Board of Trustees of the Nebraska State Colleges

Meeting Date**: September 10, 2026**

Agenda Item: **2.1**

ITEMS FOR DISCUSSION AND ACTION:

Committee: **Academic & Personnel Committee**

Action Item: **Revisions to Policy 5008, New Policy 7001 - Use of System Technology Resources**

Policy 5008 has not been significantly updated in several years. The updates to this Policy clarify the use of social media and provide more comprehensive directions for use of NSCS Technology Resources consistent with IT security standards. NSCS Technology Resources are intended to support knowledge sharing, collaboration, and the fulfillment of NSCS educational, research, public service, and work-related responsibilities. All users, including employees, student employees, volunteers, contractors, and guests, must comply with this policy, and violations may result in loss of access or disciplinary action. Since this Policy has been expanded beyond employee users, the policy is being relocated to the 7000 Series which contains all IT related policies.

The draft was routed to all NSCS employees for feedback in August. Attached is the draft that was shared with employees in track changes. A clean copy of the final version in the appropriate NSCS format is also attached.

The System Office recommends approval of Policy 5008, New Policy 7001 - Use of System Technology Resources.

ATTACHMENTS:

- 5008 with edits
- Policy 7001 with new format

POLICY ~~5008~~ 7001 Acceptable Use of ~~System~~ NSCS Technology Resources

---

PURPOSE~~Board Policy 5008 references Board Policy 7003; NSCS Information Security Program, including the Security Standards defined by Board Policy 7003. Term definitions in Board Policy 5008 may be found in Standard 1.~~

NSCS Technology Resources provided by the Colleges and the System Office ~~are the property of the Nebraska State Colleges System (NSCS) and~~ are to be used for the sharing of knowledge, collaborative efforts, and completion of job or volunteer duties within the NSCS educational, research and public service missions. This Policy governs the use of NSCS Technology Resources.

The requirements in this Policy must be followed by all users of College networks including all use of any other networks that are accessed through an NSCS connection. The requirements in this Policy apply to all users including NSCS employees (including student employees), volunteers, authorized contractors and guests. Users that violate this Policy may be subject to denial of access and disciplinary action.

DEFINITIONS

Information Technology Resources: Information Technology Resources include devices and software that have a primary function related to the collection, transfer, storage, or processing of data. Equipment includes classroom and office equipment used to display or print data. Computers, printers, monitors, keyboards, servers, drivers, switches, routers, network cable and software licenses.

Users: Users include all NSCS employees (including student employees), volunteers, authorized contractors and guests.

POLICY

Access and Credentials

Users may only gain access to NSCS Technology Resources by use of their College issued credentials.

NSCS follows the principle of least privilege in granting permission to NSCS Technology Resources. User access to NSCS Technology Resources does not imply that other users have the same access. It is the responsibility of each user to ensure that no unauthorized uses or disclosures occur.

Acceptance of any credentials (i.e. username/password, ID card or token, PIN, etc.) that provide access to NSCS Technology Resources shall constitute an agreement on behalf of the user to abide and be bound by the provisions of this Policy. Access to NSCS Technology Resources is a privilege, not a right. Every user is to be responsible for the integrity of the system, respect for the rights of other users, the integrity of the physical facilities and controls, and all pertinent license and contractual agreements related to NSCS systems.

Users shall make reasonable efforts to safeguard their credentials. No user may allow unauthorized persons to access College or System Technology Resources, except in cases necessary to facilitate computer maintenance and repairs. When any employee terminates employment with the College or System Office, his or her credentials shall be denied further access to Technology Resources.

Inspection and Monitoring

All information created, stored, transmitted, or received on NSCS Technology Resources may be subject to monitoring. This includes anything published on the internet or the NSCS or College intranet.

The NSCS reserves the right to inspect any NSCS Technology Resource without advance notice to or specific permission from any ~~employee,~~ user for any legitimate business purpose. Activity on NSCS Technology Resources may be monitored, logged, and reviewed by NSCS or College administrators, discovered in legal proceedings and/or disclosed through public record requests.

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 a user's NSCS account or NSCS owned device if the NSCS has a legitimate business need to review such files. Inspection of a user's data shall not be deemed a violation of the user's privacy. Access and inspection will be taken only after obtaining approval from the Chancellor, President, or General Counsel.

- Only those administrators named by the respective NSCS or College Chief Information Officer as being directly responsible for the security of NSCS 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. If a user suspects that someone has attained access to his/her account, the incident should be reported to the respective NSCS or College Chief Information Officer immediately in order to initiate appropriate action.

User ~~The requirements in this Policy are to be followed by all employees utilizing State College Networks including all use of any other networks that are accessed through an NSCS connection. Employees must comply with the NSCS Acceptable Use Policy (AUP) prior to gaining access to NSCS Technology Resources. The NSCS AUP is located in Standard 5. The requirements found therein apply to all persons accessing or using NSCS Technology Resources, including NSCS students, employees, and authorized contractors and guests. Individuals that violate the NSCS AUP may be subject to denial of access and disciplinary action.~~

~~Acceptance of any credentials (i.e. username/password, ID card or token, PIN, etc.) that provide access to NSCS Technology Resources shall constitute an agreement on behalf of the user or any other individual accessing such information to abide and be bound by the provisions of this Policy and the NSCS AUP. Access to NSCS Technology Resources is a privilege, not a right. Every user is to be responsible for the integrity of the system, respect for the rights of other users, the integrity of the physical facilities and controls, and all pertinent license and contractual agreements related to NSCS systems.~~

~~Employees shall make reasonable efforts to safeguard their credentials. No employee may allow unauthorized persons to access College or System Technology Resources, except in cases necessary to facilitate computer maintenance and repairs. When any employee terminates his or her employment with the College or System Office, his or her credentials shall be denied further access to Technology Resources unless otherwise determined by the President or Chancellor.~~

~~Use of Technology Resources for personal or commercial financial gain, for private business or commercial use, or for personal political or lobbying activities are prohibited.~~
Use of Technology Resources for personal or commercial financial gain, for private business or commercial use, or for personal political or lobbying activities are prohibited.

~~Limited personal use of College or System Technology Resources is permitted so long as such usage conforms with Policy, does not interfere with operations including, but not limited to, 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 College or System.~~

Responsibilities

All users ~~of College or System Technology Resources~~ are expected to respect the privacy of other users and their data ~~in accordance to the NSCS AUP~~, and to respect the legal protection of programs, publications and data provided by copyright and licensing laws. All relevant laws and regulations, including public records laws, federal copyright laws, and federal privacy laws such as the Family Educational Rights to Privacy Act (FERPA) are to be respected by users. Downloading, distributing and/or displaying any copyrighted material without permission of the copyright owner is strictly prohibited.

Each user is responsible for the security and integrity of data stored on assigned devices and NSCS Technology Resources to which they have been authorized access, including but not limited to cloud hosted applications, desktops, laptops, tablets, and mobile devices. Responsibilities include:

- Securely storing NSCS data on NSCS Technology Resources.
- Securing physical access to devices and data.
- Locking computers when left unattended.
- Logging out of devices and applications.
- 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.
- Maintaining strong passwords and protecting the confidentiality of the password.
- 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, and freedom from harassment.

To preserve the integrity and security of NSCS Technology Resources, NSCS employees purchasing information technology products and services must first consult with the College CIO, or the System Office CIO. Refer to Board Policy 8064 and Policy 7003.

User Restrictions

Use of NSCS Technology Resources for commercial financial gain, for private business or commercial use, or for personal political or lobbying activities are prohibited. Limited personal use of NSCS Technology Resources is permitted so long as such usage conforms with Policy, does not interfere with operations including, but not limited to, 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 College or System.

Users shall ensure their use of personal devices to engage in non-work activity including but not limited to internet surfing, blogging, personal email correspondence, and social media networking occurs on personal time, before or after scheduled work hours or during lunch or other approved breaks.

Unauthorized actions utilizing NSCS Technology Resources 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.

- Storing personal data to NSCS IT approved services.
- Using an account for other than the authorized purpose.
- Tampering with accounts or authorization associated with an account.
- Tampering with computers or other devices 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 an unauthorized 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 NSCS Technology Resources.
- Attempting to negatively affect NSCS Technology Resource performance.
- Transferring and/or storing NSCS data to personal or unapproved NSCS Technology Resources.
- Modifying or destroying data which are not specifically assigned to or created by the user.
- Intercepting transmissions not intended for the user.
- Vandalizing NSCS 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 cause harm to others.
- Accessing, creating, producing or distributing pornographic materials.
- Utilizing NSCS Technology Resources with the intent to harass others.
- Installing and/or spreading malicious software.
- ~~e~~Execut~~inge~~ programs that harass other users or infiltrate systems and/or damage or alter data.
-
- Placing undue burden on the networks.

- Downloading, distributing and/or displaying any copyrighted material without permission of the copyright owner is prohibited.

- Sharing proprietary information or confidential College or student information, including information protected by FERPA, Health Insurance Portability and Accountability Act (HIPAA), or other applicable laws.

- Stating or otherwise imply that the user's views are representative of those of the Board of Trustees, the NSCS, or the Colleges unless specifically authorized to do so.

Consequences for Violating this Policy

Violation may result in denial of access to NSCS Technology Resources and/or disciplinary actions.

Users may report suspected violations of this Policy to the respective NSCS or College Chief Information Officer. Users are expected to cooperate with system administrators during investigations of NSCS Technology Resource abuse and failure to do so may result in disciplinary action.

~~To preserve the integrity and security of NSCS Technology Resources, NSCS employees purchasing information technology products and services must first consult with the College CIO, or the System Office CIO. Refer to Board Policy 8064, and to Standard 10: Technology Resources Acquisition, in Board Policy 7003.~~

~~Each College, affiliate organization, and the System Office is responsible for employee use of Technology Resources and for ensuring that its employees are familiar with the provisions outlined in this Policy and in the NSCS AUP.~~

Policy Adopted: 11/11/95
Policy Revised: 2/10/05
Policy Revised: 4/25/14
Policy Revised: 11/14/19
Policy Revised: 1/24/20
Policy Revised: 4/11/22

Board of Trustees of the Nebraska State Colleges

Policy Category

POLICY NAME: Acceptable Use of NSCS Technology Resources

POLICY NUMBER: 7001

A. PURPOSE

NSCS Technology Resources provided by the Colleges and the System Office are to be used for the sharing of knowledge, collaborative efforts, and completion of job or volunteer duties within the NSCS educational, research and public service missions. This Policy governs the use of NSCS Technology Resources.

The requirements in this Policy must be followed by all users of College networks including all use of any other networks that are accessed through an NSCS connection. The requirements in this Policy apply to all users including NSCS employees (including student employees), volunteers, authorized contractors and guests. Users that violate this Policy may be subject to denial of access and disciplinary action.

B. DEFINITIONS

1. **Technology Resources**: Technology Resources include, but are not limited to, all NSCS-owned, operated, leased, outsourced, or contracted computing, networking, telephone, communication devices, and software that have a primary function related to the collection, transfer, storage, or processing of data. Equipment includes classroom and office equipment, including, but not limited to, computers, printers, monitors, keyboards, servers, drives, switches, routers, network cables, and software licenses used to display or print data; information resources; all NSCS electronic information, including data, voice, and video; all NSCS data, voice, and video networks; all NSCS application systems and software used to conduct campus business; and all NSCS-connected assets.
2. **Users:** Users include all NSCS employees (including student employees), volunteers, contractors and guests who are authorized and have been granted access to NSCS Technology Resources.

C. POLICY

1. Access and Credentials

1.1. Users may only gain access to NSCS Technology Resources by use of College issued credentials.

1.2. NSCS follows the principle of least privilege in granting permission to NSCS Technology Resources. User access to NSCS Technology Resources does not imply that other users have the same access. It is the responsibility of each user to ensure that no unauthorized uses or disclosures occur.

1.3. Acceptance of any credentials (i.e. username/password, ID card or token, PIN, etc.) that provide access to NSCS Technology Resources shall constitute an agreement on behalf of the user to abide and be bound by the provisions of this Policy. Access to NSCS Technology Resources is a privilege, not a right. Every user is to be responsible for the integrity of the system, respect for the rights of other users, the integrity of the physical facilities and controls, and all pertinent license and contractual agreements related to NSCS systems.

1.4. Users shall make reasonable efforts to safeguard their credentials. No user may allow unauthorized persons to access College or System Technology Resources, except in cases necessary to facilitate computer maintenance and repairs. When any employee terminates employment with the College or System Office, his or her credentials shall be disabled per Information Security Standard 4.

2. Inspection and Monitoring

2.1. All information created, stored, transmitted, or received on NSCS Technology Resources may be subject to monitoring. This includes anything published on the internet or the NSCS or College intranet.

2.2. The NSCS reserves the right to inspect any NSCS Technology Resource without advance notice to or specific permission from any user for any legitimate business purpose. Activity on NSCS Technology Resources may be monitored, logged, and reviewed by NSCS or College administrators, discovered in legal proceedings and/or disclosed through public record requests.

2.3. 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.

2.4. The NSCS reserves the right to access data in a user's NSCS account or NSCS owned device if the NSCS has a legitimate business need to review such files. Inspection of a user's data shall not be deemed a violation of the user's privacy.

- Only those administrators named by the respective NSCS or College Chief Information Officer as being directly responsible for the security of NSCS 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. If a user suspects that someone has attained access to his/her account, the incident should be reported to the respective NSCS or College Chief Information Officer immediately in order to initiate appropriate action.

3. User Responsibilities

3.1. All users are expected to respect the privacy of other users and their data, and to respect the legal protection of programs, publications and data provided by copyright and licensing laws. All relevant laws and regulations, including public records laws, federal copyright laws, and federal privacy laws such as the Family Educational Rights to Privacy Act (FERPA) are to be respected by users. Downloading, distributing and/or displaying any copyrighted material without permission of the copyright owner is strictly prohibited.

3.2. Each user is responsible for the security and integrity of data stored on assigned devices and NSCS Technology Resources to which they have been authorized access, including but not limited to cloud hosted applications, desktops, laptops, tablets, and mobile devices. Responsibilities include:

- Securely storing NSCS data on NSCS Technology Resources.
- Securing physical access to devices and data.
- Locking computers when left unattended.
- Logging out of devices and applications.
- 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.
- Maintaining strong passwords and protecting the confidentiality of the password.

- 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, and freedom from harassment.

3.3. To preserve the integrity and security of NSCS Technology Resources, NSCS employees purchasing information technology products and services must first consult with the College CIO, or the System Office CIO. Refer to Board Policy 8064 and Policy 7003.

4. User Restrictions

4.1. Use of NSCS Technology Resources for commercial financial gain, for private business or commercial use, or for personal political or lobbying activities are prohibited. Limited personal use of NSCS Technology Resources is permitted so long as such usage conforms with this Policy, does not interfere with operations including, but not limited to, 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 College or System.

4.2. Users shall ensure their use of personal devices to engage in non-work activity including but not limited to internet surfing, blogging, personal email correspondence, and social media networking occurs on personal time, before or after scheduled work hours or during lunch or other approved breaks.

4.3. Unauthorized actions utilizing NSCS Technology Resources 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.
- Storing personal data to NSCS IT approved services.
- Using an account for other than the authorized purpose.
- Tampering with accounts or authorization associated with an account.
- Tampering with computers or other devices 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 an unauthorized 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 College or Internet accessible NSCS Technology Resources.
- Attempting to negatively affect NSCS Technology Resource performance.
- Transferring and/or storing NSCS data to personal or unapproved NSCS Technology Resources.
- Modifying or destroying data which are not specifically assigned to or created by the user.
- Intercepting transmissions not intended for the user.
- Vandalizing NSCS 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 cause harm to others.
- Accessing, creating, producing or distributing pornographic materials.
- Utilizing NSCS Technology Resources with the intent to harass others.
- Installing and/or spreading malicious software.
- Executing programs that harass other users or infiltrate systems and/or damage or alter data.
- Placing undue burden on the networks.
- Downloading, distributing and/or displaying any copyrighted material without permission of the copyright owner is prohibited.
- Sharing proprietary information or confidential College or student information, including information protected by FERPA, Health Insurance Portability and Accountability Act (HIPAA), or other applicable laws.

- Stating or otherwise imply that the user's views are representative of those of the Board of Trustees, the NSCS, or the Colleges unless specifically authorized to do so.

5. Consequences for Violating this Policy

5.1. Violation may result in denial of access to NSCS Technology Resources and/or disciplinary actions.

5.2. Users may report suspected violations of this Policy to the respective NSCS or College Chief Information Officer. Users are expected to cooperate with system administrators during investigations of NSCS Technology Resource abuse and failure to do so may result in disciplinary action.

FORMS / APPENDICES:

None

SOURCE:

Legal Reference:

Policy Adopted: November 1995

Policy Revised: February 2005, April 2014, November 2019, January 2020, April 2022, September 2026