WESTERN NEBRASKA COMMUNITY COLLEGE

Western Community College Area Board of Governors' Policy

TITLE:	Information Security
DIVISION:	Administrative Services
CATEGORY:	Information Technology
REFERENCE:	Nebraska Revised Statutes: §81-1117.02 and § 81-6,121
NUMBER:	BP-808
APPROVAL/DATE:	F. Lynne Klemke, President, WCCA Board of Governors June 16, 2021

Purpose

This policy ensures the confidentiality, security, and integrity of all WNCC information assets and systems including, but not limited to, hardware, software, telecommunications, networks, and data.

Scope

This policy applies to all members of the WNCC community including employees, regardless of their classification or status; enrolled students; community members; guests; and volunteers.

Policy

Usage of information technology resources is a privilege provided at the discretion of the Western Nebraska Community College and for the sole purpose of conducting official College business.

It is WNCC's policy that all users (employees, students, community members, guests, and volunteers) of information technology resources owned by or licensed services to the College will:

- Protect the integrity, availability, and confidentiality of information assets (including all digital, paper, on premise, and cloud assets) managed by or provided by the College.
- Protect information assets from unauthorized release or modification and from accidental or intentional damage or destruction.
- Protect technology assets such as hardware, software, telecommunications, networks (infrastructure), and data from unauthorized use.

All users are expected to follow all security guidelines as established by the IT Governance Committee in support of this policy.

Role of the Information Technology Department

The WNCC Information Technology Department is responsible for the oversight of the security guidelines as developed by the IT Governance Committee and will perform the following actions:

- Provide secure hardware, software, telecommunications, networks (infrastructure), and procedures for addressing the business needs of the college.
- Assure that appropriate security standards are considered and met when developing or procuring hardware, software, telecommunications, and networks (infrastructure).
- Assure that all user accounts are created, maintained, and terminated in accordance with the Information Technology User Administration Guide.
- Recognize and support the necessity of authenticating internal or external parties prior to granting access to sensitive information and applications.
- Develop and follow security standards for securing workstations, servers, telecommunications, and data access within its network.
- Follow security standards established for creating secure sessions for application access.
- Ensure all employees and student workers are trained in IT security awareness, and that technical staff receive the appropriate training commensurate with their job responsibilities.
- Review its IT security processes, procedures, and practices annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment.
- Perform annual security audits of systems and user permissions to ensure compliance and accuracy.
- Track IT assets to maintain life cycle, support, and licensing.
- Test disaster recovery scenarios on an annual basis.

Compliance Measurement

The Information Technology Department will verify and promote compliance to this policy through various methods, including but not limited to, reports, internal and external audits, and feedback from and to individuals and campus departments.

Exceptions

Any exception to this policy must be submitted to the IT Governance Committee. All approved exceptions will be reviewed on an annual basis by the IT Governance Committee.

Non-Compliance

Employees

An employee found to have violated this policy may be subject to network access revocation and personal disciplinary action, up to and including termination of employment.

Students

A student found to have violated this policy may be subject to disciplinary action.

Community Members, Guests, and Volunteers

A community member, guest, or volunteer found to have violated this policy may be restricted or banned from using college resources.

Procedures

The College President shall promulgate such procedures as may be necessary for the implementation of this policy.

Revising this Policy

This Board Policy supersedes any prior WNCC policy, procedure, guideline, or handbook on this subject matter.

If statutory provisions, regulatory guidance, or court interpretations change or conflict with this Board Policy, the Board retains the right to revise accordingly and for the changes to take effect immediately.

Adoption Date (and Board of Governor's Minutes Item Number): 2010
Revision Date (and Board of Governors' Minutes Item Number):
Prior Policy Number:
630.0300.10 Electronic Data Communication
Schedule for Review:
Divisions/Department Responsible for Review and Update: Information Technology
Sponsoring Division/Department: Administrative Services
Repeal Date:
Cross Reference:
Procedure(s) for Policy:
Related Policies/References: