COMMUNITY COLLEGE
system of New Hampshire

Table of Contents – 500 Facilities Policies

562.01 Expressive Activity 2
1 Policy Statement 2
2 Policy Purpose 2
3 Scope of Policy 2
4 Definitions 2
5 Expressive Activity for the Campus Community 3
6 Expressive Activity for College Visitors 4
7 Appeal 5
8 Generally Applicable Rules for Expressive Activities 5
9 Enforcement 7
562.02 CCSNH Alcohol Policy 7
1 Policy Statement 7
2 Purpose 7
3 Policy 7
562.03 Video Surveillance Policy 8
1 Policy Statement 9
2 Policy Purpose 9
3 Scope of Policy 9
4 Notification of Video Surveillance and Policy 9
5 Camera Placement 10
6 Monitoring 10
7 Storage 11
8 Release of Information 12
9 Destruction or Tampering with Video Surveillance Technology 12
10 Violation of This Policy 12
562.04 Records Management and Retention Policy 13
1 Policy Statement 13
2 Policy Purpose 13
3 Scope of Policy 13
4 Definitions 14
5 Records Management Program Accountabilities 15
6 Recordkeeping Responsibilities for Departments and Offices 15
7 Good Records Management Practices 15
562.05 Firearms and Weapons on Campus Policy 16

1 Policy Statement 16
2 Policy Purpose 16
3 Policy 16
562.06 Information Security Policy 17
1 Policy Statement 17
2 Policy Purpose 17
3 Scope of Policy 18
4 Definitions 18
5 Information Security 19
6 Information Classification 21
7 Personnel – Information Security Responsibilities 24
8 Physical and Environmental Security 25
9 Communications and Network Management 26
10 Operations Management 31
11 Access Control 33
12 Systems Development and Maintenance 36
13 Compliance 38
562.07 Information Technology Acceptable Use Policy 39
1 Policy Statement 39
2 Policy Purpose 39
3 Scope of Policy 39
4 Privacy 40
5 General Use, Access and Ownership 40
6 Password Security and Protection 41
7 Unacceptable Use 42
562.08 CCSNH Campus Safety and Security 44
1 Policy Statement 44
2 Policy 45

** Rescinded and replaced by System Policies 562.06 and 562.07 on February 6, 2018.*

COMMUNITY COLLEGE
system of New Hampshire

562.01 Expressive Activity

Date Approved: 5/9/2018 *Date Effective: 8/6/2026*
Date of last Amendment: 8/6/2026 *Approved by: Mark Rubinstein, Chancellor*

1 Policy Statement

The Community College System of New Hampshire (CCSNH) is committed to supporting open expression and free speech by students and the public while establishing and maintaining a safe and secure environment for its students, faculty, staff, and visitors conducive to providing quality education. In light of these objectives and in developing and implementing this policy, CCSNH recognizes the freedoms established by the United States and New Hampshire Constitutions, including the rights of free speech and assembly. CCSNH also recognizes the need to preserve and protect its property, to provide a safe and secure environment for its students, faculty, staff and visitors, and to ensure the effective operation of its educational programs, business and related activities.

2 Policy Purpose

The purpose of this policy is to promote the free exchange of ideas and the safe and efficient operation of CCSNH and its colleges by:

A. Permitting free speech, assembly, and other expressive activities at its college campuses, regardless of the viewpoint expressed;

B. Maintaining an appropriate educational and work environment for all persons present on its college campuses; and

C. Protecting and maintaining the security of CCSNH and college property, students, faculty, staff and visitors.

In implementing this policy, CCSNH is not seeking to regulate the content of expressive activities.

3 Scope of Policy

This policy applies to any person seeking to engage in expressive activity on any CCSNH college campus in outdoor public areas. Expressive activities carried out under this policy shall not be considered to be authorized or endorsed by or on behalf of CCSNH or any of its colleges. This policy does not waive or otherwise impact any obligations the Campus Community may have to CCSNH or any of its colleges in the course of employment or enrollment.

This policy does not apply to the use of CCSNH college facilities or grounds for events sponsored by CCSNH or its colleges, or to conduct occurring inside CCSNH facilities. Spaces inside CCSNH facilities are not public forums.

This policy does not apply to any person or organization desiring to advertise or sell merchandise or services for commercial purposes on any CCSNH college campus.

4 Definitions

Expressive Activity includes any lawful verbal, written, audio-visual, or electronic means by which individuals may communicate ideas to one another, including all forms of peaceful assembly,

protests, speeches and guest speakers, distribution of literature, carrying signs, and circulating petitions. Expressive Activity does not include behavior, conduct, or expression that A) violates any law and could be subject to criminal action, or B), is unprotected by the free speech provisions of the United States or New Hampshire Constitutions, or C) constitutes harassment under any applicable state or federal law or regulation.

Campus Community includes students, administrators, faculty, and staff of the CCSNH college.

Blackout Days are certain days set by each college on its calendar, which may include but are not limited to examination periods, periods reserved for college events including graduation and related events, and semester break periods when classes are not in session, wherein the use of the college campus, including outdoor areas designated for expressive activities, are reserved exclusively for college related activities that are the very core of its primary educational mission. During these blackout days, no one shall be allowed to use the outdoor areas designated for expressive activities.

5 Expressive Activity for the Campus Community

A. Members of the Campus Community may use any available publicly accessible outdoor area of the college for expressive activity, without prior notification or approval of the college, during the hours when the college is generally open to the public.

B. Members of the Campus Community must not block the free passage of others or impede the regular operation of the college.

C. During business and class hours, or if the surrounding area is currently in use for a college sponsored event, use of amplification may be restricted.

D. Federal, state and local laws will be enforced.

E. Large Groups: Members of the Campus Community whose use of an outdoor area is expected or reasonably likely to have more than 20 persons in attendance shall obtain a permit from the Vice President of Student Affairs or designee at least three business days before the day of the activity. Permit forms may be obtained from the Vice President of Student Affairs or designee and must be filled out by a person who will be personally present. Permit forms will require that the applicant provide information as to the specific location requested to be used, the estimated number of persons expected to be present, and the name and contact information of at least one person who can be contacted regarding logistics of the event and will be personally present.

   Prior approval is to help ensure that there is sufficient space for the large group event, that the large group event does not conflict with any other college event or other use of the area, and that sufficient college resources are available for crowd control and security.

Expedited permit processing may be available where circumstances such as very recent or still-unfolding news developments that could not be reasonably anticipated exist and the permit may be issued with adequate planning.

The college may direct groups that exceed 20 persons to areas that do not interfere with college operations, public safety, the educational process, and unobstructed access to the college for its students, faculty, staff and visitors.

F. Reserved Space: In addition to the rights and limitations set forth above, any registered student or student organization may seek to reserve the use of specific outdoor areas designated for expressive activity. Such a request will be granted unless it would conflict or interfere with a previously scheduled event or activity or violate CCSNH or college policy. A registered student or student organization that has reserved a specific area under this policy will have priority over any others seeking to use the area during the scheduled period of time.

G. Members of the Campus Community who are employees of CCSNH shall comply with any and all workplace policies and regulations regarding speech, conduct, and professional ethics. This includes adhering to rules governing workplace communication, confidentiality, prohibitions on discrimination and harassment, and the use of government resources for personal or political purposes.

6 Expressive Activity for College Visitors

Members of the public who are not members of the Campus Community shall, before engaging in expressive activity on any CCSNH college campus, obtain a permit from the Vice President of Student Affairs or his/her designee of the relevant College at least three business days before the day of the activity. If extraordinary circumstances, such as very recent or still-unfolding developments that could not be reasonably anticipated by the applicant, exist, the College may waive the three business day requirement if it is also determined that the proposed activity may be conducted safely and in compliance with this policy despite the reduced time for notice and planning.

Permit forms may be obtained from the Vice President of Student Affairs or designee and must be filled out by a person who will be personally present.

Expressive activities shall occur only within publicly accessible outdoor areas designated by the College for use by college visitors for that purpose, and shall at no time block an entrance or exit to any building, or impeded free access to the buildings, sidewalks, walkways and parking lots or otherwise interfere with CCSNH or college business, the educational process, or public access to college grounds. Colleges may, but are not required to, pre-designate preferred spaces for general use by college visitors for expressive activities to facilitate visitors in choosing an appropriate location.

Permit forms will require that the applicant provide information as to the specific location requested to be used, the estimated number of persons expected to be present, and the name

and contact information of at least one person who can be contacted regarding logistics of the event and will be personally present.

Prior approval is required to assure the reasonable conduct of the educational process, unobstructed access to the college for its students, faculty, staff and visitors and to maintain public safety and protect college property. The College may request additional information or consultation with the requestor to determine whether campus or third-party services or security is warranted, which will be at the requestor's expense.

Generally, there is no limitation to the number of times a person or group may request access these areas. Access shall not be provided on blackout days and is otherwise limited to hours when the college is open to the public. During work and class hours, or if the area is currently in use for a college sponsored event, amplification will be restricted if it interferes, in any manner, with college operations.

The college may direct groups that exceed 20 persons to areas that do not interfere with college operations, public safety, the educational process, and unobstructed access to the college for its students, faculty, staff and visitors.

7 Appeal

If a person or organization is aggrieved by a decision of the Vice President or designee, an appeal may be taken to the President within three college business days of that decision. The appeal shall be in writing, stating the basis therefore, and the relief sought. The President shall promptly issue a written decision.

8 Generally Applicable Rules for Expressive Activities

In order to maintain a safe and secure environment for its students, faculty, staff and visitors conducive to providing quality education, the following rules apply to expressive activity on college grounds:

A. Expressive activity may occur only during normal operating hours as established by each College .

B. Signs, banners, placards, equipment and any other structures of any kind that are placed on college grounds shall not be affixed to or supported by any tree, post, building, fixture, or any other college structure. Due to the potential presence of underground utility, electrical and drainage lines, no signs, banners, placards, equipment or structures of any kind may be driven into the ground. No signs, banners, placards, equipment or other structures shall be left unattended, and any items left unattended may be removed by the College. All signs, banners, placards, equipment and any other structures shall be removed at the conclusion of the expressive activity and, in any event, no later than 8:00 p.m. on the day of the expressive activity.

C. Climbing, stepping, sitting, standing or leaning upon monuments, fences, lighting fixtures, trees, buildings, entrances or any other structure not intended for that purpose is strictly prohibited.

D. Vehicles are not allowed on college grounds except in areas designated for vehicular use.

E. Individuals distributing literature or any other item shall remove those items if discarded in or around the area of their activity at the conclusion of their activity. Distribution by placing any material on vehicles in the parking lots is prohibited.

F. All persons must comply with all CCSNH and college policies, campus rules and regulations, and local, state, and federal laws and regulations.

G. Nothing in this Policy shall be construed as limiting CCSNH's ability to maintain and enforce reasonable time, place, and manner restrictions on any expressive activity, including when issuing permits pursuant to this Policy.

H. Temporary Signage and Equipment

Signs and equipment are not allowed on campus property in connection with expressive activities except as specifically listed below:

i. On the day of a scheduled event, and when such event has been approved by the college pursuant to its policies, signs and equipment may be brought to the campus no more than one hour prior to the official start time of the event and must be removed from campus within one hour following the conclusion of the event.
ii. Signs must be sized so that they can be comfortably held by one person. Larger signs are prohibited.
iii. Equipment must be limited to what is necessary to engage in the expressive activity.
iv. Signs may not use the logo, seal, name or any other denotations for the college or CCSNH without written permission. Nothing in the text or graphics of any signs can state or imply endorsement by the college or any sanctioned group within the college (i.e., "Manchester Community College Students for Smith").
v. Signs and equipment that are placed on college grounds shall not be affixed to or supported by any tree, post, building, fixture, or any other college structure.
vi. Due to the potential presence of underground utility, electrical and drainage lines, no signs or equipment of any kind may be driven into the ground.
vii. All signs and equipment shall be removed at the conclusion of the expressive activity and, in any event, no later than 8:00 p.m. on the day of the expressive activity, unless otherwise agreed to by the college.
viii. Signs and equipment may not be hung or taped to any walls, railings, or furniture without prior approval of the college.
ix. The college may remove or require the event organizer to remove signs or equipment it considers disruptive, vulgar, or excessive in number.
x. Signs and equipment may not be carried, placed or used in any way that disrupts college operations, including with respect to access to the campus and any campus facilities, parking, roadway and walkways.

COMMUNITY COLLEGE
system of New Hampshire

9 Enforcement

CCSNH and its colleges reserve the right to stop any activity that substantially interferes with or disrupts normal business activities, interferes with the educational process, or violates this or any other CCSNH or college policy. Any person who violates this or any other CCSNH or college policy may be subject to an order to leave college property and may result in appropriate administrative and/or disciplinary action consistent with the rules and regulations governing students and/or employees of CCSNH and its Colleges, which may include dismissal or expulsion for students or discharge for employees.

562.02 CCSNH Alcohol Policy

Date Approved: 6/19/2012 *Date Effective: 6/19/2012*
Date of last Amendment: 11/5/2015 *Approved by: Ross Gittell, Chancellor*

1 Policy Statement

CCSNH and its colleges are committed to establishing and maintaining an environment that fosters mutually beneficial interpersonal relations and a shared responsibility for the welfare and safety of others. Accordingly, CCSNH and its Colleges recognize that in implementing an alcohol policy consideration must be given to the duty to promote a safe and secure, positive and productive environment.

2 Purpose

Because alcohol can have a significant effect on the academic, working and residential environment, CCSNH has adopted this policy for governing alcohol use by students, staff, faculty, visitors, and guests. While CCSNH policy permits responsible consumption of alcohol at some places and times, the consumption of alcohol should never be the primary purpose or focus of an event. Alcohol-free social events are encouraged.

3 Policy

A. Alcohol is not permitted on CCSNH property, including any of the colleges, academic centers, and leased facilities except as specifically allowed by CCSNH policy.

B. A request for approval to serve alcoholic beverages form must be submitted to the president of the college or chancellor of CCSNH for each function being planned where alcohol, beer or wine will be served. This form must be submitted 30 days prior to the event. All bar service must be provided by a holder of an appropriate New Hampshire Liquor License. The vendor must provide a certificate of insurance providing evidence of commercial general liability insurance, including liquor liability coverage, and workers compensation as required by law. This certificate of insurance must name CCSNH as an additional insured with respect to commercial general liability including liquor liability and evidence limits of liability as required by CCSNH. If requests are received with less than a 30-day notice, the president or the chancellor has the right to deny approval and service will not be granted.

C. The acquisition, distribution, possession, or consumption of alcohol by employees and other members of the CCSNH community must be in compliance with all local, state, and federal laws and CCSNH policy. Except as expressly permitted by the president or chancellor, employee consumption of alcohol while on duty is prohibited.

D. Non-alcoholic beverages must be provided at events where alcoholic beverages are served.

E. Restrictions on alcohol use on CCSNH property vary by location, and, in some cases, by time.

    a. Residence halls and apartment housing. Possession or consumption of alcohol by anyone under legal drinking age is prohibited. Residents of legal drinking age may consume alcohol in their rooms or apartments provided:

        i. A resident of legal drinking age may have just one open alcohol container at a time for personal consumption;

        ii. Alcohol may not be consumed in common areas such as lounges, hallways, etc.;

        iii. Excessive amounts of alcohol, including kegs, punch bowls, beer balls, or excessive amounts in bottles or cases, are strictly prohibited; and

        iv. Consumption of alcohol is done so in a responsible manner and the resident's conduct otherwise conforms to all rules and policies including the Student Code of Conduct;

    b. Dining halls and cafeterias. During periods when dining halls and cafeterias are not open to students and are assigned to workshops or conferences, alcohol may be served and consumed.

    c. Academic, administrative, classroom buildings or grounds. Consumption of alcohol is permitted only as part of an approved event, such as a fundraising event or a celebration of a special accomplishment. The chancellor or the president of the college sponsoring the event must give the required approvals.

F. CCSNH and its colleges have an interest in off-premises events held in their names. If alcohol is used illegally or inappropriately at such events, CCSNH or the college may take steps to protect its interests including, but not limited to, instituting disciplinary action against an employee or student.

G. Any request for variation from this policy including activities related to educational programs must be submitted to the president of the college or the chancellor.

H. Each college may adopt alcohol policies that are more restrictive than this CCSNH policy.

Date of last Amendment: 5/10/2022 *Approved by: Ross Gittell, Chancellor*

1 Policy Statement

CCSNH and its Colleges are committed to maintaining the safety and security of its faculty, staff, students and visitors and to maintaining an environment conducive to quality education, individual privacy, diversity, and freedom of expression. Accordingly, CCSNH and its Colleges recognize that in implementing a video surveillance system, consideration must be given to the duty to promote a safe and secure environment and an individual's right to privacy.

Video surveillance is used by CCSNH and its Colleges to promote a safe and secure college environment by:

A. Deterring acts of harassment, violence, vandalism and theft;

B. Aiding in the identification of individuals who commit such acts; and

C. Assisting in the investigation of any crime committed on college property.

2 Policy Purpose

This policy provides guidelines for the use of video surveillance on CCSNH and College property in a way that enhances safety and security, while at the same time respects the reasonable expectation of privacy held by its faculty, staff, students and visitors.

3 Scope of Policy

This policy applies to all faculty, staff, students and visitors on CCSNH and College property and governs the use of video technology controlled by CCSNH and its Colleges.

The following uses of video technology are not governed by the provisions of this policy:

A. Academic Use This policy does not apply to the legitimate academic use of video cameras for educational purposes.

B. Private Video Cameras This policy does not apply to private video cameras owned and operated by members of the campus community.

C. Law Enforcement Surveillance This policy does not apply to cameras used covertly by any law enforcement agency for criminal surveillance pursuant to proper legal authority.

D. Unrelated to Surveillance This policy does not apply to video cameras or webcams established for reasons unrelated to surveillance activity, including remote monitoring of facilities construction to ascertain project progress, campus public relations initiatives or videotaping of athletic or other events.

4 Notification of Video Surveillance and Policy

CCSNH and its colleges shall have signage posted at all campus entrances that indicate video surveillance is utilized on campus.

This policy will be made available to all students, faculty, staff and visitors by posting on CCSNH's and each College's website and printing in appropriate publications.

5 Camera Placement

In approving camera locations, CCSNH college management shall be guided by the following rules.

A. Public Areas Video surveillance shall be restricted to public areas. These may include, but are not limited to, the following areas:
   i. Streets, alleys, service drives, parking lots and loading docks
   ii. Athletic fields, gymnasiums and auditoriums
   iii. Dining facilities and other public gathering spaces
   iv. Building entrances, lobbies, foyers, hallways
   v. Classrooms, meeting rooms, programming rooms, laboratories, libraries
   vi. Cash handling areas and safes
   vii. Sidewalks and other pedestrian walkways

B. Private Areas Video surveillance is limited to those areas where individuals would not have a reasonable expectation of privacy. Accordingly, except when specifically authorized, such as through the use of a search warrant, video surveillance shall not be approved for use in or directed into any of the following places:

   i. Bathrooms, shower areas, locker and changing rooms
   ii. Private offices, except as noted below
   iii. Rooms used for medical, physical or mental health treatment including the entrances, exits, lobbies or hallways of on-campus health centers and counseling centers
   iv. Residence hall rooms

   Video surveillance may be approved for use in private offices for the limited purpose of safeguarding money, documents, pharmaceuticals or supplies. Cameras used for video surveillance of such work areas shall not be directed or zoomed to view computer screens.

C. Residential Housing Hallways and Lounges Video surveillance for safety and security purposes will not be directed into residential interior hallways and lounges, unless the College President or designee determines that a specific safety or security risk exists.

D. Placebo Cameras CCSNH and its Colleges will not utilize inoperative, perfunctory, placebo, or "for looks-only" video surveillance equipment.

6 Monitoring

The existence of video surveillance does not imply or guarantee that the cameras will be monitored continuously in real time or otherwise.

All CCSNH and college employees involved in monitoring video surveillance will perform their duties in accordance with the practices outlined in this policy. The following guidelines shall apply

to on-site and remote monitoring of video surveillance cameras at all CCSNH property, Colleges and academic centers:

A. Generally. Monitoring of video surveillance cameras shall be conducted in a manner that is professional, ethical, legal and consistent with all CCSNH and college policies, including, but not limited to, those governing sexual harassment and equal employment opportunity. Camera monitors shall monitor based on suspicious behavior, not individual characteristics. Monitoring individuals based upon a person's race, gender, gender identity or expression, sexual orientation, national origin, disability, or other protected characteristic is strictly prohibited.

B. Training All personnel involved in the supervision, application, use or monitoring of video surveillance technology at CCSNH and its Colleges will meet the following requirements:

   i. Be trained in the technical, legal and ethical parameters of appropriate video camera use; and

   ii. Receive a copy of this policy and provide a written acknowledgement that they have read and understood its contents.

C. Audio Recordings The video surveillance systems used by the CCSNH and its Colleges will record video only, no audio.

D. Evaluations of Employee Performance Video surveillance cameras will not be used by the CCSNH or its colleges to monitor or evaluate employee performance or to monitor employees during their non-working time. Video surveillance cameras may be used, however, to monitor a student or employee work area, such as an area with financial transactions, even if there is only one student, faculty or staff member in that area. Video surveillance cameras used to monitor a work area will not be used to view the contents of computer screens.

E. Data Collection Video surveillance cameras will not be used to collect data about behavior or groups of individuals using an area over a period of time such as parking patterns or types of use of study or recreational areas.

7 Storage

Video tapes or other media will be stored and transported in a manner that preserves security. Further, recorded images not related to or used for an investigation shall be kept confidential and destroyed on a regular basis. Accordingly, the following guidelines regarding the storage of video surveillance records shall be strictly adhered to:

A. Location Video surveillance records shall be stored in a secure location with access limited to authorized CCSNH and/or College personnel only.

B. Timeframe Generally, video surveillance records will be stored for a period of not less than 30 days, after which they will be promptly erased, unless retained as part of an internal investigation, criminal investigation, court proceedings (criminal or civil) or other bona fide use, as approved by CCSNH and/or College President or designee. Additionally, CCSNH

and/or College President or designee may determine that video surveillance records of identified high priority areas be stored for a period of not less than 90 days before being erased.

C. Alterations No attempt shall be made to alter any part of any surveillance recording. If CCSNH and/or College President or designee, or law enforcement officials, however, determine that it is necessary to release video surveillance records as set forth in section VIII, the faces and identifying features of all those on the video that are not of interest to the investigation shall be blurred prior to the release of such records.

Access Log An access log shall be maintained by CCNSH and/or each College of all instances of access to, or use of, surveillance records. This log shall include the date, time, and identification of the person or persons to whom access was granted, as well as a summary of the reason for which access was necessary.

8 Release of Information

Recorded information obtained through video monitoring will only be released when authorized by the Chancellor and/or the President of the College, according to procedures established in this policy. The following guidelines will govern dissemination of recordings obtained through use of the surveillance technology:

A. Law Enforcement Purposes Information obtained through video monitoring will be used for security and law enforcement purposes, and CCSNH or the College will cooperate and assist local law enforcement officials as requested with criminal investigations. This includes providing copies of video recordings within CCSNH's or the College's possession.

B. Commercial Use Under no circumstances shall the contents of any captured video recordings be exploited for purposes of profit or commercial publication, nor shall such recordings be publicly distributed except as required by law.

Release Pursuant to Valid Judicial Orders Video recordings will be released as required by subpoenas or other judicial process or orders after consultation with CCSNH's and/or the College's legal counsel.

9 Destruction or Tampering with Video Surveillance Technology

Any person who tampers with or destroys a video surveillance camera or any part of the video surveillance system will be subject to appropriate administrative and/or disciplinary action, as well as possible criminal charges.

10 Violation of This Policy

Violation of policy will result in appropriate administrative and/or disciplinary action consistent with the rules and regulations governing students and/or employees of CCSNH and its Colleges, which may include dismissal or expulsion for students or discharge for employees. Any information obtained in violation of this policy may not be used in a disciplinary proceeding against a member of CCSNH or its College faculty, staff, or student body.

COMMUNITY COLLEGE
system of New Hampshire

562.04 Records Management and Retention Policy

Date Approved: 8/19/2014 *Date Effective: 8/19/2014*
Date of last Amendment: 9/25/2023 *Approved by: Ross Gittell, Chancellor*

1 Policy Statement

CCSNH and its Colleges are committed to meeting their administrative needs, complying with applicable laws, and providing a source for historical research through systematic and consistent management of all records, regardless of medium or format, created and/or maintained by their employees in the course of their academic and administrative functions. Because CCSNH and its Colleges do not have a centralized records management office, the Community College System Office and each of the Colleges are responsible for the retention, disposal and transfer of records generated by their respective institutions.

The effective management of records will:

A. Meet legal standards for protection, storage, accessibility, and disposition;
B. Protect the privacy of students, faculty, and staff as required by law;
C. Ensure optimal and efficient usage of space and other resources;
D. Promote openness and transparency;
E. Contribute to documentation of CCSNH and its Colleges' historical records; and
F. Support effective governance and management of CCSNH and its Colleges.

2 Policy Purpose

The purpose of this policy is to:

A. To define certain terms relevant to records management and retention;
B. To establish accountability for records management and retention;
C. To strengthen safeguards against the inadvertent disclosure of confidential records;
D. To operate in conjunction with other CCSNH policies, programs, and best practices (by functional area) relating to the generation or maintenance of records, including, but not limited to, CCSNH's Information and Security Access Program (ISAP);
E. To establish the length of time certain categories are required to be maintained and stored;
F. To establish the time at which certain categories of records should be destroyed, absent exceptional circumstances;
G. To preserve physical and electronic storage space; and
H. To establish appropriate records destruction practices.

3 Scope of Policy

This policy applies to all CCSNH and College departments, offices and employees responsible for creation, receipt, maintenance, storage, use, destruction, or preservation of institutional records in any format.

Retention of information is based on the content of the information, not the medium. Records may be transferred from one storage medium to another, e.g. paper copy to a scanned image, as long as the integrity of the information remains intact. If the record is transferred to another storage medium, the original may be destroyed once the information is verified. This should be done not only to save time and space, but to ensure the appropriate copy is used when accessing the information.

4 Definitions

CCSNH – Consists of the Community College System of New Hampshire System Office and each of its constituent colleges.

CCSNH Active Record(s) – An original CCSNH Record currently used by the office, department or other area of CCSNH that generated it. Active Records remain active for varying numbers of years, depending on the purpose for which they were created and regulatory requirements. Active Records may be retained in the originating office or at an offsite storage company. Active Records include records in all formats, including but not limited to: paper, fiche, digitized or scanned documents, electronic documents, and all other formats.

Electronic Record - A record kept in a non-tangible electronic format. Electronic Records include but are not limited to: word processor documents, spreadsheets, databases, HTML documents, scanned or imaged documents, and any other type of file warehoused online, on a mainframe, on a computer hard drive, or on any external storage medium. The same retention standards that apply to tangible Records also apply to Electronic Records.

Duplicate Record – Is a copy of a CCSNH Record held by another department or office as necessary to fulfill that department's official function. Duplicate Records should not be retained longer than the CCSNH Record copy.

Personally Identifiable Information (PII) – Refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Records that contain personally identifiable information must be maintained or destroyed in accordance with CCSNH's Information Security and Access Program.

Records Owner – Is the office or department designated as having responsibility for management, retention, and timely destruction of particular types of CCSNH Records (example, the Registrar's Office may be the Records Owner of student transcripts).

Records Preservation/Hold Order – is an internal procedure to ensure that certain information is preserved which may be needed for reasonably anticipated or government investigation, audit, or litigation. A Records Preservation/Hold Order temporarily sets aside the retention period stated in the CCSNH Records Retention Schedule and suspends destruction for the affected records until the Records Preservation/Hold Order is released.

Records Retention Schedule – identifies what records are being managed and how long the records need to be retained based on CCSNH's operational, legal/compliance, financial and historical requirements.

COMMUNITY COLLEGE
system of New Hampshire

5 Records Management Program Accountabilities

CCSNH departments and offices are responsible for creating, implementing and monitoring their department or office-specific records retention and disposition procedures.

CCSNH legal counsel is responsible for providing legal advice on recordkeeping requirements, for developing and maintaining a Records Retention Schedule and for issuing and monitoring a Records Preservation/Hold Order where there is reasonable anticipation of litigation, government investigation, or audit.

CCSNH Information Technology is responsible for identifying and providing appropriate storage and media, protective procedures and systems to protect records on electronic media in conjunction with the CCSNH Records Retention Schedule and Records Preservation/Hold Order. This includes purchasing, designing, modifying or redesigning information systems, business applications and communication systems so that records may be adequately created, maintained and destroyed as a routine part of CCSNH operations.

Third parties who manage CCSNH Records are responsible for compliance with CCSNH recordkeeping requirements and for making CCSNH Records available upon request by authorized personnel. CCSNH Records Owners are accountable for ensuring that third parties working on their behalf comply with all applicable recordkeeping requirements and standards.

6 Recordkeeping Responsibilities for Departments and Offices

In addition to the accountabilities described above, it shall be the responsibility of each department or office to ensure that the following are done:

A. Review the types of CCSNH Records in its possession and determine appropriate formats to ensure usability, integrity and accessibility for as long as the records are needed.
B. Adopt and implement written procedures specific to all records managed by the department or office.
C. Assign a department or office Records Officer.
D. Train and educate staff concerning this policy, the CCSNH Records Retention Schedule, and any departmental or office procedures for handling records.
E. Ensure that access to records and systems containing PII is restricted in accordance with CCSNH's ISAP.
F. CCSNH Records that have met their authorized retention period are destroyed in accordance with CCSNH Records Retention Schedule and ISAP.
G. Duplicate Records (including duplicate electronic records) are destroyed upon determining that such duplicate records are no longer necessary to fulfill the department or office's mission.

7 Good Records Management Practices

CCSNH employees must manage CCSNH Records in a reliable manner to ensure their authenticity

and usefulness. In order to do this, departments and offices have the responsibility to implement practices to ensure that their employees:

A. Create records that fully and accurately document their core activities.
B. Manage and store records in a manner that facilitates timely, accurate retrieval.
C. Ensure that records are stored in authorized, secure locations and in safe and stable environments.
D. Allow only those with proper authority to access records and information systems.
E. Know and comply with laws, regulations, standards and professional ethics that bear on the management of their records.
F. Destroy records that have met their authorized retention period and are not subject to a Records Preservation/Hold Order in a manner that provides an appropriate level of protection of the information contained in the records.

562.05 Firearms and Weapons on Campus Policy

Date Approved: 12/15/2015 *Date Effective: 12/15/2015*
Date of last Amendment: N/A *Approved by: Ross Gittell, Chancellor*

1 Policy Statement

In order to promote the safety and security of students, faculty, staff and visitors, the Community College System of New Hampshire (CCSNH) prohibits the use and possession of firearms, weapons and explosives on property owned or controlled by CCSNH, including its colleges and academic centers.

2 Policy Purpose

CCSNH, its colleges and academic centers are committed to providing a safe and secure educational and work environment for students, faculty, staff and visitors.

3 Policy

A. As used in this policy, the terms "firearms, weapons and explosive materials" include, but are not limited to, shotguns, rifles, pistols, BB guns, dart guns, paint guns, starter pistols, blow guns, crossbows, bows and arrows, swords, stilettos, knives over three inches in length, hatchets, martial arts weapons, nun-chucks, throwing stars and any chemical compound, mixture, or device, the primary or common purpose of which is to function by explosion.

B. The use and possession of firearms, weapons and explosive materials, even if legally possessed, are prohibited while in the buildings or on the grounds of CCSNH, its colleges and academic centers or while occupying any vehicle owned by the Community College System of New Hampshire whether on or off campus. A CCSNH college president may, but is not required to, permit persons authorized by law to possess firearms, crossbows, and bows and arrows to store unloaded firearms, crossbows, and bows and arrows in their parked vehicles so long as they are adequately secured, i.e., in a locked vehicle and/or locked case.

C. Because the use of a starter pistol or prop firearms, weapons or explosive devices for theatrical performances or activities on campus can present a potential danger, any person, class, club or other organization that plans to use or possess a starter pistol, prop, replica, training or toy weapon or explosive device of any type on any campus must obtain prior approval by the designated campus safety officer.

D. Active law enforcement officers duly authorized to carry firearms and other weapons are exempt from this policy.

E. The chancellor or president of a college may grant permission in writing to an individual, academic or operational department or other organization to possess firearms, weapons or explosive materials on campus for instructional or other qualified purposes and in other special circumstances and conditions as deemed appropriate.

F. Any person violating this policy will be subject to appropriate disciplinary, legal and/or administrative action, provisions of state and federal laws and may be subject to sanctions including but not limited to removal from CCSNH, its Colleges and Academic Centers.

562.06 Information Security Policy

Date Approved: 2/6/2018 *Date Effective: 2/6/2018*
Date of last Amendment: N/A *Approved by: Ross Gittell, Chancellor*

1 Policy Statement

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.

2 Policy Purpose

The purpose of this policy is to:

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

COMMUNITY COLLEGE
system of New Hampshire

3 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.

4 Definitions

A. Authentication: Process of identifying an individual based on username and password.
B. Availability: The ability of a user to access information or resources in a specified location and in the correct format.
C. CCSNH Chief Information Officer: The individual at CCSNH who is responsible for the information technology and computer systems that support enterprise goals.
D. 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.
E. 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.
F. 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.
G. Encryption: Encryption is the conversion of electronic data into another format, which cannot be easily understood by anyone except authorized parties.
H. Firewall: A network appliance that controls incoming and outgoing network traffic based on a configured set of rules.
I. 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.

J. 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.

K. 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.

L. 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.

M. 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.

N. 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.

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

5 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 ensuring 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.

6 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 consequences of loss, legal or retention requirements, sensitivity, and value of the information. In classifying data, the characteristics 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:

        i. Directory information;
        ii. Financial accounting reports and budgets;
        iii. Contracts;
        iv. Admissions metrics and statistics;
        v. Donor contact information;
        vi. 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:

   i. Admissions records;
   ii. Student records other than directory information;
   iii. Personnel records;
   iv. Internal personnel practices;
   v. Confidential commercial, or financial information from any source or third-party information subject to a nondisclosure agreement with CCSNH or the Colleges;
   vi. Library user information;
   vii. Campus security investigations, emergency, measures and surveillance information;
   viii. Test questions, scoring and other examination information;
   ix. Equity complaints and investigations;
   x. Collective bargaining negotiations;
   xi. Information subject to attorney-client privilege;
   xii. 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:

   i. Social security numbers;
   ii. Health information;
   iii. 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;

iv. Personal financial information, including checking or investment account numbers;
v. Driver's license or non-driver identification numbers;
vi. 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.

7 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 ensure 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 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.

8 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 visible only to the authorized user of the computer and should use a screen saver with a screen saver password to ensure that information is not displayed after a specified period of time.

9 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.

1. evaluate and document the sensitivity of the information to be shared
2. identify the responsibilities of each party for protecting the information
3. provide a signoff procedure for each party to accept these responsibilities
4. define the minimum controls required to transmit and use the information
5. record the measures that each party has in place to protect the information
6. define a method for compliance measurement
7. establish a procedure and schedule for reviewing the controls
8. 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.

1. separate operational responsibility for networks and computer systems
2. establish responsibilities and procedures for remote use (See Access Control)
3. 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:

1. If a user can make an unauthorized change to an application
2. If a user can access an application and cause it to perform unauthorized tasks
3. If an unauthorized individual can access an application and destroy/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:

1. 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.
2. Protection against malicious software on portable computing resources must be implemented and maintained at current levels.
3. 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.
4. When in use, portable computing resources on which Restricted Information is stored must not be left unattended.
5. When not in use, portable computing resources on which Restricted Information must be physically secured.
6. 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.

7. 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 if 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.

1. Care should be taken to prevent conversations involving confidential matters from being overheard
2. Avoid the use of mobile phones when discussing Restricted Information
3. Avoid leaving messages involving confidential matters on voicemail systems
4. Contact the recipient to ensure protection of a fax and verify the destination fax phone number when sending Restricted Information
5. Avoid using third-party, Internet or wireless fax services to send or receive Restricted Information
6. Care should be taken in sending teleconference access numbers if Restricted Information will be discussed during the teleconference
7. 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 its 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.

1. Wireless network access points must not be installed without CIO approval.
2. 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.
3. 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 content of such pages is not reviewed prior to posting, the content 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 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.

10 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:

1. Software and tools for development must be maintained in development environments isolated from production environments.
2. When not required, access to compilers, editors and other system utilities must be removed from production environments.
3. Login procedures and environmental identification must be sufficiently unique between development, test and production environments.
4. 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 its 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 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.

11 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.

1. Creating user accounts
2. Granting user account privileges
3. Removing user account privileges
4. Periodic reviewing of user accounts
5. Periodic reviewing of user account privileges
6. Assigning of new authentication tokens (password reset processing)
7. 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:

1. Passwords must not be stored in clear text
2. Passwords should not be subject to disclosure through dictionary attack or easily guessed
3. Passwords must be confidential and not shared with any other person
4. Passwords should be changed at regular intervals
5. Temporary passwords should be changed at the time of first logon
6. Passwords should contain a mix of alphabetic, numeric, special and upper/lower case characters
7. 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:

1. Usernames
2. Dates and times for logon and logoff
3. Workstation identity (location)
4. Record of rejected attempts to access applications
5. Record of rejected attempts to access data

12 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.

1. Development of a data profile to understand the risks
2. Identification of security measures based on data protection requirements
3. Implementation of security controls based on the identified security measures and the technical architecture of the system
4. Implementation of a process for testing the effectiveness of the security controls
5. 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.

13 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 its 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 its 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.

562.07 Information Technology Acceptable Use Policy

Date Approved: 2/6/2018 *Date Effective: 2/6/2018*
Date of last Amendment: 5/23/2025 *Approved by: Mark Rubinstein, Chancellor*

1 Policy Statement

Information technology resources are used by individual employees, students, and other persons affiliated with the Community College System of New Hampshire (CCSNH) and its Colleges. These resources are to be used for educational and business purposes in serving the interests of CCSNH and its Colleges. Misuse of information technology resources poses legal, privacy and security risks and therefore it is important for all users to understand the appropriate and acceptable use of such resources. Effective security and protection is a team effort. It is the responsibility of every user to know this policy, the standards contained herein, and to conduct their activities accordingly.

2 Policy Purpose

This policy establishes the proper use of CCSNH information technology resources and makes IT Users aware of what CCSNH deems as acceptable and unacceptable use.

3 Scope of Policy

This policy applies to employees, students and any other person who has access to CCSNH information technology resources including computers, email, Internet, social media, the network and any other CCSNH information technology or storage system (collectively "IT Users"). All IT

Users are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with CCSNH policy and standards.

4 Privacy

CCSNH reserves the right to monitor, duplicate, record, and/or log all use of CCSNH technology resources with or without notice. This includes, but is not limited to, email, Internet access, file access, logins, and/or changes to access levels. IT Users shall have no expectation of privacy in the use of CCSNH technology resources.

5 General Use, Access and Ownership

A. CCSNH Information Assets stored on electronic and computing devices, whether owned or leased by CCSNH, employees, students, or a third-party, remain the property of CCSNH. Computer and telecommunication equipment, software, operating systems, storage media, Intranet, network accounts providing electronic mail, Internet access and browsing, and related network systems, are the property of CCSNH. These systems are to be used for educational and business purposes serving the interests of CCSNH and its Colleges.

B. Access to CCSNH technology resources is a privilege not a right. CCSNH technology resources include, but are not limited to, computers, equipment, email, Wi-Fi, Internet access and browsing, Intranet, social media, telecommunications and network services, video network services, web services, software, applications, printing and scanning services, and user and technical support provided by Information Technology Staff. Accepting access to any CCSNH technology resource carries an associated expectation of responsible and acceptable use. Failure to meet the standards set forth herein constitutes a violation of this policy and may result in disciplinary action up to and including termination or denial of access, termination of employment or, for students, dismissal from the College.

C. IT Users may access, use and share CCSNH Information Assets only to the extent and for such purposes that access is authorized. This policy expressly prohibits accessing or attempting to obtain unauthorized access, supplying false or misleading information to access, and circumventing user authentication or security of any host, network or account. IT Users are prohibited from accessing data not intended for the IT User, logging into a server or account without express authorization, and probing the security of systems or networks without express authorization.

D. An IT User's access to technology is not transferable. Access privileges may not be shared with any other person including, but not limited to, devices, passwords and MFA device tokens

E. IT Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of CCSNH Information Assets.

F. As general practice, local administrative rights on CCSNH provided devices is prohibited

G. CCSNH provided devices are to be used primarily for business purposes. Limited personal use should be approached with caution to minimize potential impact to institutional resources and systems

H. Personal devices can be used to access some CCSNH services such as email or OneDrive, and Teams. Use of personal devices to access any CCSNH provided resources or services should be approached with caution to ensure the protection of CCSNH data and resources. To safeguard sensitive information, no CCSNH data should be downloaded or stored on personal devices.
I. Only CCSNH devices can obtain access via the administrative network, which include systems such as Banner.
J. CCSNH provides a VPN client for secured access from CCSNH provided devices to internal systems. This client can only be installed on CCSNH provided devices and should never be installed on a personal device.
K. Access to CCSNH services by faculty and staff is only permitted from within the United States, no international access of CCSNH systems is permitted.
L. CCSNH reserves the right to immediately and without prior notice, disconnect any system or terminate any user access to protect the security of CCSNH technology resources, CCSNH Information Assets, and CCSNH IT users.

6 Password Security and Protection

A. Passwords and MFA (Multi Factor Authentication) are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the network. CCSNH has established the following standards for password security and protection.
B. Multi Factor Authentication is a requirement for accessing CCSNH resources and all accounts, faculty, students and staff, are defined with MFA as a requirement, acceptable means for obtaining an MFA code include
    i. The OKTA authentication mobile application
    ii. SMS text
    iii. And under limited circumstances, a key fob (which can be acquired from the local IT staff)
C. IT Users must create passwords that:
    1. Contain a minimum of 14 characters and a maximum of 64 characters. Passwords may contain or be any combination of the following:
        i. Both upper and lower case letters.
        ii. Contain numbers (for example, 0-9).
        iii. Contain special characters (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).
D. IT Users should not create passwords that:
    1. Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
    2. Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
    3. Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
    4. Contain patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

5. Contain common words spelled backward or preceded or followed by a number (for example, terces, secret1 or 1secret).
6. Are some version of “Welcome123” “Password123” “Changeme123”

E. IT Users should not write passwords down or store them anywhere in their office or in a file on a computer system or mobile devices (phone, tablet) without encryption. Instead, IT Users should create passwords that can be remembered easily. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

F. All system-level passwords (for example: root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

G. All user-level passwords (for example: email, web, desktop computer, and so on) must be changed at least once a year.

H. Passwords must not be shared with anyone, including administrative assistants, secretaries, managers, co-workers, and family members, other students. All passwords are to be treated as sensitive, confidential CCSNH information.

I. Passwords must not be inserted into email messages or other forms of electronic communication or saved using the "Remember Password" feature of applications (for example, Internet browsers).

J. Any IT User suspecting that his/her password may have been compromised must report the incident and change all passwords.

K. Patching on CCSNH provided devices accessing central systems will be performed automatically monthly at minimum. IT Users need to allow patch application and perform any necessary reboots.

7 Unacceptable Use

A. System and Network Activities

The following activities are strictly prohibited:

1. Connecting computers or other devices directly to the CCSNH network that have not been registered with or approved by CCSNH.
2. Installing software or hardware on or modifying the software or hardware configuration of a CCSNH-owned IT asset without appropriate authorization from CCSNH Chief Information Officer.
3. Utilizing a CCSNH provided device to access or create TikTok(s).
4. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by CCSNH.
5. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CCSNH or the end user does not have an active license is strictly prohibited.

6. Violation of federal, state or local laws and regulations regarding access and use of information resources (e.g., Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, Computer Fraud and Abuse Act, code of professional conduct, etc.).
7. Except for internet browsing, accessing data, a server or account for any purpose other than CCSNH educational or business purposes, even if access is otherwise authorized, is prohibited.
8. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate CCSNH official should be consulted prior to export of any material that is in question.
9. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
10. Using a CCSNH technology resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws and policies.
11. Effecting a security breach or disruption of network communication. Security breaches include, but are not limited to, accessing data that the IT User is not an intended recipient of or logging into a server or account that the IT User is not expressly authorized to access. For purposes of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
12. Using any kind of program, script, or command designed to interfere with a user's computer or network session or collect, use or distribute another user's personal information.
13. Port scanning, security scanning and executing any form of network monitoring that will intercept data not intended for IT User's host.
14. Circumventing user authentication or security of any host, network or account.
15. Introducing honeypots, honeynets, or similar technology on the CCSNH network.
16. Interfering with or denying service to any user other than the IT User's host (for example, denial of service attack).
17. Providing information about, or lists of, CCSNH employees or students except as expressly authorized.

B. Email and Communication Activities

CCSNH faculty and staff must use their assigned CCSNH email address for all email communication to students and other official business of CCSNH and its Colleges. CCSNH faculty and staff shall not forward CCSNH email to personal email addresses.

When using CCSNH technology resources to access and use the Internet, users must realize that their communications may be viewed as representing CCSNH unless they clearly indicate otherwise.

The following activities are strictly prohibited:

1. Sending unsolicited email messages including sending "junk mail," chain letters, Ponzi or other pyramid schemes of any type, or other inappropriate use of email distribution lists.

2. Any form of harassment via email, telephone or texting, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Unauthorized use of CCSNH and its Colleges registered internet domain names.
5. Solicitation of email for any other email address, other than that of the sender's account with the intent to harass or to collect replies.

C. Blogging and Social Media

1. CCSNH employees who engage in blogging or use social media, whether using CCSNH technology resources or personal computer systems, should at all times be accurate, exercise appropriate restraint, show respect for the opinion of others, and make every effort to indicate when the CCSNH employee is and is not an institutional spokesperson.
2. When an employee is expressing beliefs and/or opinions in blogs or social media, the employee may not, expressly or implicitly, represent themselves as a representative of CCSNH or its Colleges.
3. The name, seal, images and other insignia of CCSNH or any of its Colleges shall not be used without the express written permission of CCSNH.
4. CCSNH hosted web pages and blogs are not to be used for activities unrelated to the business purposes or educational mission of CCSNH or its Colleges without prior written authorization.
5. CCSNH IT Users are prohibited from revealing any CCSNH confidential or proprietary information, trade secrets or any other Restricted Internal, Confidential or Private Information when engaged in blogging or use of social media.

562.08 CCSNH Campus Safety and Security

Date Approved: 7/1/2017 *Date Effective: 7/1/2017*
Date of last Amendment: N/A *Approved by: Ross Gittell, Chancellor*

1 Policy Statement

CCSNH and its Colleges are committed to establishing and maintaining a safe and secure environment for its faculty, staff, students and visitors conducive to providing quality education while protecting individual privacy, diversity, and freedom of expression. Accordingly, CCSNH and its Colleges recognize that in implementing a campus safety and security program, consideration must be given to the duty to promote a safe and secure educational and work environment while providing an open and accessible campus ready to serve the educational needs of a diverse population.

Policy Purpose

The characteristics of the faculty, staff, student body, the physical plant, grounds and layout of the seven community college main campuses, academic centers and additional locations vary widely. The purpose of this policy is to provide a framework for CCSNH and each of its component colleges to develop internal and external security measures, and rapid and comprehensive emergency response plans taking into account a variety of factors including the demographics

and size of the student body, faculty and staff, the nature of the educational programs, the physical characteristics and layout of the facilities, and applicable local, state and federal laws.

2 Policy

Safety and Security Program

To promote a safe and secure educational and work environment, CCSNH and each of its Colleges shall establish and maintain a campus safety and security program for each campus and additional location. The campus safety and security program shall at a minimum include a security assessment and emergency operation plan. In establishing a campus safety and security program, security measures should be considered that 1) maintain and promote a safe environment that is open, transparent and supports delivery of a quality education 2) are effective, and 3) may reasonably be implemented within budgetary and resource limitations.

1. Facilities Security Assessment

The Safety and Security Program shall include an assessment of physical security as provided through three core standards identified as surveillance, access control and emergency alerting.

A. Surveillance

Surveillance is a core capability that increases the ability to view surroundings both internal and external and a valuable security tool when used to observe danger and potential threats, deter dangerous behavior, assist in collecting evidence and to locate victims and perpetrators. Surveillance cameras that are visible to the public mitigate the perception of anonymity and increase transparency in and around the campus facilities. Key leadership and certain administrative personnel should engage in and have access and exposure to surveillance monitoring as needed for security purposes. Surveillance monitoring should be located in areas of the campus that allow access by authorized personnel during emergencies.

B. Access Control

Access control, by actively engaging and/or controlling the flow of people into the campus facility, is another core capability that protects against unauthorized persons gaining access to facilities, instills expectations of behavior and sets boundaries. In addition to electronic or other physical barriers, access control may involve some level of interaction with staff to make determinations about entry or denial. Consideration should be given to layering access control throughout the facility to act as an obstacle to threat progression and establishing a credentialing identification system for faculty, staff, students and visitors.

C. Emergency Alerting

Emergency alerting is the third core capability that provides leadership with the ability to communicate effectively and rapidly with students, faculty, staff and visitors during an emergency. Being able to address the entire campus population when announcing response actions or coordinating rescue procedures is vital during emergencies.

Establishing primary and subordinate locations within the facility to promote effective use of emergency alerting in a variety of circumstances should be considered. The system must include redundant capabilities to make emergency calls for help to off-site emergency organizations and communicating to the public official information about emergency conditions.

2. Personnel
   A. Roles and Responsibilities

In developing a campus safety and security program, CCSNH and each College will establish roles and responsibilities of key administrators, faculty and staff members related to campus safety and security including prevention, preparedness, emergency response and after action. At a minimum, roles and responsibilities must be established for the following:

Administration

1. Developing campus security programs including conducting campus security assessments and determining allocation of resources
2. Developing and coordinating safety programs to promote compliance with applicable safety and health standards and regulations
3. Preparing and implementing campus security plans and procedures emergency operation plan
4. Establishing internal communications system to facilitate general and emergency communications between maintenance, security and leadership
5. Establishing and activating campus emergency notification systems
6. Reporting of concerning behavior and suspicious activity
7. Conducting of internal investigations of incidents to determine effective methods to reduce or eliminate hazards
8. Tracking incidents, preparing daily logs, reports and other documentation
9. Establishing training programs for students, faculty and/or staff regarding safety and security standards, policies, procedures and protocols
10. Adopting memoranda of understanding with local emergency service providers and law enforcement to establish communication and coordination in matters that may pose a threat to campus safety and security including information sharing and event reporting

Monitoring, Testing and Inspections

1. Conducting campus patrols of campus facilities including all buildings, grounds, parking lots, doors and entrances for fire, thefts, lighting, damage and other safety hazards
2. Monitoring video surveillance and entrances and answering incoming calls and direct response accordingly
3. Managing identification and key and card access systems

4. Inspecting life-safety equipment such as, fire extinguishers, AEDs, emergency lights and parking lot lighting
5. Testing alarms (fire, intrusion systems) and equipment (emergency phones, video monitoring) to ensure all equipment is working properly

B. Training

In developing a campus safety and security program, CCSNH and each College will provide training for faculty, staff and students as appropriate related to campus safety and security including prevention, preparedness and emergency response. Such training may cover the following topics:

1. Role and responsibility of personnel with campus security duties
2. Relevant state and federal laws including FERPA, Clery and Violence Against Women Act
3. Security awareness in the higher educational environment
4. Conflict resolution and management of aggressive behavior
5. Incident management
6. Disaster and emergency response
7. Behavior health
8. Drug identification and effects
9. Blood borne pathogens and hazardous materials
10. First aid, CPR, AED utilization
11. Defensive driving
12. Investigation and interviewing techniques and procedures

3. Emergency Operation Plan

In developing a campus safety and security program, CCSNH and each College will develop a site-specific emergency response plan which is based on and conforms to the Incident Command System (ICS)[1] and the National Incident Management System (NIMS)[2]. The plan should address hazards including but not limited to acts of violence, threats, earthquakes, floods, tornadoes, structural fire, wildfire, internal and external hazardous materials releases, medical emergencies, and any other hazard deemed necessary by CCSNH and College officials and local emergency authorities. The plan should be coordinated with state and local emergency authorities and with the emergency operations plan in the municipality in which the campus or academic center is

---

[1] *The Incident Command System (ICS) is a management system designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. ICS is normally structured to facilitate activities in five major functional areas: command, operations, planning, logistics, intelligence and investigations, finance and administration. It is a fundamental form of management, with the purpose of enabling incident managers to identify the key concerns associated with the incident—often under urgent conditions—without sacrificing attention to any component of the command system.*

[2] *The National Incident Management System (NIMS) is a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work together seamlessly and manage incidents involving all threats and hazards—regardless of cause, size, location, or complexity—in order to reduce loss of life, property and harm to the environment. The purpose of the NIMS is to provide a common approach for managing incidents and provide for a flexible but standardized set of incident management practices with emphasis on common principles, a consistent approach to operational structures and supporting mechanisms, and an integrated approach to resource management. By using NIMS, communities are part of a comprehensive national approach that improves the effectiveness of emergency management and response personnel across the full spectrum of potential threats and hazards (including natural hazards, terrorist activities, and other human-caused disasters) regardless of size or complexity.*

located. Each College shall review its plan at least annually, and shall update the plan, as necessary. Each plan shall address all the three phases of all critical incidents.

A. Prevention and Preparedness – Prevention decreases the need for response by taking appropriate steps to mitigate vulnerabilities, while preparedness builds and maintains the capability to conduct a rapid, coordinated, effective response during a critical incident.

B. Coordinated Response – A proper response will follow emergency management plans and use the skills learned through training. Each College together with state and local emergency authorities must use the plans designed during prevention and preparedness phase to effectively provide a coordinated response.

C. After Action – Following a critical incident, the affected campus must focus on resuming teaching and learning as quickly as possible. The plans must provide for management of recovery and reviewing response actions.