

## **POLICY 8400**

### **INFORMATION SECURITY**

**Policy Category:** Information Technology

**Area of Administrative Responsibility:** Information Technology Services

**Board of Trustees Approval Date:** June 13, 2023

**Effective Date:** June 9, 2023

**Amendment History:** N/A

**Contents:**

[Purpose](#)

[Definitions](#)

[Policy](#)

[Enforcement](#)

[Applicable Legislation and Regulations](#)

[Related References, Policies, Procedures, Forms and Appendices](#)

#### **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

nt

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



**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\*\*](#)