

 <b>CSN Policy</b>	<b>Information Systems and Electronic Resources Acceptable Use Policy</b> <b>General Policy #2, Version 3</b>
<b>Number: GEN 2.3</b>	<b>Effective Date: 05/20/2011</b>
<p style="text-align: center;"><b>MOST RECENT CHANGES</b></p> <p>Version 3:</p> <ol style="list-style-type: none"> <li>1. Section II.G – Password characteristics enhanced.</li> <li>2. Policy was rewritten into the approved format, as per GEN 1.2.</li> <li>3. Section II.L.1 – Reporting Violations</li> <li>4. Section II.L.2 – Disabling of Accounts</li> <li>5. Section II.L.3 – Additional Penalties</li> </ol>	

## 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 College of Southern Nevada (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, 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
  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 College activities
- G. Passwords are an important aspect of computer security. They are the front line of protection for user accounts and system integrity. A poorly chosen password can result in the compromise of CSN's entire network.
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 and may only be used by the person for whom the password was created.
    - c. A password may not be posted in a place accessible by others.
    - d. User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
    - e. Group passwords are allowed only in the case of the highest level administrator passwords for servers.
    - f. Passwords must not be inserted into email messages or other forms of electronic communication.
    - g. Pre-validated Active Directory accounts that are not validated and activated within three calendar days will be disabled.
  2. Password Construction: Users must select passwords that contain at least eight alphanumeric characters including at least one special character. A special character is defined as a non alphanumeric character (e.g., ~, !, @, #, \$, %, ^, &, \*, (, ), -, =, +, ?, [, ], {, }). Simple or weak passwords must not be used. Simple or weak passwords have the following characteristics:
    - a. The password contains less than eight characters.
    - b. The password is a word found in a dictionary (English or foreign).
    - c. The password is a common usage word such as:

- d. Names of family, pets, friends, co-workers, fantasy characters, etc.
  - e. Computer terms and names, commands, sites, companies, hardware, software.
  - f. Birthdays and other personal information such as addresses and phone numbers.
  - g. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - h. Any of the above spelled backwards.
  - i. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
3. Password Changes:
- a. All users who are CSN staff/faculty or vendors/contractors and have user-level passwords (e.g., network, domain, email, desktop computer, etc.) must change their passwords every 90 days.
  - b. All users who are CSN students and have user-level passwords (e.g., network, domain, email, desktop computer, etc.) must change their passwords every 180 days.
  - c. User-level passwords must be unique for four consecutive password changes, i.e., a password cannot be reused for 4 password changes.
  - d. All users will receive an automated email notifying them their password will expire in 14 days and, if necessary, that their password will expire in 1 day. If the current password is not changed before it expires, a password change will be prompted upon the user's first log in attempt after the expiration date and the user will not be able to log in to the CSN network until the password is changed.
- 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, 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 the school's Active Directory for authentication, authorization and auditing, must be reported to OTS.

2. 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.
3. 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.
4. 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.
5. 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.

### 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>

CSN Student Conduct Code

<http://www.csn.edu/pages/1722.asp>

"Student Rights and Responsibilities" section of the Student Handbook

<http://www.csn.edu/pages/1722.asp>

### 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](mailto:general.counsel@csn.edu), 702.651.7488) and/or the Recommending Authority.

**VI. SIGNATURES**

Recommended by:

/s/ William r. Kerney  
Signature  
Faculty Senate Chair  
Recommending Authority Title

5/10/11  
Date

Reviewed for Legal Sufficiency:

/s/ Richard L. Hinckley  
General Counsel

5/11/11  
Date

Approved by:

/s/ Michael D. Richards  
CSN President

5/20/11  
Date

**VII. ATTACHMENTS**

A. History

## HISTORY

- Version 3:
  - 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
  - 11/9/2010: Forwarded to the CIO for Review
  
- Version 2:
  - 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
  
- Version 1:
  - 6/20/2007: Approved by CSN President Richard Carpenter
  - 6/2007: Forwarded to President Carpenter bypassing Faculty Senate Review