PERSONNEL, NEBRASKA STATE COLLEGE SYSTEM

POLICY: 5008 Employee Use of System Technology Resources Page 1 of __

Policy 5008 references Board Policy 7003: NSCS Information Security Program, including the Security Standards defined by 7003. Term definitions in Policy 5008 may be found in Standard 1, located here (URL-TBD).

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

The NSCS reserves the right to inspect any NSCS Technology Resource without advance notice to or specific permission from any employee, for any legitimate business purpose.

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, which may be found here (URL-TBD). 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 NSCS 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.

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.

Consistent with the NSCS AUP, employees are also expected to respect the integrity of Technology Resources and shall not intentionally execute programs that harass other users or infiltrate systems and/or damage or alter data.

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. 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: