backup and recovery procedures for centrally-maintained computer-based Information Assets and for recommending backup and recovery procedures for departmentally-maintained

computer-based Information Assets to provide protection and timely recovery from any corruption, loss or theft of computer-based information.

3. Information Owners are responsible for implementing procedures to provide authorized access to and protection of non-computer-based information.

VI. Information Classification

Information Assets have different values, risks, content and lifecycles. Depending upon these characteristics, Information Assets require different levels of protection.

A. Categories – Public or Restricted

Information Owners are responsible for initial classification of information as Public or Restricted (Internal, Confidential or Private) based upon the consequences of loss, the legal or retention requirements, the sensitivity and the value of the information. In classifying data, the characteristics to be considered should include, among other things, the need to maintain confidentiality, data integrity and availability. Information Owners in consultation with Information Technology Staff are responsible for making decisions regarding user access rights, user access privileges and daily management of the information. The Information Owner should periodically reassess the Information Asset's classification through an analysis of the value, risks, content and lifecycle of the information.

1. **Public Information** is information that can be freely provided to anyone without any possible damage to CCSNH and the Colleges. Examples of Public Information are: Board of Trustees' minutes; course catalogs; press releases.

2. **Restricted Information** is all other information. Restricted Information is categorized as Internal, Confidential and Private with correspondingly increased levels of sensitivity and restrictions imposed on its handling and distribution. Restricted Information categorized as Private or Confidential is more critical and sensitive than Restricted Information categorized as Internal and should be protected in a more secure manner. Information Owners are responsible for working with Information Technology Staff to implement different levels of protection for different types of Restricted Information.

    a. **Internal Information** is information that is available to individuals with a legitimate educational or business interest for official purposes but not released to others unless requested pursuant to and authorized by CCSNH and the Colleges business practices, consistent with applicable law. The unauthorized disclosure, access or use of Internal Information would have a limited adverse impact on CCSNH, the Colleges and/or others. Examples of Internal Information include:
        - Directory information;
        - Financial accounting reports and budgets;

- Contracts;
- Admissions metrics and statistics;
- Donor contact information;
- Nonpublic CCSNH policies and procedure manuals.

b. **Confidential Information** is information that is available only to designated personnel or third parties with a legitimate educational or business interest but not released to others except pursuant to and authorized by CCSNH and the Colleges' business practices, consistent with applicable law. Confidential Information is information that is not available to the public under applicable state or federal law, including but not limited to information protected by the Family Educational Right to Privacy Act (FERPA) and the New Hampshire Right to Know Law (RSA 91-A). The unauthorized disclosure, access or use of Confidential Information would have a significant adverse impact on CCSNH, the Colleges and/or others. Examples of Confidential Information include:
    - Admissions records;
    - Student records other than directory information;
    - Personnel records;
    - Internal personnel practices;
    - Confidential commercial, or financial information from any source or third-party information subject to a nondisclosure agreement with CCSNH or the Colleges;
    - Library user information;
    - Campus security investigations, emergency, measures and surveillance information;
    - Test questions, scoring and other examination information;
    - Equity complaints and investigations;
    - Collective bargaining negotiations;
    - Information subject to attorney-client privilege;
    - Student grievance and disciplinary proceedings.

c. **Private Information** is information that is available only to designated personnel or third parties with a legitimate educational or business interest but not released to others except as expressly authorized by CCSNH and the Colleges' business practices, consistent with applicable law. Private Information is information that contains personally identifiable information (PII) pertaining to individuals and protected by state or federal law, including the Family Educational Right to Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the New Hampshire Right to Privacy Act (RSA 359-C) and the New Hampshire Right to Know Law (RSA 91-A). The unauthorized disclosure, access or use of Private Information would have a significant adverse impact on CCSNH, the Colleges and/or others and may require CCSNH to report such unauthorized disclosure to various federal or state agencies and/or financial institutions as well as the

individuals whose information was disclosed. Examples of Private Information include:

- Social security numbers;
- Health information;
- Credit card account information including credit card or debit card numbers, security codes, access codes, or passwords that would permit access to an individual's financial (credit card or bank) account;
- Personal financial information, including checking or investment account numbers;
- Driver's license or non-driver identification numbers;
- Individual health insurance policy identification numbers

B. Restricted Information – Protecting Personal Privacy Interests

Restricted Information that uniquely identifies individuals must be maintained consistent with federal and state laws and regulations and with CCSNH and College policies. All individuals with access to Personally Identifiable Information (PII) must preserve and protect the confidentiality of that information. PII must be secured and protected by:

1. Restricting access to only authorized individuals;
2. Correcting information if incorrect information is known to exist;
3. Removing or making inaccessible information, if appropriate and consistent with applicable laws, regulations and CCSNH and College policies;
4. Collecting information in a manner consistent with applicable laws, regulations and CCSNH and College policies;
5. Protecting computer-based and non-computer-based access controls;
6. Retaining and disposing of information in a manner consistent with applicable laws, regulations and CCSNH and College policies including, where applicable, disposing of information by physical destruction of the media on which the information is stored or by erasing the information from the media in a manner that results in the information being totally unrecoverable;
7. Accessing and using information only as authorized for legitimate educational and business purposes;
8. Not disclosing information unless expressly authorized or required by law, regulation or CCSNH and College policies.

C. Restricted Information – Protecting CCSNH and Third-Party Interests

Restricted Information (Internal or Confidential) that concerns CCSNH, its Colleges or third-party organizations must be maintained consistent with federal and state laws and regulations and with CCSNH and College policies and contractual obligations. All individuals with access to Internal or Confidential Information that concerns CCSNH, its Colleges or third-party organizations must preserve and protect that information. Internal and Confidential Information must be secured and protected by:

1. Restricting access to only authorized individuals;

2. Correcting information if incorrect information is known to exist;
3. Removing or making inaccessible information, if appropriate, and consistent with applicable laws, regulations and CCSNH and College policies;
4. Collecting information in a manner consistent with applicable laws, regulations and CCSNH and College policies;
5. Protecting computer-based and non-computer-based access controls;
6. Retaining and disposing of information in a manner consistent with applicable laws, regulations and CCSNH and College policies, including, where applicable, disposing of information by physical destruction of the media on which the information is stored, or by erasing the information from the media in a manner that results in the information being totally unrecoverable;
7. Accessing and using information only as authorized for legitimate business purposes;
8. Not disclosing information unless authorized or required by law, regulation or CCSNH and College policies.

D. Public Information – Accessibility of Web Content

Public Information that is maintained on CCSNH and College websites must comply with federal and state laws and regulations as well as CCSNH and College policies and standards. CCSNH and the Colleges shall develop Protocols for Developing Accessible Web Content and Protocols for Responding to Accessible Web Content Issues to accomplish compliance.

VII. Personnel – Information Security Responsibilities

To reduce the risk of human error and misuse of information, personnel information security responsibilities will be considered during the hiring process for employees, during the contracting process for third parties, and by monitoring compliance with information security responsibilities during the length of an individual's employment or a third party's contract.

A. Information Security in Job Responsibilities

The information security responsibilities of employees and third parties must be documented. For employees, information security responsibilities should be included in job descriptions, trainings and acknowledgements, as appropriate, and for third parties, they should be included in contractual terms and conditions. These information security responsibilities may include both general and specific responsibilities for protecting information and for performing tasks related to information security procedures and processes such as requirements that limit access to Restricted Information to those who have a need to know as defined by job duties and subject to approval, prohibit disclosure of Restricted Information except for a legitimate educational or business purpose, and prescribe acceptable electronic transfer, storage and disposal methods.

B. Information Security Training

Personnel with access to Information Assets must be provided with specific information security training to insure knowledge of their security responsibilities to protect information and

knowledge of CCSNH and College information security policies, procedures and protocols to minimize information security risks. These same persons must additionally be provided with specific update training to maintain knowledge of current CCSNH and College information security policies and procedures.

All personnel must be provided with general information security training to ensure knowledge of CCSNH and College information security policies and procedures.

C. Reporting and Responding to Security Incidents

Actual or suspected information security incidents must be reported following the procedures defined in the Cyber Incident Reporting Procedure and the Procedure for Responding to a Suspected Breach of Private Data. All persons with access to Information Assets must be made aware of their duty to report and the procedures for reporting different types of incidents that might impact the security of Information Assets.

Actual or suspected information security software malfunctions, such as a virus not being detected, must be report to the CCSNH CISO following the procedures defined in the Cyber Incident Reporting Procedure. The event should be thoroughly described by the person reporting the incident.

Actual or suspected information security threats or weaknesses, such as unauthorized access to Restricted Information, must be reported to the CCSNH CISO or College CISO following the procedures defined in the Procedure for Responding to a Suspected Breach of Private Data. The event should be thoroughly described by the person reporting the incident. Persons must not attempt to prove a suspected security weakness or threat unless authorized to do so by the CCSNH CIO as testing a suspected weakness or threat may have serious, although unintended, consequences.

The CCSNH CISO should notify the person(s) involved and his/her supervisor of the results of the investigation into a security incident and measures that should be taken to prevent a similar incident after the incident has been resolved and closed.

D. Tracking Security Incidents

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

VIII. 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. CCSNH and the Colleges should review these and other locations on an ongoing basis to determine the need for additional physical security mechanisms to reduce overall information security risks.

A. Physical Security

A breach of physical security may threaten the integrity of CCSNH Information Assets. Physical security is achieved by creating physical barriers around the Information 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 physical barrier.

CCSNH and the Colleges should perform an analysis 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 should then be implemented. A physical security perimeter must be established for information processing and storage facilities of critical or sensitive information including the CCSNH data center and CCSNH and College network wiring closets for data, security and telephone equipment and cabling.

The protection of critical or sensitive information contained on storage devices such as hard disk drives or magnetic tape media 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.

B. 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 uninterruptible electrical power distribution must be established for information processing and storage facilities for critical or sensitive information including the CCSNH data center and CCSNH and College major networking closets for data, security and telephone equipment and cabling. Special environmental systems for backup electrical power distribution should be established for the CCSNH data center and CCSNH and College major networking closets for data, security and telephone equipment and cabling. Special environmental systems for air conditioning and humidity control and for uninterruptible electrical power distribution should be established for other network wiring closets for data, security and telephone equipment and cabling.

The protection of critical or sensitive information visible on computer screens is another important element of environmental security. Computer screens should be faced so as to be visible only to the authorized user of the computer and should use a screen saver with a screen saver password to insure that information is not displayed after a specified period of time.

IX. Communications and Network Management

The CCSNH network must implement appropriate security controls to ensure the integrity of data flowing across the networks, and, if there is a business need, additional measures to ensure the confidentiality of the data must also be implemented. Before CCSNH or any of the Colleges outsources an application to a third-party vendor or other external entity, the CIO must ensure that measures are in place to mitigate any new security risks created by connecting the CCSNH network to a third-party network and must have periodic security reviews performed to ensure compliance with this standard. All third-party connections to the CCSNH network must be authorized by the CIO.

A. Sharing Information with External Entities

Minimally the below process must be followed before sharing Restricted Information with an external entity.

- evaluate and document the sensitivity of the information to be shared
- identify the responsibilities of each party for protecting the information
- provide a signoff procedure for each party to accept these responsibilities
- define the minimum controls required to transmit and use the information
- record the measures that each party has in place to protect the information
- define a method for compliance measurement
- establish a procedure and schedule for reviewing the controls
- define a method for disposition of the information

B. Network Management

Minimally, the below controls must be implemented to prevent unauthorized access and use of the CCSNH network.

- separate operational responsibility for networks and computer systems
- establish responsibilities and procedures for remote use (See Access Control)
- implement special controls when necessary to safeguard the integrity and confidentiality of data passing over public networks

C. Vulnerability Scanning

Computer systems that provide information through a public network must be subjected to vulnerability scanning. These systems must 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 CCSNH network must 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 scans will be reviewed in a timely manner by the Computer Information Security Committee 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 must be performed at least regularly to ensure that no major vulnerabilities have been introduced into the environment. The frequency of scans will be determined by the Computer 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 CIO.

D. 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

The output of the testing will be reviewed in a timely manner by the appropriate members of the Computer Information Security Committee 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 regularly to ensure that no major vulnerabilities have been introduced into the environment. The frequency of tests will be determined by the Computer Information Security Committee 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 penetration and intrusion testing by the CIO.

E. Acceptable Use of Computer Systems and Networks

All provided access must adhere to the acceptable use of computer systems and networks as defined in the Acceptable Use Policy.

F. External Connections

Connections from the CCSNH network to external networks must be approved by the CIO after a risk analysis has been performed to ensure that the connection to the external network will not compromise the CCSNH network. Connections will only be allowed when the external networks have acceptable security controls and procedures or when the CCSNH has implemented appropriate security measures to protect CCSNH network resources. Firewalls, DMZs (demilitarized zones) or both may be implemented between the third-party and CCSNH to achieve an appropriate level of protection. Any connections between CCSNH 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 CCSNH 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 Information Technology Staff and authorized third-party staff will be permitted to use tools to monitor network activity on external connections. Authorized Information Technology Staff will regularly monitor external connections for abuses and anomalies.

G. Internal Connections

Wired connections from devices that are not maintained by Information Technology Staff to the CCSNH network must be approved by the CIO after a risk analysis has been performed to ensure that the connection from the device will not compromise the CCSNH network. Connections will only be allowed when the devices that are not maintained by Information Technology Staff have acceptable security controls and procedures to protect CCSNH network resources. These controls and procedures are to include, but are not limited to, firewalls and properly updating operating system and virus protection software. 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 Information Technology Staff and authorized third-party personnel will be permitted to use tools to monitor network activity on internal connections. Authorized Information Technology Staff will regularly monitor internal connections for abuses and anomalies.

H. Portable Devices

Portable computing resources and information media must be secured to protect the integrity of Restricted Information. No portable computing resource may be used to store or transmit Restricted Information without appropriate security measures that have been approved by the CIO and approved or implemented by Information Technology Staff in order to protect the Restricted Information. No outside computing resource (sometimes referred to as Bring Your Own Device (BYOD)) may be used to store or transmit Restricted Information. All Restricted Information may only be accessed using a CCSNH owned and managed device.

The use of portable computing resources such as laptops, notebooks, PDAs (personal digital assistants) and mobile phones, must involve special care to protect Restricted Information. Approval for use of portable computing resources to access Restricted Information is contingent on satisfaction of the below requirements:

- When using portable computing resources in public and other unprotected locations external to CCSNH or the Colleges, the use of encryption to protect the transmission of Restricted Information must be implemented and special care must be taken to protect against unauthorized persons viewing Restricted Information
- Protection against malicious software on portable computing resources must be implemented and maintained at current levels

- Back-ups of Restricted Information on portable computing resources must be created regularly, and the physical information media on which the back-ups are maintained must be adequately secured to protect against loss or theft
- When in use, portable computing resources on which Restricted Information is stored must not be left unattended
- When not in use, portable computing resources on which Restricted Information must be physically secured
- Portable computing resources on which Restricted 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
- Portable computing resources on which Restricted Information is stored must use encryption or other means to ensure that Restricted Information is secured from unauthorized access in the event that the portable computing resource is lost or stolen

While an off-worksite desktop PC would not be considered a portable device, the above regulations for the use of portable devices to store or transmit Restricted Information apply equally to off-worksite desktop PCs.

I. Telephones, Scanning and Fax Equipment

Employees should adhere to the following guidelines when using telephones, scanning and fax equipment, both internal and external to CCSNH and the Colleges, to mitigate potential information security risks.

- Care should be taken to prevent conversations involving confidential matters from being overheard
- Avoid the use of mobile phones when discussing Restricted Information
- Avoid leaving messages involving confidential matters on voicemail systems
- Contact the recipient to ensure protection of a fax and verify the destination fax phone number when sending Restricted Information
- Avoid using third-party, Internet or wireless fax services to send or receive Restricted Information
- Care should be taken in sending teleconference access numbers if Restricted Information will be discussed during the teleconference
- Confirm that all attendees are authorized participants before starting any confidential discussions when chairing a teleconference

Fax equipment and scanners should be configured to regularly delete any stored files that exist on the internal hard drives. When fax machines and scanners are placed out of commission, the hard drives should be removed and destroyed.

J. Wireless Networks

Wireless devices and technology create opportunities for providing instruction and conducting business functions of CCSNH and the Colleges. Everything that is transmitted on a wireless network, however, could be intercepted by a person within the coverage area of a wireless

transmitter. The following guidelines should be adhered to when implementing and using wireless networks.

- Wireless network access points must not be installed without approval of the CIO
- Suitable security controls, such as authentication, encryption and MAC (Media Access Control) address restriction, must be implemented to ensure that a wireless network access point cannot be exploited to disrupt college services or gain unauthorized access to Information Assets
- Restricted Information must not be transmitted on a wireless network unless suitable security controls, such as encrypted VPN, have been implemented and approved by the CIO

K. Modem Usage

Dial-up modems must not be connected to computer systems which are also connected to the CCSNH network without approval of the CIO.

L. Public Web Servers and Public Websites

The Internet provides an opportunity for CCSNH and the Colleges to disseminate information and provide interactive services quickly and cost effectively. Because a public web server is accessible globally and provides a potential connection path to the CCSNH network, an insecure public web server may be used to obtain Restricted Information, disrupt college services or assist in an illegal activity such as an attack on the website of some other organization. Website services for the entire CCSNH community are provided on a centralized server(s) by the Information Technology Department and that the use of any other CCSNH or College computer for the purpose of serving a website is prohibited except as expressly authorized by the CIO.

CCSNH and the Colleges' website content must be approved by CCSNH or the College. Content may be reviewed with consideration for copyright issues, for confidentiality, privacy and sensitivity, for accuracy and for any potential legal implications of providing the information. Faculty, staff and student organizations have the ability to create CCSNH hosted web pages. While the content of such web pages is not reviewed prior to posting, the content of such web pages is subject to compliance with the Acceptable Use Policy, with federal and state laws regarding use of computers and electronic communications. No material included on such CCSNH hosted web pages may violate any laws or CCSNH policies, including but not limited to, those regarding obscenity, harassment of others and copyright infringement. Any person who knowingly violates such laws or CCSNH policies will be subject to loss of access privileges, disciplinary action and possible prosecution.

X. Operations Management

Operating instructions and incident response procedures should be established and documented for the management and operation of all information processing facilities. Procedures should 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.

A. Security Incident Management

All provided access to Information Assets must adhere to the Cyber Incident Reporting Procedure and the Procedure for Responding to a Suspected Breach of Private Data for reporting any event that may have an impact on the security of Information Assets.

Security incident management procedures and responsibilities must be established and documented to ensure an effective, orderly and timely response to any security incident in order to restore any disrupted services as quickly as possible. The response to any security incident must additionally include analysis of the cause of the incident and implementation of any corrective actions to prevent re-occurrence of the same incident.

B. Separation of Development, Test and Production Environments

Development, test and production computing environments must be separated either logically or physically. Procedures must 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 must be maintained in development environments isolated from production environments
- When not required, access to compilers, editors and other system utilities must be removed from production environments
- Login procedures and environmental identification must be sufficiently unique between development, test and production environments
- Short-term access controls must 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 CIO to ensure adequate protection of production environments. CCSNH and the Colleges must also consider a stable testing environment where user acceptance testing may be conducted without changes being made to the software being tested.

C. 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 must be documented, implemented and tested prior to acceptance of systems and must be regularly reviewed during use of systems. The processor, memory and storage requirements of systems must 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.

Information Technology Staff and the CIO must 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.

D. 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, data or any other hardware, software, Information Asset or CCSNH system or College process that could significantly disrupt the operations of CCSNH or a College. All persons who have access to CCSNH Information Assets must adhere to procedures defined in the Cyber Incident Reporting Procedure for reporting a suspected malicious code incident.

E. Software Maintenance

All vendor software must be maintained at supported levels to ensure accuracy, integrity and supportability unless otherwise approved by the CIO. All CCSNH- or 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.

F. Information Back-Up

Critical CCSNH and College data and software must be backed-up regularly. A risk assessment must be performed for all systems on which Information Assets are 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 must be considered. Systems to be analyzed must include networks, servers and workstations.

For critical systems processes must 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 must be developed, implemented and periodically tested for all critical CCSNH and College systems. The results of testing must be documented and any detected deficiencies must be corrected in a timely manner.

G. System Security Checking

Systems that provide critical services must 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 CISO and immediately corrected by Information Technology Staff. The CISO must be informed of the vulnerability and must initiate an investigation to determine if any Restricted Information

had been compromised.

XI. Access Control

Logical and physical access control mechanisms must be implemented in order to protect the availability, privacy, confidentiality and integrity of Information Assets. The level of security provided by these mechanisms for each information asset should be commensurate with the criticality, sensitivity and legal properties of the asset. Information Owners will be responsible for making decisions regarding user access rights and privileges based on job responsibilities of the user consistent with the protections set forth in this policy.

A. User Registration Management

CCSNH and the Colleges must 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 computer applications and the information required in the performance of their job responsibilities.

The user registration management process must 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 Owners must approve access rights (who should have access) and privileges (what access should be provided) for information resources within their area of responsibility.

B. Privileged Accounts Management

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

C. User Password Management

Passwords are a common means of authenticating the identity of a user to provide access to information systems. Password standards must be developed and implemented to ensure that authorized individuals accessing CCSNH information technology resources are following proven password practices or rules. Whenever possible, these password practices or rules must be automatically required by system controls and should include but not be limited to the 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
- Passwords should contain a mix of alphabetic, numeric, special and upper/lower case characters
- Passwords should not be automatically included in any logon process

D. Network Access Control

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

E. Remote Access Control (User Authentication for External Connections)

CCSNH requires that individual accountability be maintained by all persons who have access to CCSNH Information Assets at all times, including during remote access, in order to maintain information security. Any access from an external connection to the CCSNH network is a remote access. Remote access to any CCSNH computer system must be authorized by the CIO and performed via a suitable security control, such as encrypted VPN. External connections to the CCSNH network must 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 must be in place to control remote access to CCSNH systems and networks from fixed and mobile locations.

Connections from the CCSNH network to external networks must be approved by the CIO 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 CCSNH has implemented appropriate security measures to protect the CCSNH network resources from the external network.

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

All persons who have access to CCSNH Information Assets must be authorized by CCSNH management to work from a remote location. Appropriate arrangements must be made through written policy and procedures to ensure that the remote work environment provides adequate security for CCSNH data and computing resources including protection against theft of CCSNH equipment, misuse of CCSNH equipment, unauthorized disclosure of Restricted Information and unauthorized access to the CCSNH network or other facilities by anyone other than the authorized user.

F. Segregation of Networks

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

G. Operating System Access Control

Access to operating system code, commands and services must be restricted to those personnel who need this access in the normal performance of their job responsibilities. When possible, each individual should 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. In the rare circumstance, 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 CIO 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 CCSNH email system.

H. Application Access Control

Access to CCSNH computer applications and systems must be restricted to those personnel needing such access to perform their job responsibilities. Access to source code for applications and systems must be further restricted to those personnel whose job responsibilities include direct support for the applications.

I. Monitoring Application Access and Use

Computer applications and systems must 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 must 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 identity (location)
- Record of rejected attempts to access applications
- Record of rejected attempts to access data

XII. Systems Development and Maintenance

The software for information systems is acquired or developed to support the business and instructional needs of CCSNH and the Colleges. These information systems are critical to the operation of CCSNH and the Colleges 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 CCSNH and the Colleges. Security issues must 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 CIO and CISO must be kept informed of all security issues during the entire implementation project.

Security requirements and controls must reflect the value to CCSNH and the Colleges 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 the Information Owner and Information Technology Staff, reviewed by the Computer Information Security Committee and approved by the CIO.

For information systems that are critical to CCSNH and College operations this process to assess threats and manage risk must 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

A. Input 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, CCSNH or College personnel must be identified to perform the data validation.

B. Control of Internal Processing

Even data that has been accurately and correctly entered into an information system may be corrupted by intentional or unintentional acts, or by processing errors. Data validation checks and business rules must be incorporated into information systems to identify inaccurate or incorrect data, and to prevent or stop a process from running that may be corrupting or compromising data and, more broadly, Information Assets.

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 should be developed as part of the information system.

C. Message Integrity

Message authentication is a technique used to ensure message integrity by detecting unauthorized changes to electronically transmitted data. Message authentication must be considered for information systems where there is a security requirement to protect electronically transmitted data. A security assessment of threats and risks must be performed to determine if message integrity is required and to identify the most appropriate method of message authentication. Message authentication does not protect against unauthorized disclosure. Encryption techniques must be used to protect against unauthorized disclosure during the electronic transmission of data.

D. Cryptographic Controls

Encryption is a cryptographic technique used to protect the confidentiality of information. Encryption must be considered when other security controls do not provide an adequate level of protection for information. The required level of protection will be determined based on a risk assessment that takes into account the encryption algorithm and the length of cryptographic keys. To the extent possible, consideration must also be given to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world and to the controls that apply to the export and import of cryptographic technology.

E. Cryptographic Key Management

If cryptographic techniques are used, a secure environment must be established to protect the deployed cryptographic keys. Access to this secure environment must be tightly controlled and limited to Information Technology Staff responsible for the implementation of this encryption. If a cryptographic key were compromised or lost, all information encrypted with the key would have to be considered at risk.

F. Protection of System Test Data

Test data must be protected. Acceptance testing of information systems usually requires large volumes of data and often the best test data is a copy of production data. When this is the case

the personnel performing the tests or having access to test data must be authorized by the appropriate Information Owner in the same way that access is authorized to production data.

G. Change Control Procedures

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 of CCSNH and the Colleges. Formal change control procedures must be developed, implemented and enforced to ensure that information security is not compromised. These change control procedures must apply to CCNSH information systems including computer hardware, computer application software, computer system software, network hardware and network software.

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

XIII. Compliance

Compliance with this Information Security Policy is mandatory. Each person who has access to CCSNH Information Assets must understand his or her role and responsibilities regarding information security issues and the protection of Information Assets. Failure to comply with this Policy or any other security policy that results in the compromise of CCNSH or College information may result in appropriate action including disciplinary action as permitted by negotiated agreement, policy, regulation, rule or law. The CISO will facilitate all matters relative to compliance with this Policy and CCSNH and the Colleges will take all administrative and legal steps necessary to protect their Information Assets.

A. Monitoring

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

B. Policy Amendments and Management

Requests for changes to this Policy must be presented to the CISO. The CISO will review requested changes with the Information Security Committee. Approved changes will formally be included in a revision to this Policy. This Policy will minimally be reviewed on an annual basis.