CSN Policy	Information Systems & Electronic Resources Acceptable Use Policy
Policy Category: General	**Effective Date: 7/5/2017**

MOST RECENT CHANGES

1. Section II.D.
Clarification providing for monitoring.
2. Section II.F.
Clarification of what would cause someone to unduly consume resources.
3. Section II.G.
Reworded and reorganized Point 2. and 3. were simplified to identify that OTS has responsibility for password policies. OTS responsibility for password guidelines added.
4. Section II.H.
Clarification provided for monitoring.
5. Section II.M.
Wording clarified to express what communication vehicles serve as CSN's official mode of communication.
6. Section II.M.
The policy regarding automatic forwarding of e-mail was moved from Section O, II, a.
7. Section II.M.
Clarification of the Netiquette portion of the policy.
8. Section II.N.
Clarification provided to example examples of when CSN may extract data from the logs.
9. Section II.O.1.
Wording added to identify network and shared departmental file storage account holders.
10. Section II.O.2.a.
Wording changed because of an onsite server based archival system to a cloud-based backup system.
11. Section II.O.2.b.
Clarification of records storage. "H" drive storage for faculty and staff is increased from two gigabytes to ten. Change to "H" drive back-up storage policy from five years to two years.
12. Section II.O.2.c.
Reworded to address employees separating from active employment. Clarification added that employees cannot access network resources upon separation. Storage policy for the e-mails of separated employees to meet the requirements of the NSHE Schedule.

I. POLICY PURPOSE

This policy governs the use of information technology systems and electronic resources at CSN.

II. POLICY STATEMENT

A. This policy shall be applicable to all CSN students, staff, faculty and contractors/vendors (defined hereafter as 'users') who have access to or who are responsible for an account or any form of access that supports or requires a password on any system that uses the school's Active Directory for authentication, authorization and auditing and that resides at any CSN facility, who have access to the CSN network, who stores electronically any non-public CSN information elsewhere, or who uses a CSN-owned laptop computer.

B. Information technology systems and electronic resources are provided to the members of the CSN community with the understanding that they will use them with mutual respect, cooperation and collaboration, and in compliance with all applicable policies, laws and regulations.

C. These resources are finite but their usage is growing and expanding; the resources must be

shared generally and as with any interconnection of electronic resources; one individual can have a dramatic effect on others within the network. Therefore, the use of the CSN network and electronic resources is a revocable privilege.

D. All constituents will benefit if all users of the CSN electronic systems avoid any activities that cause problems for other users. CSN reserves the rights to monitor, limit, and restrict electronic messages, network/systems traffic, and the public or private information stored on computers owned, maintained, or managed by CSN. Anyone who uses computers not owned, maintained, or managed by CSN that abuse campus services may also be denied access to campus resources. Email/voice mail, web pages, and digital content are subject to archiving, monitoring (in the case of wrongdoing or computer misconduct as determined by CSN), or review, and/or disclosure by other than the intended recipient as provided in NSHE Board of Regents' Handbook, Title 4, Chapter 1, Section 22, "Privacy Issues".

E. CSN requires access to its information technology systems and electronic resources (hereinafter "Systems") to be authorized and pre-approved, and that users understand that laws currently exist that prohibit the following:

1. Electronic libeling or defamation
2. Sending/Posting/Broadcasting messages that incite hate or violence
3. Transmitting repeated unwanted personal advances
4. Falsifying information or impersonation
5. Unauthorized use of, providing, or copying of protected intellectual or copyrighted property

F. CSN's network is a private network separate and distinct from the public Internet. Therefore, access to and use of CSN's network must comply with all CSN's policies, rules and regulations and with all local, state, and federal laws. Examples of prohibited activities outside of prescribed course related activities include but are not limited to:
1. Posting or transmission of confidential information
2. Use of offensive or discriminatory language
3. Transmission or display of graphic images, sounds or text that is sexual or offensive in nature
4. Unauthorized use of other's passwords or accounts
5. Use of the Systems for personal profit or gain
6. Use of the Systems to harass, threaten, or otherwise invade the privacy of others
7. The installation or use of any servers on the network not expressly approved by the Office of Technology Services (hereafter "OTS")
8. Deliberate attempts to cause breaches of the network, servers, telecommunications systems or security or to examine network traffic
9. Initiation of activities which unduly consume computing or network resources such as downloading of files or steaming media for personal use that disproportionally burdens network or server resources.
10. Use of applications, for example P2P, to receive and/or distribute copyrighted materials, such as movies, music, and video
11. Tampering with computer files, software, or knowingly introducing a virus or malicious code to the to the CSN systems
12. Unauthorized changes to the CSN web pages
13. Playing games in CSN computer labs for entertainment
14. Excessive use of network bandwidth, storage, and any computer resources for purposes unrelated to CSN activities

G. Passwords are an important tool for network security. To protect the CSN network all passwords connected with a CSN account are subject to the following:
1. Password Protection: A password authenticates the holder as an authorized user of CSN's computer system that uses the school's Active Directory for authentication, authorization and auditing and must be protected from disclosure to others.
    a. Each user is responsible for the security of their password(s).
    b. A password must not to be shared with others or posted in a location where others may see it and may only be used by the person for whom the password was

created.
   c. User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
   d. Group passwords are allowed only in the case of the highest level administrator passwords for servers.
   e. Passwords must not be inserted into email messages or other forms of electronic communication.
   f. Pre-validated Active Directory accounts that are not validated and activated within three calendar days will be disabled.
2. Password construction and changes: OTS will monitor password requirements to ensure they are state of the art for protecting the CSN network. OTS will notify system users of new requirements for passwords. These guidelines will be updated and displayed on https://www.csn.edu/passwordreset.

H. Users must understand that email is not absolutely private and should practice caution in sending messages that a user would not want everyone to see. OTS does not make a practice of monitoring email and other files. When there is a reasonable suspicion of wrongdoing or computer misconduct (for example, harassing a coworker or visiting a website that CSN deems inappropriate, such as security-related sites, adult content sites, sites promoting violence, etc.), CSN reserves the right to examine material stored on or transmitted through its Systems in accordance with NSHE Board of Regents' Handbook, Title 4, Chapter 1, Section 22.

I. CSN and users of its Systems must comply with the copyright protection given by international agreements and federal law to owners of software and intellectual property under the United States copyright laws, including but not limited to the Copyright Act of 1976 and the Federal Digital Millennium Copyright Act of 1998, and including the restrictions that apply to the reproduction of software and intellectual property. Users of the Systems must ensure that the bounds of permissible copying under the fair use doctrine are not exceeded (i.e., a backup copy may be made). It is against the law to copy or reproduce any licensed software or intellectual property, or to download from the Internet any copyrighted material, including fonts, music, movies, and videos without permission of the copyright holder and any illegal activity will be dealt with as outlined below as well as expose the user to criminal charges. No one may use software that has been obtained illegally on the CSN Systems or on personal equipment used at CSN. Violation of these requirements will subject the offender to disciplinary action at CSN as outlined below, as well as expose the user to accountability in a court of law.

J. While computer equipment and access to the Systems is provided for CSN work and education purposes, incidental personal use is permitted as long as it is not inconsistent with this Policy and it doesn't interfere with employment and education responsibilities.

K. Eating and drinking is not permitted in the immediate area of any computer in open labs and classrooms.

L. Violations
1. Any suspicion of a password being compromised on a system that uses CSN's Active Directory for authentication, authorization and auditing must be reported to OTS.Active Directory accounts suspected of being compromised or misused will be disabled by OTS. OTS will disable Active Directory accounts promptly at notice of termination by HR or the employee's department.
2. CSN may also impose restrictions pertaining to computer use, including a loss of computing privileges on a temporary or permanent basis, a decrease of disk quota, and the removal of files in the System's temporary or scratch area.
3. In addition to liability and penalties that may be imposed under federal, state or local laws, users of the Systems who fail to fulfill their responsibilities and engage in prohibited conduct may be subject to disciplinary action. CSN may restrict or suspend user privileges while the alleged violation(s) are being investigated and disciplinary action pursued. Disciplinary action shall be taken by the Vice President of Student Affairs relative to student violations, and by the appropriate CSN officer relative to faculty, staff,

and/or CSN affiliate violations. A violation may also result in a referral to law enforcement authorities.

4. In accordance with CSN and NSHE policies and state and federal laws, OTS may monitor the CSN Network for activity that violates this Acceptable Use Policy.

M. E-mail Acceptable Use Policy

In promoting communication and distance learning initiatives, CSN has established a student, faculty and staff email system, a learning management system, along with other communication tools. These systems serve as CSN's official modes of communication. All communication directly linked to the purposes and mission of CSN will be conducted using the tools provided by CSN. This includes information communicated by students, faculty, staff and CSN's administrative offices.

CSN email users will not be permitted to set up automatic forwarding options on CSN email accounts to forward CSN emails to other personal email systems such as Gmail, Yahoo, Outlook.com, etc.

Acceptable Use -*The* use of student email accounts, must be in support of educational and academic activities or research and consistent with the educational objectives of the CSN. Transmission of any material in violation of any United States, Nevada, or other pertinent jurisdiction's law, regulation, or rule, or any Nevada System of Higher Education Board of Regents policy or CSN policy, is prohibited.
This includes, but is not limited to, threatening or obscene material or material protected by trade secret. Illegal acts are strictly prohibited. Using Intranet accounts to play games is not acceptable use.

Privileges -The use of CSN's Intranet is a privilege, not a right, and inappropriate use can result in a cancellation of those privileges.

Netiquette - Users are expected to use e-mail in a manner abiding by all applicable guidelines and laws.

1. For students, these guidelines are included in the Rules of Conduct and Procedures for Students of the Nevada System of Higher Education (Title 2, Chapter 10).

2. For faculty and staff, professional codes of conduct apply. These guidelines are included in the NSHE Code (Title 2, Chapter 6).

Additional Prohibitions - Behavior that is subject to interruption or revocation of user privileges and disciplinary action under this Code are violations of federal, State, and local law, and include conduct that threatens the safety or well-being of the campus community and any other behavior that adversely affects the CSN or its educational mission.

No Guarantee of Privacy – As noted previously, CSN electronic mail (email) is *not* guaranteed to be private. This is because system administrators who operate the system do have access to all email, and compliance with applicable law and implementation of CSN policies, including this policy, may result in monitoring. Messages relating to, or in support of illegal activities, may be reported to the authorities.

Reliability - CSN makes no warranties of any kind, whether expressed or implied, for the reliability of the electronic services. CSN will not be responsible for any damages employees or students suffer from use of the electronic resources. This includes loss resulting from delays, non·deliveries, misdeliveries, or service interruptions.

Security - Security on any computer system is a high priority, especially when the system

involves many users. If a student or employee believes that he or she can identify a security problem, he or she should notify a system administrator to help identify and resolve any associated problems. Students and employees should not give their passwords to any other individual. Attempts to log into the system by any other user may result in cancellation of user privileges. Attempts by non·system administrators to log in to the system as a system administrator or other system staff will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with computer systems may be denied access to the system and subject to other disciplinary actions that could include termination of employment or expulsion of a student.

N. Wireless Network Acceptable Use Policy

Users of CSN's Wireless Network Services agree to the following:

Compliance:
Use of CSN's wireless network is subject to this Policy. All wireless users, to include faculty, staff, students, guests, outside contractors, vendors, etc., must comply with the Policy. By your use of the CSN wireless network, you acknowledge your compliance obligations with the Policy. No user shall use the wireless network so as to interfere with the ability of others to access network resources. No user will attempt to penetrate the security of any CSN communications network or computer system. No technology resource will be used for an unsanctioned commercial purpose.

ServiceExpectations:
The CSN wireless network is intended as a supplement to the wired network and for use with portable electronic devices; it is not intended to be a user's sole connection to CSN's network or IT Resources. The wireless network should not be expected to provide the same quality of service as CSN's wired network infrastructure. When reliability and performance are critical, CSN's wired network infrastructure should be used. Stationary computing devices, such as PC/Mac towers, printers, servers, and other critical IT Resources must be connected to CSN's wired network infrastructure where reasonably possible.

Data Security:
Data transmitted over a wireless network can be easily intercepted, and it is critically important to implement security measures in conjunction with any use of wireless network access. These security measures should include authentication and strong data. Users are encouraged to use an encrypted VPN connection to access personal data.

Sharing Files and Accessing Information of the World Wide Web:

CSN supports the free exchange of information and ideas facilitated by sharing authorized or otherwise appropriate computer files. However, any copyrighted material must only be used with permission. Without the appropriate permission, the account owner or wireless user can experience the following: be asked to immediately remove the material; material removed by CSN personnel; civil liability, and/or criminal prosecution, and denial of access to the CSN network**.** Using CSN's network to download or share copyrighted music, movies, television shows or games without the appropriate permission may result in legal sanctions, network termination or both**.**

- *BitTorrent, Limewire, Gnutella, eDonkey, and other filesharing programs can transmit files on your computer to others in violation of copyright laws, with or without your knowledge. If these programs are on your computer, you will be held responsible for any copyright violations that may result.*

Privacy:
Many software systems are designed to collect usage information and to log user activity. CSN routinely aggregates the data stored in these log files for analytical purposes. In general, CSN makes no attempt to extract from the logs data regarding the activity of individual users. CSN does, however, reserve the right to do so in order to maintain a

functioning network. (For example, CSN may extract logs if an automated IT security systems report displayed that a user's computer/account is infected or compromised.)

Other:

CSN reserves the right to restrict the use of or permanently disconnect any wireless device from the campus network if that wireless device or wireless access point disrupts or interferes with services provided by CSN, or behaves in such a way that the service or security of IT Resources is impacted.

Any departments requiring wireless service in contravention of this standard when CSN's wired network option is not feasible must file the formal Security Policy/Procedure Exception Form with the Chief Information Officer and their Vice President prior to use of wireless service in contravention of this standard.

O. Records Retention & Network Storage and Managing & Storing Email & Attachments

1. SCOPE AND PURPOSE

NSHE adopted on July 1, 2016, a comprehensive Records Retention and Disposition Schedule ("Schedule") that was developed specifically to address the universities' and colleges' particularized records, documents, etc. The Schedule can be found in the Regent's Procedures and Guidelines Manual, Chapter 18.
The retention and destruction of all messages, documents, records, etc. at CSN should follow the Schedule. Many or most of such messages, documents, or records now are electronically created and maintained; the Schedule applies to both paper and electronic versions.

All CSN email account holders, and CSN network personal ("H"- drive) and shared departmental file storage ("J"-drive) account holders must understand how CSN is applying the Schedule as it applies to the mechanics of the retention and backup of CSN emails and files, records, documents, etc. stored on the CSN network drive and email server infrastructure.

NSHE's Schedule specifically addresses the management and retention of emails. In part, it notes:

> "**What is Email?** Email is not a record type, but is a means of conveying information similar to the United States Postal Service. Its retention is based upon the content of the email message, not the fact that it is an email message.
>
> An email (electronic mail) message is comprised of the following components:
>
> - textual message
> - metadata (To, From, Subject, Time, Date, System, etc.)
> - attachments

Each component is part of the record or non-record, as the case may be. In many instances, email has taken over the role of "general correspondence" and memoranda, as well as the telephone message. If an email message meets the criteria of a record, it must be managed in accordance with the Schedule.

Email Management: The key to effectively managing email is to get rid of the non-records and any transient/transitory records that have outlived their administrative/legal/fiscal value as quick as possible so that one is left with only those e-mails that need to be managed on an on-going basis. One should approach the management of email in a manner similar to how they handle processing their "snail mail" at work and home:

- Open the email and review the document's content; this may mean thoroughly reading

the document, but more often than not, one is able to judge just by a cursory look at the document, the subject line, and/or the sender to determine whether:

- **It is a non-record** and should be deleted immediately, just as one would discard the "snail mail" non-record into the trash can or recycle bin.

- **It is a transient/transitory record** which should be disposed of as soon as the information is no longer of administrative, legal or fiscal value. One might create a "Transient/Transitory" folder or create sub-folders of record type/series or projects for the transient/transitory messages.

- **It is a record** and therefore, should be placed in an appropriate folder by record type/series, project, retention time, or other filing schema that works for one's office/organization and allows that unit to effectively manage the life cycle of the record."

Each CSN account user must manage their email and electronic file storage so that they are efficient tools which do not place an undue burden on the finite capacity of computer system resources, while complying with the Schedule. Retention and storage of emails and other files are costly and must be undertaken in order to take advantage of system capabilities in a cost effective manner.

2. ELECTRONIC STORAGE

a. E-mail

Email communications are an integral part of communications that occur at CSN. As noted in the Schedule, emails are in some ways similar to paper mail that must be sorted and managed, and in other ways closer attention must be paid to avoid large quantities of emails simply building up. Some emails comprise information that the user will want or be required to maintain for a lengthy period of time, and many emails are the opposite and once read can be discarded.

E-mail is not a storage system, it is a communication tool. As such, CSN cannot provide an email system that has unlimited capacity and we must use the available capacity in a prudent manner to be efficient in our job performance. In addition, it is imperative that records kept pursuant to the Schedule be appropriately stored. E-mail for all users will be backed up daily. E-mails will be available for a period of seven years after which they will be permanently deleted, on a continuous basis, with no opportunity for recovery. This applies to both active and inactive e-mail accounts and backups.

Any e-mail attachments related to official communications that must be saved can be saved to the user's CSN "H" network drive for storage beyond seven (7) years.

Whenever a user completely deletes e-mails from their mailbox, they can be recovered for fourteen (14) days. After fourteen (14) days, the deleted e-mails will not be recoverable.

b. File Systems

Network storage space is provided for the storage of files, records, documents, messages, etc. that are related to CSN business. Each CSN computer user is typically assigned access to both an individual storage drive, "H" drive, and a departmental shared drive, "J" drive. The "H" drive is for the employee's work files and the "J" drive is for the storage of shared work-group files. Records that must be kept pursuant to the Schedule will be appropriately stored in "J" drives, not "H" drives.

To ensure there is adequate storage space for each employee, the "H: drive" has been allotted a storage max size of ten (10) gigabytes for faculty and staff, only after the on-line (on Cloud) storage of at least 1-Terrabyte per individual is provided. This storage may not be used for personal movies, music, games, photos, etc. Nor should the storage be used for copyrighted materials without proper permission or licenses as this is a violation of federal law.

"H" drive folders are backed up on a daily basis. The backups of "H" files will be purged after two (2)years, on a continuous basis. This means that deleted files will be unrecoverable after a two (2) year period.

"J" drive folders are backed up on a daily basis. "J" drives will not be purged or overwritten on any set schedule. The "J" drive should be used to store department related records, documents, files, messages, etc. in compliance with the Schedule. However, destruction dates should be added to or noted on files so that after the appropriate retention period has passed, they can be discarded and not build up over decades utilizing storage capacity unnecessarily.

In order to provide CSN faculty and staff with a tool for sharing files, CSN will provide access to cloud storage. Storage of any PII, credit card or other financial information is not permitted. The data in cloud storage will not be backed up so deleting a file permanently deletes the data with no opportunity for recovery. In addition, users should be aware that CSN can legally access everything uploaded to this cloud storage in the case of wrongdoing or computer misconduct as determined by CSN.

c. Exiting Employees
Employee email accounts will be closed upon separation from active employment. As of the separation date, the employee will no longer have any access to their e-mail account, their "H" drive, all "J" drives, OneDrive or any backups of any data. It is the responsibility of the exiting employee's manager to inform the Department of Human Resources prior to the employee's exit date, if the e-mail account for the exiting employee is to be forwarded to a supervisor, or retained for a maximum of thirty days (unless a longer period of retention is authorized by the relevant Vice President). Human Resources personnel will then notify the Office of Technology Services of the request. If notification is not given when the employee's network account is closed, only the e-mail will be stored according to the Schedule.

d. **Inactive Employees**
An employee who has not logged into the system for five (5) months will have their accounts disabled. After twelve (12) months of inactivity, these accounts will be purged. Departments must notify the Office of technology if an employee will be out on sabbatical or inactive for a period longer than four (4) months.

3. LITIGATION HOLDS

When litigation is pending or threatened against CSN or its employees, court rules impose a duty upon CSN to preserve all documents and records that pertain to the issues. It is the responsibility of employees who have actual knowledge of matters in which it can be reasonably anticipated that a court action will be filed, a subpoena has been served or notice of same has been given, or records are sought pursuant to an audit, a government investigation or in similar circumstances to attempt to preserve CSN records, including emails or instant messages.

Employees should consider that all e-mail entering or leaving the CSN messaging system will be captured and subject to litigation based research without consideration of the subject or if the message is personal in nature.

A 'litigation hold' directive overrides the Schedule, as well as any other records retention schedules that may have otherwise called for the transfer, disposal or destruction of relevant documents, until the hold has been cleared by written directive.

III. PROCEDURE
N/A

IV. AUTHORITY AND CROSS REFERENCE LINKS

Nevada Constitution Article 11

http://www.leg.state.nv.us/const/nvconst.html - Art11

Nevada Revised Statutes sections 197.110 (2) and 205.473 through 205.513
http://www.leg.state.nv.us/nrs/NRS-197.html#NRS197Sec110
http://www.leg.state.nv.us/nrs/NRS- 205.html#NRS205Sec473

Board of Regents Handbook Title 4, Chapter 1, Section 22
http://system.nevada.edu/Board-of-R/Handbook/TITLE-4---/T4-CH01---General-Policy- Statements.pdf

Board of Regents Handbook Title 2, Chapter 6 et al
http://system.nevada.edu/Board-of-R/Handbook/TITLE-2---/T2-CH06---Rules-and-Disciplinary- Pro.pdf

Rules of Conduct & Procedures for Students Policy
https://www.csn.edu/sites/default/files/u421/student_conduct_code_policy.pdf

"Student Rights and Responsibilities" section of the Student Handbook
http://www.csn.edu/pages/1722.asp

NSHE Records Retention and Disposition Schedule
http://system.nevada.edu/tasks/sites/Nshe/assets/File/BoardOfRegents/Procedures/PGMCH18RECORDSRETENTIONANDDISPOSITIONSCHEDULE.pdf

V. DISCLAIMER

The President has the discretion to suspend or rescind all or any part of this policy or related procedure(s). The President shall notify appropriate CSN personnel, including the Administrative Code Officer and Faculty Senate Chair, of the suspension or rescission.

Questions about this policy should be referred to the CSN Administrative Code Officer (general.counsel@csn.edu, 702.651.7488) and/or the Faculty Senate Chair.

VI. SIGNATURES

Recommended by:

/s/ Alok Pandey _____ 7/5/17_____
Faculty Senate Chair Date

Reviewed for Legal Sufficiency:

/s/ Richard L. Hinckley _____ 7/6/17_____
General Counsel Date

Approved by:

/s/ Michael D. Richards _____ 7/5/17_____
President Date

VII. ATTACHMENTS

A. History

- 2016-2017:

1. Section II, B.
Removal of the unnecessary words: “College of”

2. Section II, D.
Clarification providing for monitoring

3. Section II, F.
Clarification of what would cause someone to unduly consume resources

4. Section II, G.
Removal of unnecessary words to produce a simple, direct explanation
Point 1., (c) was remove and added to b to eliminate redundancy in language
Point 2. and 3. were simplified to identify that OTS has responsibility for password policies

5. Section II, H.
Clarification provided for monitoring

6. Section II, M.
Wording clarified to express what communication vehicles serve as CSN’s official mode of communication

7. Section II, M.
The policy regarding automatic forwarding of e-mail was moved from Section O, II, a

8. Section II, M.
Clarification of the Netiquette portion of the policy.

9. Section II, N.
Clarification provided to example examples of when CSN may extract from the logs data

10. Section II, O, I
Wording added to identify network and shared departmental file storage account holders.

11. Section II, O, II, a.
Wording changed to account for the change from an onsite server based archival system to a cloud-based backup system

12. Section II, O, II, b.
Clarification of where records that need to be stored according to the NSHE Schedule should be stored. “H” drive storage for faculty and staff is being increased from two gigabytes to ten. Change to “H” drive back-up storage policy from five years to two years. Explanation of the guidelines surrounding a new tool available to faculty and staff – Microsoft OneDrive

13. Section II, O, II, c.
The word termination was changed to separate to indicate that the policy applies to all individuals who leave the college. Clarification added so that employees understand that they cannot access any network resources upon separation for any reason. Storage policy for the e-mails of separated employees changed to meet the requirements of the NSHE Schedule.

14. Section II, O, 2
Section (d), inactive employees, was added.

15. Authority and Cross Reference Links
The link for the student rules of conduct was corrected.

- 04/29/2016: Records Retention and Network Storage and Managing And Storing Email Attachments were added.

- 04/17/2013: Wireless network acceptable use section was added.

- 04/02/2013: E-mail acceptable use section was added.

- 05/20/2011: Approved by CSN President Mike Richards
    - 05/11/2011: Reviewed by General Counsel
    - 05/10/2011: Recommended by Faculty Senate (B. Kerney)
    - 1/21/2011: Revision Submitted by Policy Review Committee (F. Jackson)
        - Policy was rewritten into the approved format, as per GEN 1.2.
    - 12/8/2010: Changes and Additions Presented to Faculty Senate
        - Section II.F – Password Construction, Protection & Changes
        - Section II.K.1 – Reporting Violations
        - Section II.K.2 – Disabling of Accounts
        - Section II.K.3 – Additional Penalties
    - Section II.G – Password characteristics enhanced.
    - Policy was rewritten into the approved format, as per GEN 1.2.
    - Section II.L. – Reporting Violations
    - 11/9/2010: Forwarded to the CIO for Review

- 5/27/2008: Signed by President Richards
    - 5/9/2008: Recommended by Faculty Senate
    - 2/2008: Returned to Senate Chair with Revisions
    - 1/2008: Forwarded by Faculty Senate Chair to Ad-Hoc Committee on the Use of Online Resources for Review

- 6/20/2007: Approved by CSN President Richard Carpenter
    - 6/2007: Forwarded to President Carpenter bypassing Faculty Senate Review