UNBC UNIVERSITY OF
NORTHERN BRITISH COLUMBIA

# Policy

## INFORMATION SECURITY POLICY

**Number:** IM 2
**Classification:** Information Management
**Approving Authority:** Board of Governors
**Designated Executive Officer:** President
**Effective Date:**
**Supersedes:** N/A
**Date of Last Review/Revision:** January 2025
**Mandated Review Date:** January 2031

**Associated Procedures: [Insert the number and title of the policy's corresponding procedures].**

## TABLE OF CONTENTS

## 1.0 BACKGROUND

UNBC's approach to Information Security directly impacts students, employees, and its commitment to strive for teaching, learning, and research excellence and impact; therefore, the University takes a systematic approach to establishing, implementing, operating, monitoring, maintaining, reviewing, and improving its Information Security.[i] UNBC leadership is committed to satisfying all of the applicable requirements related to Information Security [ii] and  to a process of continual improvement of the Information Security Management System.[iii]

## 2.0 PURPOSE

The purpose of this policy is to establish responsibilities at UNBC for developing and implementing a framework for managing the security of the University's information assets, in accordance with BC's *Freedom of Information and Protection of Privacy Act* (FIPPA), and the International Organization for Standardization's (ISO) standards on Information Security, Cyber Security, and privacy protection.[iv]

## 3.0 PRINCIPLES

The principle of preserving Confidentiality, Integrity and Availability of information must inform all UNBC's Information Security objectives.[v]

## 4.0 SCOPE

4.1 This policy applies to all data and information management systems in the custody or control of the University, and to all University Employees, Officers of the University, Volunteers, and Service Providers who have access to University Information Systems.

4.2 This policy does not apply to data collected, created, processed, or stored as part of research activities, or information management systems (IMS) for research data, if the data is not stored in a University IMS.

## 5.0 DEFINITIONS

5.1 **Administrator** means an individual engaged in directing and overseeing a distinct program, unit, office, or department of the University (e.g., manager, director, dean, etc.).

5.2 **Availability** means ensuring timely and reliable access to and use of information.[vi]

5.3 **Confidentiality** means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.[vii]

5.4 **Controls** are processes, policies, devices, practices, or other conditions and or actions that maintain and/or modify risk.[viii]

5.5 **Confidential Information** means any information that is not intended to be made available or disclosed to unauthorized individuals, entities, or processes[ix]

5.6 **Cyber Security** is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its Availability, Integrity, authentication, Confidentiality, and nonrepudiation.[x]

5.7 **Information Security Management System** is a part of the overall information management system that utilizes a risk management approach used to establish, implement, operate, monitor, review, maintain and improve Information Security.[xi]

5.8 **Information Security** is the preservation of Confidentiality, Integrity and Availability of information.[xii]

5.9 **Information Security Incident** is a single or series of unwanted or unexpected Information Security events that have a significant probability of compromising business operations and threatening Information Security.[xiii]

5.10 **Information System** is a set of applications, service, information technology assets, or other information-handling components.[xiv]

5.11 **Integrity** means guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.[xv]

5.12 **Sensitive Information** is any information that needs to be protected from unavailability, unauthorized access, modification or public disclosure because of potential adverse effects on an individual or UNBC.[xvi]

# 6.0 POLICY

## 6.1 Risk Identification and Assessment

6.1.1 The Chief Information Security and Privacy Officer (CISPO) is responsible for identifying and assessing Information Security risks at UNBC, including, but not limited to, the following:
i. conducting Information Security Risk Assessments;
ii. cyber risk threat detection and response measures;
iii. investigating known or suspected Information Security Incidents; and
iv. identifying information assets and corresponding Information Security requirements.[xvii]

6.1.1 All employees are responsible for reporting known or suspected Information Security threats (E.g. phishing, malware, compromised credentials) to the CISPO.

6.1.3 An Information Security assessment must be initiated prior to:[xviii]
i. the implementation of any new Information System, or significant changes to the existing Information System that collects or processes Sensitive Information.

6.1.4 An Information Security assessment must be initiated after:[xix]
i. a change in the threat landscape (e.g. a new type of Information Security attack) has occurred;
ii. an audit of existing safeguards identified a deficit in the efficacy of existing safeguards; or the CISPO or designate determines that an Information Security risk assessment is required.

6.1.5 A completed Information Risk Assessment is classified as confidential and only shared with the Chief Information Officer (CIO) and UNBC employees involved in risk treatment and must include the following:
i. identification and description of Information Security risks associated the loss of Confidentiality, Integrity and Availability of information;[xx]
ii. an assessment of potential consequences and likelihood of failing to adequately preserve Confidentiality, Integrity, and/or Availability of information;[xxi] and
iii. an evaluation of each identified Information Security risk and whether it satisfies risk acceptance criteria or must be prioritized for risk treatment.[xxii]

6.2 Risk Treatment and Information Security Controls

6.2.1 The CIO or designate is responsible for:

i. the protection of Information Systems and other associated assets;[xxiii]and

ii. the integration of the Information Security Management System requirements into UNBC's data processes.[xxiv]

6.2.1 All employees are responsible for the supporting the Integrity of data within UNBC managed Information Systems and are responsible for applying Information Security in accordance with the Information Security Controls listed in the specific information assets *Standards of Use*, released by the CIO. [xxv]

6.2.3 Once an Information Security risk assessment has been completed, the CIO or designate is responsible for selecting the appropriate Information Security risk treatment option including:[xxvi]

i. deciding not to start or continue with the activity or initiative that gives rise to the risk; or

ii. identifying technical, physical, or administrative Controls to manage the likelihood or severity of the Information Security risk. [xxvii]

6.2.4 As part of Information Security risk treatment, the CIO or designate is responsible for documenting:[xxviii]

i. all necessary Controls,

ii. justification for the inclusion of the Controls, and

iii. the implementation status of the Controls.

6.3 Competency Based Training

6.3.1 Administrators are responsible for determining the requisite competencies individuals must have in order for them to access University Information Systems that their unit manages.[xxix]

6.3.2 Administrators ensure that individuals have the appropriate education or training prior to accessing Information Systems they are responsible for managing, and, where necessary, provide training to ensure competency.[xxx]

6.3.3 Administrators are responsible for retaining all relevant documentation of education or training. [xxxi]

### 6.4 Monitoring and Auditing of Information Security Processes and Controls

6.4.1 The CISPO is responsible for maintaining an Information Security Risk Registry, and routinely verifying the suitability and efficacy of safeguards and Controls used to treat the identified risks.[xxxii]

6.4.2 If the routine verification process identifies a deficit in the suitability or efficacy of safeguards and Controls, then the CISPO is responsible for re-initiating an Information Security risk assessment.

6.4.3 The Office of Data Governance, Privacy, and Information Security coordinates an external audit of UNBC's Information Security Management Systems every 3 years as part of a commitment to continual improvement.

6.4.4 In preparation of an external audit, the Office of Data Governance, Privacy and Information Security is responsible for the following:

i. solicitating feedback from the University community on the University's current information security program;
ii. defining the audit scope and criteria;[xxxiii]
ii. selecting auditors who ensure an objective audit process;[xxxiv]and
iii. ensuring that the results of the audit are shared with the Board of Governors. [xxxv]

## 7.0 REPORTING

The CISPO is responsible for reporting annually to the Board of Governors on the progress of Information Security objectives that were identified in the Information Security Management System audit.[xxxvi]

## 8.0 AUTHORITIES AND OFFICERS

The authorities and officers for this policy are as follows:
Approving Authority: Board of Governors
Designated Executive Officer: President
Procedural Authority: President
Procedural Officer: Chief Information Security and Privacy Officer

## 9.0 RELEVANT LEGISLATION

9.1 *Freedom of Information and Protection of Privacy Act* (FOIPPA)

9.2 NIST Cybersecurity Framework (CSF) 2.0: Providing guidelines for managing cybersecurity risks, ensuring comprehensive protection across all device categories.

9.3 NIST SP 800-53 Rev5: Security and Privacy Controls for Information Systems and Organizations

9.4 ISO/IEC 27001 Information security, cybersecurity and privacy protection - Information security management systems – Requirements

9.5 ISO/IEC 27002 Information security, cybersecurity and privacy protection - Information security controls

9.6 ISO/IEC 27005 Information security, cybersecurity and privacy protection - Guidance on managing information security risks

## 10.0 RELATED POLICIES AND OTHER ASSOCIATED DOCUMENTS

10.1 *Protection of Privacy Policy*

10.2 *Records Management Policy*

10.3 *Acceptable Use Policy (2012)*

[i] ISO/IEC 27000:2018.4.2.1
[ii] ISO/IEC 27001:2022. sect 5.2.c.
[iii] ISO/IEC 27001:2022. sect 5.2.d
[iv] ISO/IEC 27000:2018,0.1.
[v] ISO/IEC 27002:2022. Sect 5.1
[vi] NIST SP 800-12 REV 1. Sect 1.4.
[vii] NIST SP 800-12 REV 1. Sect 1.4.
[viii] ISO/IEC 27005:2022, 3.1.15.
[ix] ISO/IEC 27002:2022.3.1.7
[x] NIST SP 1800-25. B-1
[xi] ISO/IEC 18598:2016. sect 3.1.23.
[xii] ISO/IEC 27000:2018,3.28.
[xiii] ISO/IEC 27005:2022, 3.1.12
[xiv] ISO/IEC 2700:2018, 3.37
[xv] NIST SP 800-12 REV 1. Sect 1.4.
[xvi] ISO/IEC 27002:2022.3.1.33

[xvii] ISO/IEC 27000:2018.4.5.1.a
[xviii] ISO/IEC 27005:2022.9.1.
[xix] ISO/IEC 27002:2022, 7.1
[xx] ISO/IEC 27002:2022, 7.2.1.
[xxi] ISO/IEC 27002:2022, 7.3.
[xxii] ISO/IEC 27002:2022, 7.4.
[xxiii] ISO/IEC 27002:2022, 5.2.b
[xxiv] ISO/IEC 27001:2022. sect 5.1.b
[xxv] ISO/IEC 27002:2022, 5.4.c.
[xxvi] ISO/IEC 27005:2022.8.2
[xxvii] ISO/IEC 27005:2022. 8.1.
[xxviii] ISO/IEC 27005:2022.8.5.
[xxix] ISO/IEC 27001:2022.7.2.a
[xxx] ISO/IEC 27001:2022.7.2.b
[xxxi] ISO/IEC 27001:2022.7.2.c
[xxxii] ISO/IEC 27000:2018.4.5.7
[xxxiii] ISO/IEC 27001:2022.9.2.2.a
[xxxiv] ISO/IEC 27001:2022.9.2.2.b
[xxxv] ISO/IEC 27001:2022.9.2.2.c
[xxxvi] ISO/IEC 27001:2022. sect 5.3.b