INFORMATION SECURITY POLICY

Approved: April 20, 2017

Policy Officer: Associate Vice-President, ITS
Related Information: Appendix A: List of Information Security Related Documents

1) VISION

Information security enables an environment that balances the needs of teachers, students, researchers and administrators with the protection of information resources from unauthorized change, disclosure and access.

2) PURPOSE

Assign and authorize roles and responsibilities for information security at UNB and the guiding principles for implementation.

3) SCOPE

a) UNB community
b) UNB information systems and information resources

4) OUT OF SCOPE

a) Paper-based records
b) Special-purpose library collections and records including University Archives
c) Intellectual property owned by a UNB community member that is not under UNB custody or control. This may be defined through collective agreements.

5) DEFINITIONS

a) **Administrative Authority** means the UNB community member with functional stewardship/custody of UNB information resources and/or administrative responsibility for Units such as Vice-Presidents, Associate Vice-Presidents, Deans, Chairs, Directors, the University Secretary and other unit heads.

b) **Custody / Stewardship** is the responsibility for the physical possession, care, security, classification, storage, retention, and disposal of university records for legitimate purposes and for institutional compliance with legislation, regulation, contracts (including research agreements), and collective agreements. The University maintains control over a university record even if it is in the custody of a third party or an off-campus employee. The usage of terms is interchangeable.

c) **Information Resources** means electronic records/information and infrastructure owned by, under the control of, or in the custody of UNB. This includes but is not limited to data, database records, electronic services, network services, intellectual property, software, computers, mobile devices, information systems, UNB network connected devices and services.

d) **Information Security** means the protection of UNB information resources against disclosure to unauthorized persons (confidentiality), improper modification (integrity) and non-access when required (availability).**Information Security Incident** means any adverse event whereby an information resource is threatened, improperly modified, used for an unintended purpose, or has had an unauthorized access.

e) **Information Security Program** means the strategies, initiatives, projects, policies, standards, procedures and other activities required to achieve the Information Security Policy vision.

f) **Information System** means the UNB people, processes, organization, and facilities that collect, process, store, display, transmit, and disseminate information resources.

g) **Providers are** UNB community members who design, manage, and operate UNB information resources such as technical support employees, project managers, system designers, application programmers, or system administrators.

h) **Threat** means a circumstance or event (e.g., an action or lack of action a person should reasonably be expected to know) with the potential to subject information systems or information resources to unauthorized change, disclosure or access.

i) **Unit** means a group of people, linked by a common interest or purpose, including but not limited to, faculties, departments, divisions, schools, institutes and centres.

j) **UNB Community** includes:
   i) All employees including but not exclusive to full and part-time faculty and librarians, support staff, administrators, teaching assistants;
   ii) All persons holding non-employment appointments including but not exclusive to adjuncts, honorary research associates, post-doctoral fellows, visiting professors and stipend lecturers;
   iii) All students including those in non-employment appointments, and student employees; and
   iv) Any other person who has access to UNB records for the purpose of conducting administrative, operational, teaching, learning or research functions or activities at UNB.

k) **UNB Records** are records/information owned by or in the custody or control of UNB.

l) **Vulnerability** means an identified security weakness in an information resource or information system that could lead to an information security incident.

The *Policy for the Provision of Access to Information* is the source of the following definitions.

n) **Control** is the authority to determine how a record is classified, used and to whom it is disclosed throughout its life cycle. The University has control over all University records. It is considered to have control over a university record even if it is in the custody of a consultant or an off-campus employee.

o) **Record / Information** is a record of information in any form, and includes information that is written, photographed, recorded or stored in any manner, on any storage medium or by any means, including by graphic, electronic or mechanical means, but does not include electronic software or any mechanism that produces records.

p) **Third Party** is a person, group of persons or an organization other than the University.

6) **ROLES AND RESPONSIBILITIES:**

a) **Administrative Authorities** secure the information resources for which they are responsible.

b) Information Technology Services

i) advance data governance and an information security program across UNB
ii) ensure appropriate collaboration and consultation occur
iii) secure technology based information resources for which ITS is responsible
iv) advance IT security awareness and education
v) develop tools and resources to facilitate implementation of information security responsibilities
vi) coordinate responses to electronically based information security incidents, threats and vulnerabilities

c) Providers

i) Provide input on and be knowledgeable about information security procedures, standards and guidelines for which they are stakeholders
ii) analyze potential threats and the feasibility of various security arrangements in order to provide recommendations to Administrative Authorities
iii) apply information security standards

d) UNB Community:

i) comply with related information security procedures and standards
ii) protect the information resources for which they are responsible and to which they have access
iii) consult, as necessary, with the appropriate administrative authority regarding this policy and its supporting procedures, standards and guidelines

7) GUIDING PRINCIPLES FOR IMPLEMENTATION

a) Consult and collaborate with UNB community stakeholders
b) Consciously apply the lens of teachers, students, researchers and administrators to all information security standards of procedures, standards and guidelines
c) Prioritize work based on benefits, risk (impact & probability), resource (cost and staff availability) and potential mitigations
d) Balance individual privacy with the need to identify threats and vulnerabilities
e) Balance access requirements and ease-of-use with the need for security
f) Leverage existing UNB security standards and industry standard information security practices adapted for UNB

8) COMPLIANCE AND INTERPRETATION

Administrative Authorities, Information Technology Services and University Secretariat share responsibility for the interpretation of the Information Security Policy.

Administrative Authorities and Information Technology Services oversee compliance with Information Security procedures and standards based on the information systems and resources for which they are responsible.

The appropriate University Vice President receives appeals.