BOARD OF TRUSTEES OF THE NEBRASKA STATE COLLEGES

ITEMS FOR DISCUSSION AND ACTION\FISCAL, FACILITIES AND AUDIT

ACTION: **First and Final Round Approval of Revisions to Board Policy 7003; Information Security Program**

Board Policy 7003 has been reformatted and revisions have been made to remove the Information Security Standards from the public facing website. The Information Security Standards will be made available to System Office staff and the Colleges' students, faculty and staff via secure authenticated intranets.

The System Office recommends approval of the Revisions to Board Policy 7003; Information Security Program.

ATTACHMENTS:

- Revisions to Board Policy 7003 (PDF)

Board of Trustees of the Nebraska State Colleges

Information Technology and Security

POLICY NAME: Information Security Program (ISP)

POLICY NUMBER: 7003

A. PURPOSE

The purpose of this policy is to establish an Information Security Program (ISP) for the State Colleges.

B. DEFINITIONS

None

C. POLICY

1. Importance of Information Security

The following shall constitute Board policy concerning information security.

- Each College and the System Office will have an Information Security Program (ISP) which ensures availability, confidentiality, and integrity of NSCS Technology Resources. Collectively, these programs will constitute the ~~Information Security Program (ISP) for the NSCS, and this~~ NSCS ISP which shall satisfy the Gramm-Leach-Bliley Act (GLBA) requirements for non-public financial data.
- The ISP will comply and align with other NSCS policies and shall be based on the NSCS Information Security Standards. ~~identified in this Policy.~~ Each College and the System Office shall develop, maintain, and apply the NSCS Information Security Standards which can be securely accessed from the following SharePoint sites:
  - CSC: NSCS Security Standards
  - PSC: NSCS Security Standards
  - WSC: NSCS Security Standards
  - NSCS: NSCS Security Standards
- Each President shall designate an individual responsible for each College ISP. The Chief Information Officer shall be the individual responsible for the System Office ISP and shall serve as the System Office Information Security Officer (SOISO).

- The SOISO shall coordinate with each President's designee to review the NSCS ISP ~~no less frequently than~~ annually, and to update as necessary.
- To protect all Technology Resources of the NSCS, this Policy and NSCS ISP applies to all faculty, staff, students, visitors, vendors, and contractors, and to all systems that access, store, or transmit NSCS data.
- In all Standards, the principles of least privilege, least functionality, and defense in depth, shall be applied.

~~**2.** Information Security Program Standards~~

~~Each College and the System Office shall implement and apply the following NSCS ISP Standards:~~

~~Standard 1: Definitions and Related Law, Policy and~~

~~Standard 2: References Responsibilities, Enforcement and~~

~~Standard 3: Exceptions Security Training and Awareness~~

~~Standard 4: Information Protection~~

~~Standard 5: Acceptable Use Policy~~

~~Standard 6: Computer and Network Security~~

~~Standard 7: Configuration and Change Management~~

~~Standard 8: Email~~

~~Standard 9: Physical Security~~

~~Standard 10: Technology Resources Acquisition~~

~~Standard 11: Payment Card Data Protection~~

~~Standard 12: HIPAA Security Rules and the HITECH Act Cloud~~

~~Standard 13: Computing~~

~~Standard 14: Information Systems Security Risk Management~~

~~Standard 15: Bring Your Own Device (BYOD)~~

~~Standard 16: Incident Management~~

FORMS / APPENDICES:

None

SOURCE:

Policy Adopted: November 2019

Policy Revised: January 2020, April 2022, January 2023