NSCS Information Security Standard 5: Acceptable Use Policy

Privacy notifications, including an explanation of the data that are collected and for what purpose, and whom to contact regarding privacy information, will be included with all external facing websites.

Users must agree to comply with the NSCS Acceptable Use Policy (AUP) prior to gaining access to NSCS Technology Resources.

NSCS Acceptable Use Policy

Rev: 8
Date: 11-21-2023
Nebraska State College System (NSCS)

Acceptable Use Policy

The Acceptable Use Policy applies to all individuals accessing or using NSCS Technology Resources. This includes NSCS students, employees, and authorized contractors and guests.

Use of Technology Resources

Confidentiality

NSCS follows the principle of least privilege in granting permission to Technology Resources. Your access to Technology Resources does not imply that others have the same access. It is the responsibility of each NSCS employee to ensure that no unauthorized disclosures occur.

Privacy

The NSCS provides and supports Technology Resources to employees for effective performance of job duties.

Activity may be monitored, logged, and reviewed by system administrators or discovered in legal proceedings. All information created, stored, transmitted, or received on Technology Resources may be subject to monitoring by system administrators.

Inspection of an individual's data by NSCS Information Technology personnel in the course of responding to a request from that individual shall not be deemed a violation of the individual's privacy.

NSCS Rights

The NSCS reserves the right to monitor, manage, and/or deny network access to any device attempting to use an NSCS network. This action may be taken, without prior approval, to maintain the integrity of NSCS Technology Resources, to protect the rights of others authorized to access the network, or if misuse of NSCS Technology Resources is suspected.

The NSCS reserves the right to access data in an individual's NSCS account or NSCS owned device if the NSCS has a legitimate business need to review such files. This action will be taken only after obtaining approval from the President, appropriate Vice-President, or General Counsel.

Individual Rights

Individuals are granted access to and permitted use of NSCS Technology Resources. Access is granted for the purpose of achieving employment and educational goals based on the individual's need and classification.

Employees are granted access for the duration of employment. Individuals are considered employees if hired for full-time and part-time positions. Student employees funded via work study or institutional

funds may qualify for employee access.

Students are granted access for the duration of their student status with the NSCS. Individuals are granted access to Technology Resources by use of their campus issued Credentials.

Responsibilities

Each individual is responsible for the security and integrity of data stored on assigned devices and resources to which they have been authorized access, including but not limited to desktops, laptops, tablets, and mobile devices. Responsibilities include:

- Performing and securely storing backups of data where not provided by the IT department.
- Securing physical access to devices and data.
- Locking computers when stepping away.
- Logging out of sessions.
- Monitoring access to assigned computer accounts.
- Reporting suspected security compromise or unauthorized access to the IT Help Desk and changing passwords immediately.
- Maintaining device connection to the College network for application of operating system and software updates.
- Installing, using, and updating virus protection software.
- Maintaining strong passwords and protecting the confidentiality of the password.
- Abiding by password procedures established for Technology Resources.
- Using accounts and privileges for their authorized purposes.
- Respecting the right of other individuals with regard to data access, intellectual property, privacy, academic freedom, copyright, freedom from harassment.

Restrictions

Unauthorized actions include but are not limited to the following:

- Providing computer accounts to an individual not authorized for such access to include sharing one's own account with others.
- Attempting to or successfully logging in to an account other than that which is officially assigned.
- Using an account for other than the authorized purpose.
- Tampering with accounts or authorization associated with an account.
- Tampering with computers not specifically assigned to the user.
- Sharing remote access authorization with anyone.
- Using knowledge of security or access to damage resources, obtain credentials, or gain unauthorized access to accounts.

- Operating unauthorized servers on the campus network. All servers must have prior approval by the college CIO before activation on the campus network.
- Extending the network by connecting a hub, switch, router, wireless access point or any other device.
- Altering source addresses of network traffic.
- Altering source addresses (forging) of email.
- Sending mass emails (spamming) for purposes other than official business.
- Using the Internet to maliciously damage campus or Internet accessible Technology Resources.
- Attempting to negatively affect Technology Resource performance.
- Modifying or destroying data which are not specifically assigned to or created by the user.
- Intercepting transmissions not intended for the individual.
- Vandalizing Technology Resources.
- Including profane, vulgar or other harassing language within email messages, programs, and/or files.
- Engaging in non-collegial activities which threaten, defame, slander, or otherwise to cause harm to others.
- Accessing pornographic materials.
- Utilizing Technology Resources with the intent to harass others.
- Installing and/or spreading malicious software.
- Placing undue burden on the networks.
- Violating copyright laws.
- Prohibited Uses of Technology Resources, per Policy 5008:
- Using computers, software, or other NSCS equipment for personal or commercial financial gain is prohibited.
- Political or lobbying activities is prohibited.
- Private business or commercial use is prohibited.

Actions

- Limited personal use of Technology Resources is permitted so long as such usage conforms to policy, does not interfere with operations including security of the system, network response time, or a user's performance of duties as an employee, and does not result in additional costs or inefficiencies to the NSCS.
- Violation or refusal to adhere to this Acceptable Use Policy may result in denial of access to Technology Resources and/or disciplinary action.

- Individuals are encouraged to report suspected violations of policies to the Chief Information Officer. Individuals are expected to cooperate with system administrators during investigations of Technology Resource abuse and failure to do so may result in disciplinary action.
- The NSCS has final authority to determine what constitutes acceptable use and the right to initiate disciplinary action.
- Only those administrators named by the Chief Information Officer as being directly responsible for the security of Technology Resources may use special privileges which permit the examination, copying or printing of files, programs, email, or other information in an account, without the individual's prior permission.
- The designated administrators may only use their special privileges in compliance with this Policy. A system administrator may not divulge any information obtained using special privileges to any person other than the Chief Information Officer who will take the appropriate action. If an individual suspects that someone has attained access to his/her account, the incident should be reported to the Chief Information Officer immediately in order to initiate appropriate action.

Revision History

April/14/2019:	Initial submission by PCSS
May/8/2019:	Initial review by SOISO/CISOs
July/8/2019:	Second review by SOISO/CISOs
July/26/2019:	Third review by SOISO
Aug/15/2019:	Fourth review by SOISO
Sept/30/2019:	Fourth review by SOISO/CISOs using campus feedback
May/26/2023:	Annual review by SOISO/CISOs
Nov/21/2023:	Annual review by SOISO/CISOs