Information Security Management System

Policy Number:	**2808**
Key Process Area:	**Information Technology**
Owner:	**VP FA**
Current Approved Date:	**Aug 05, 2020**

POLICY STATEMENT

New Brunswick Community College (NBCC) is committed to building increased awareness and a shared responsibility for information security management throughout the organization. NBCC has adopted and established a commitment to satisfy International Organization for Standardization/International Electro-technical Commission's ISO/IEC 27001:2013 requirements for developing an effective Information Security Management System (ISMS).

PURPOSE

The purpose of this policy and the related standards and procedures is to set forth security practices necessary to protect the Confidentiality, Integrity and Availability of NBCC's network, systems, data and organizational reputation. An environment where all cybersecurity risk is eliminated is neither reasonable nor cost-effective. The ISMS is designed to minimize risk to the College operations, to ensure compliance with legislative requirements and to ensure that information is used for its intended purpose.

SCOPE AND LIMITATIONS

The scope of this policy includes all information technology assets governed by NBCC. All staff, students and service providers who have access to or utilize information assets of NBCC, including data at rest, in transit, or in process shall be subject to these requirements. All software applications running on devices, physical or virtual, where NBCC data is being housed, developed, provisioned, or managed by staff, student employees, contractors, and vendors are subject to this policy. The policy statements contained herein and in the supporting reference documents: Government Information Technology Systems Security Policy Standards and Directives should be considered minimum baseline requirements for providing a secure environment for developing, implementing, and supporting information technology infrastructure and systems. This policy is intended to comply with all applicable laws and regulations. In the event of a conflict, applicable laws and regulations shall take precedence.

1.0 DEFINITIONS

ISO/IEC 27001:2013 Certification

- a multi-phase external audit process defined by the ISO/IEC standards. Successful completion of this process results in the ISMS being certified compliant with ISO/IEC 27001:2013

Information Security Management System

- a set of policies, standards and systems to manage risks to information assets, designed and implemented to ensure acceptable levels of risk.

Corrective Actions

- corrective actions are steps that are taken to remove the causes of an existing non-conformity or undesirable outcomes. Corrective action will target the root cause so that the non-conformity or undesirable situation do not re-occur.

Non-conformity
- the certification audit will grade the audit criteria as 'conforms or non-conforms.' There are two types of non-conformities:

- ***Major Non-conformity***—A major breakdown or failure to fulfill one or more requirements of the ISMS
- ***Minor Non-conformity***—A single identified lapse, which would not raise significant doubt as to the capability of the ISMS to achieve the security standards and objectives of the organization.

2.0 IMPLEMENTATION

2.1 Requirements

Leadership Commitment: NBCC Senior Executive Team shall demonstrate leadership and commitment with respect to the ISMS.

Information Security Management: NBCC Information Security Team will develop an annual information security plan.

Risk Management: The development and maintenance of the ISMS is based on NBCC enterprise risk management principles and risk assessment methodologies provided by the ISO/IEC Standard.

Statement of Applicability: NBCC Information Security Team will document the information security controls selected for implementation, identify progress, and provide required justification for exclusions.

Document Control: Departments and teams are responsible for managing and updating their procedures and documentation in the ISMS documentation library each year. When a new procedure, or version of a procedure, is issued for inclusion in the ISMS, it will include a document revision level, contact information, the date and time of last update or the correction report and data classification if protected.

Internal Audit: Internal audits of the Information Security Management System shall be conducted annually.

Management Reviews: Management reviews will be conducted by the Information Security Team at various intervals.

Non-conformity and corrective actions: ISMS nonconformities, amendments and corrections will be documented and maintained by the NBCC Information Security Team. Recipients of any of the ISMS corrective action reports must submit a corrective action plan to the ISMS manager. Corrective action plans will be managed by the Information Security Team.

Records Retention: Unless specified otherwise, ISMS records will be maintained electronically by the Information Security Team according to the NBCC Classification Plan and Retention Schedules.

Training: All staff, students and service providers included in the ISMS scope shall be made aware of the relevance and importance of their information security activities and how they contribute to the achievement of the goals and objectives. Information Solutions will provide training for all ISMS participants.

2.2 Roles and Responsibilities

Individuals who are authorized to access institutional data shall adhere to the appropriate Roles and Responsibilities, as defined in this policy. These roles and responsibilities are defined within the ISMS as follows:

- **Lead Internal Auditor:** The Lead Internal Auditor is responsible for managing and performing internal audits, as required by the maintenance and optimization section of the ISMS. An internal audit is a systematic, independent, and documented process of collecting audit evidence and its objective assessment in order to determine whether the audit criteria have been met and to what degree.

- **Corporate Information Security Officer (CISO):** The Corporate Information Security Officer is a management-level employee of NBCC who oversees the College's Information Security Management Program.

- **Data Steward:** A Data Steward is a senior level employee of the College who oversees the lifecycle of one or more sets of NBCC's data.

- **Data Custodian:** A custodian is an employee of the College, who has administrative and/or operational responsibility over NBCC's data.

- **User:** A user is any employee, or third-party agent of the College, who is authorized to access NBCC's Information Systems and/or NBCC's data.

2.3 Enforcement

Violations of this policy may result in disciplinary action, suspension or loss of the violator's use privileges, with respect to NBCC's data and College owned systems. Additional administrative sanctions may apply up to and including termination of employment or third-party agent status with the College. Civil, criminal and equitable remedies may also apply.

3.0 OTHER RELATED DOCUMENTS

Use of Mobile Devices Standard Operating Procedure (2808.5231)
NBCC - ISMS Acceptable Use of Technology Resources (2808.4750)
NBCC Information Security Data Classification Guidelines (5306.5278)