POLICY 8400

INFORMATION SECURITY

Policy Category: Information Technology
Area of Administrative Responsibility: Information Technology Services
Board of Trustees Approval Date:
Effective Date: June 139, 2023
Amendment History: N/A
Contents:

PURPOSE

The purpose of this policy is to assist the Nassau Community College (NCC) personnel in fulfilling responsibilities relating to the protection of information assets and to comply with regulatory and contractual requirements involving information security and privacy.

This policy framework is based on guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-171.

Roles, responsibilities and procedures will be established to ensure the maintenance and a continual improvement of NCC's Information Security Program. Although no set of policies and procedures can address every possible scenario, this framework, taken as a whole, provides a comprehensive governance structure that addresses key controls in all known areas needed to provide for the confidentiality, integrity, and availability of the organization's information assets. This framework also provides administrators guidance necessary for making prioritized decisions, as well as justification for implementing organizational change.

The scope of this policy includes all information assets governed by the organization. All faculty, staff, students, student workers, and service providers who have access to or utilize assets of the

organization, including data at rest, in transit or in process shall be subject to these requirements. This policy applies to:

- All information assets and IT resources operated by NCC.
- All information assets and IT resources provided by NCC through contracts, subject to the provisions and restrictions of the contracts; and
- All users of NCC information assets and IT resources.

DEFINITIONS

A. **Associate Vice President for Information Technology Services (AVP ITS):** The AVP ITS or his or her designee is accountable for the implementation of the Information Security Program including security policies, standards, and procedures; and security compliance including managerial, administrative, and technical controls. The AVP ITS is to be informed of information security implementations and ongoing development of the Information Security Program design.

B. **Information Security Qualified Individual (IS QI):** The IS QI, or alternatively a managed cyber-security provider contracted by NCC, is responsible for the development, implementation, and maintenance of a comprehensive Information Security Program for NCC. This includes security policies, standards, and procedures which reflect best practices in information security.

C. **Information Security Program (ISP):** A collection of initiatives that form the basis for any cyber security plan involving confidential data.

D. **Family Educational Rights and Privacy Act (FERPA):** The Family Educational Rights and Privacy Act of 1974, as amended, ("FERPA" or "Act") was designed primarily to ensure that educational records would be maintained in confidence and available to eligible students for inspection and correction when appropriate and that any such recorded information would not be made freely available to individuals outside the school without consent or as otherwise allowed by law.

E. **Gramm-Leach-Bliley Act of 1999 (GLBA):** U.S. law that applies to financial institutions and includes privacy and information security provisions that are designed to protect consumer financial data. This law applies to how higher education institutions collect, store, and use student financial records, records regarding tuition payments and/or financial aid, containing personally identifiable information.

F. **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 2:** Addresses protection for Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations. As defined, CUI could include data received as part of a research grant or data received to conduct business, e.g., student financial aid information.

G. **Written Information Security Program (WISP):** A document detailing a description of the complete manner in which a company implements the administrative, technical, or physical safeguards in place to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle member information.

POLICY

A. STATEMENTS:

The NCC ISP is framed on NIST and controls implemented based on the Center for Internet Security (CIS) Critical Security Controls priorities. This policy is further defined by control standards, procedures, control metrics, and control tests to assure functional verification.

The NCC ISP is based on NIST Special Publication 800-171. This publication is structured into multiple control groupings, herein referred to as Information Security Standards. These Standards must meet all statutory and contractual requirements, including those requirements mandated by GLBA and FERPA.

The Information Security Program is led by the AVP ITS, and as delegated to the IS QI.

Cabinet Responsibilities:

a. Ensures the ISP's continuing adequacy, effectiveness, and efficiency.
b. Responsible for the final determination of risk acceptance or mitigation, should there be conflict of opinions between the Information Security Program, the IS QI and/or the AVP ITS.

The responsibilities of the AVP ITS, and as delegated to the IS QI, shall include:

a. Report the status and direction of the ISP to the Cabinet.
b. Review and recommend strategies related to the ISP.
c. Review and approve information security policies and standards, and other supporting documentation.
d. Approve and maintain oversight of the risk management process, including risk assessment methodology, risk acceptance criteria, residual and accepted risks.
e. Review the Business Continuity Plan.
f. Perform a full review of the WISP.
g. Approve actions to resolve issues identified during reviews in an effective and timely manner.
h. Advise on year-over-year goals and priorities for the ISP.
i. Ensure compliance with all ISP requirements, policies, standards, and procedures.
j. Review findings results from various audits and assessments.
k. Oversee implementation of remediation plans to ensure high priority risks have been resolved.

ENFORCEMENT

Enforcement is the responsibility of NCC's President or AVP ITS. Users who violate this policy may be subject to discipline up to and including termination consistent with the terms and conditions of any applicable Collective Bargaining Agreement, if any. The institution may temporarily suspend an account when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the institution or other computing resources or to protect NCC from liability.

Exceptions to the policy may be granted by the AVP ITS, or by his or her designee. All exceptions must be reviewed annually.

APPLICABLE LEGISLATION AND REGULATIONS

The Gramm - Leach Bliley Act (GLBA)

Family Educational Rights and Privacy Act (FERPA)

General Data Protection Regulation (GDPR)

New York State Information Security Breach and Notification Act

NIST 800-171 Rev 2

FIPS-199

RELATED REFERENCES, POLICIES, PROCEDURES, FORMS AND APPENDICES

POLICY 8100 Use of College Computer Resources

POLICY 8200 Network Security

POLICY 8300 Email

SUNY Policy 6608, Information Security Guidelines: Campus Programs & Preserving Confidentiality

SUNY Policy 6900, Information Security Policy