UNIVERSITY OF MANITOBA

UNIVERSITY OF MANITOBA
POLICY

Policy:	**INFORMATION SECURITY**
Effective Date:	February 3, 2020
Revised Date:	
Review Date:	February 3, 2030
Approving Body:	Board of Governors
Authority:	*The University of Manitoba Act*
Responsible Executive Officer:	Vice-President (Administration)
Delegate: (If applicable)	Chief Information Officer
Contact:	Director, Information Security and Compliance
Application:	All students, employees, and all individuals holding an academic appointment (even if unpaid), Academic Staff, teaching staff, researchers, administrative and other staff, all employee groups, post-doctoral fellows, adjunct appointments, nil-salaried appointments, senior scholars, professor emeriti, University retirees, External Parties, volunteers, contractors and suppliers, Board of Governors members, Senate members, and Faculty/College/School Councils

Part I
Reason for Policy

1.1 Access to University networks, computing facilities, University Information, Academic Information and Information Systems are necessary for the University Community to do their work. The policy is necessary to ensure the security, protection, and privacy of all Information and University Information Systems and to identify responsibility and accountability for adopting and applying the Information Security Policy, Procedure and Standards.

1.2 Information and the supporting Information Systems used to process, store, retrieve, and transmit Information plays a vital role in the conduct and success of the University of Manitoba's teaching, learning, research, outreach and Business Processes. As more Information is used and shared by the University Community,

both within and outside the University, a focused effort must be made to protect Information.

1.3 Nothing in this Policy is meant to infringe or impede upon the academic freedom of Academic Staff at the University, nor to monitor, censor or restrict the use of Academic Information at the University. Academic Information differs in nature from other Information retained on the University's Information Systems and may be the Intellectual Property of Academic Staff.

1.4 Confidentiality Protection, Integrity Protection, and Availability Protection of Information are essential to maintaining the University's reputation, legal position, and ability to conduct its operations. Failure to protect the University of Manitoba's Information could have financial, legal, and ethical ramifications.

Part II
Policy Content

2.1 The definition/terms for the purpose of this Policy are as follows:

(a) **"Academic Information"** includes information and data that is retained on the University's Information System for a research, scholarly or educational purpose, and can exist in many forms including but not limited to written or printed on paper, stored electronically, recorded on magnetic disk or tape, or spoken in conversation. Academic Information may be the Intellectual Property of Academic Staff.

(b) **"Academic Staff"** refers to all individuals whose primary assignment is instruction, research, and/or service/academic administration. This includes employees who hold an academic rank such as professor, associate professor, assistant professor, instructor, lecturer, librarian, or the equivalent of any of those academic ranks. The category also includes a dean, director, associate dean, assistant dean, chair or head of department, visiting scholars, senior scholars, and those holding unpaid academic appointments, insofar as they perform instructional, research, and/or service/academic administrative duties.

(c) **"Availability Protection"** is protection to ensure that access to Information and Information Systems is provided in a timely manner.

(d) **"Business Processes"** are a collection of related, structured activities or tasks that in a specific sequence produces a service or product (serves a particular business goal such as receiving orders, invoicing, shipping products, updating employee information, or setting a budget).

(e) **"Confidentiality Protection"** is defined as protection to ensure that Information and Information Systems are accessible only to those persons authorized to have access.

(f) **"Cyber Attack"** is an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the Information and/or Information Systems; or stealing Information.

(g) **"Exceptions"** are the circumstances under which an Information Owner has identified the inability to adhere to the Information Security Policy, Procedure or Standards, and if the Exception is approved, has formally accepted the risks associated with non-compliance.

(h) **"Executive Staff"** is defined as the Executive or Administration excluded Academic Staff, including the President, Vice-Presidents, Associate Vice-Presidents, Vice-Provosts, Comptroller, and Executive Directors.

(i) **"External Parties"** are external to the University. This includes business partners, vendors, third party services, contractors, consultants, guests, volunteers and those affiliated with the University that are not also students or employees accessing or using Information and Information Systems.

(j) **"Information**" includes all records and data in the custody and/or control of the University and can exisit in many forms including but not limited to written or printed on paper, stored electronically, recorded on magnetic disk/ or tape, or spoken in conversation.

(k) **"Information Owners"** are those individuals who have primary responsibility for Business Processes through which Information is received, created, stored, handled, or discarded, whether in physical or electronic form. When Information spans across multiple Business Processes, Information may have multiple Information Owners under this Policy.

(l) **"Information Security and Compliance"** is a section within Information Services and Technology (IST), led by the Director of Information Security and Compliance.

(m) **"Information Security Breach"** is an incident in which sensitive, private, confidential or otherwise protected Information has been accessed, disclosed and/or released in a manner that is not authorized by the Information Security Policy, Procedure or Standards. Information Security breaches can involve Information, University Information, Academic Information or Intellectual Property.

(n) **"Information Security Standards"** are the compliance standards authored by Information Security and Compliance to provide guidance to the University Community.

(o) **"Information Systems"** are the technology and data owned, controlled and/or used by the University to create, maintain and disseminate Information which include, but are not limited to, computer systems and networks.

(p) **"Information Trustees"** are the Executive Staff at the University, along with the deans, department heads and directors of the individual Academic Faculties and Administrative Units.

(q) **"Information Users"** are individuals who have been granted access to specific Information resources in the performance of their assigned duties. All members of the University Community are Information Users of some part of the University of Manitoba's Information resources, even if they do not have responsibility for managing those resources.

(r) **"Integrity Protection"** is protection and safeguards to ensure that Information is accurate and complete.

(s) **"Intellectual Property"** is defined as all original literary, dramatic, musical and artistic works, performances, communication signals and sound recordings capable of Copyright protection under the *Copyright Act* (Canada).

(t) **"IST (Information Services & Technology)"** is an Administrative Unit reporting to the Vice-President (Administration). IST provides information technology and communication resources and expertise in support of the educational, research and administrative activities of the University. The department is comprised of four sections: Information Security and Compliance; Planning and Governance; Client Services; and Technology Services.

(u) **"University Community"** means all students, employees, and all individuals holding an academic appointment (even if unpaid), Academic Staff, teaching staff, researchers, administrative and other staff, all employee groups, post-doctoral fellows, adjunct appointments, nil-salaried appointments, senior scholars, professor emeriti, University retirees, External Parties, volunteers, contractors and suppliers, Board of Governors members, Senate members, and Faculty/College/School Councils.

(v) **"University Information"** includes all records and data in the custody and/or control of the University which are used in Business Processes, and exists in many forms including but not limited to written or printed on paper, stored electronically, recorded on magnetic disk or tape, or spoken in conversation.

2.2 The primary purpose of this policy is to:

(a) ensure the protection of all Information and Information Systems (including but not limited to all computers, mobile devices, networking equipment, software and Information) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems;

(b) ensure Information Users are aware of, and comply with, any current and relevant provincial and federal legislation;

(c) minimize the University's exposure to Cyber Attacks;

(d) ensure that Information Users understand their own responsibilities with respect to Confidentiality Protection, Integrity Protection and Availability Protection of the Information, and Information Systems they handle; and

(e) protect the University from liability or damage through misuse of its Information and Information Systems.

2.3 Policy Statement:

The University is committed to protecting the University Information, Academic Information, and Information Systems used in its teaching, learning, research, outreach and Business Processes and the Information User groups we support, including the University Community and the public. The use of Information Systems imposes certain responsibilities and obligations on users of the systems. Such use is granted by the University of Manitoba subject to compliance with University policies and procedures as well as with provincial and federal laws.

2.4 This policy applies to:

(a) the University Community who access or in any way make use of University Information Systems;

(b) the protection and security of Academic Information on University Information Systems, but not as to the content (subject to compliance with relevant legislation and University policies or procedures) or ownership of Academic Information stored on the University Information Systems;

(c) all Information and Information Systems, including those used by the University under license or contract. Information and Information Systems exists in many forms and recorded on any media, and all computer hardware, computer software, and communications networks owned or operated by the University or on the University's behalf; and

(d) any device, regardless of ownership and including equipment privately owned by University Community members (e.g., laptop computers, tablet computers, smart phones, USB storage devices, etc.), but only with respect to the ways in which they connect to or access Information and Information

Systems and the activities they perform with the Information and Information Systems.

Part III
Accountability

3.1 The Office of Legal Counsel is responsible for advising the President that a formal review of this Policy is required.

3.2 The Vice-President (Administration) is responsible for the implementation, administration and review of this Policy.

3.3 Information Trustees are accountable to ensure the exercise of due diligence in protecting all Information that falls within their respective Faculties or Administrative Units by:

(a) understanding and mitigating risks associated with the loss of Confidentiality Protection, Integrity Protection, or Availability Protection of University Information and Information Systems used in the Faculty or Administrative Unit;

(b) determining, in coordination with other responsible Administrative Units (e.g., Office of Legal Counsel, Information Security and Compliance, Access and Privacy Office, Audit Services, etc.) and through participation in risk assessment activities, the appropriate levels of protection for Information (including Academic Information) and Information Systems that are owned and managed within their areas;

(c) actively promoting and visibly supporting Information security awareness in the Faculty or Administrative Unit and ensuring that all Information Users participate in relevant security training; and

(d) ensuring that the Information Security Procedure and Standards that are referred to by this Policy are communicated to and followed by the Faculty or Administrative Unit.

3.4 Information Owners are responsible for:

(a) Assigning University Information classification categories;

(b) maintaining records of University Information in all classification categories, their locations, and individuals whom have access to them;

(c) reviewing and authorizing Information User access to Information and Information Systems based on Business Processes;

(d) reviewing and authorizing privileged Information User access to Information Systems;

(e) controlling changes to University Information and Information Systems;

(f) defining recovery time objectives and recovery point objectives for University Information, Academic Information and Information Systems and ensuring that backup and recovery processes can meet those objectives;

(g) ensuring compliance with applicable record retention policies and schedules;

(h) documenting Exceptions that identify risks and controls due to the inability to follow the Information Security Policy, Procedure and Standards in their respective Faculties and Administrative Units;

(i) ensuring that Information and Information Systems that are no longer needed are disposed of securely; and

(j) ensuring that essential Business Processes continue in the event that the existing Information and Information Systems are unavailable.

3.5 Information Users have a responsibility to:

(a) review, understand, comply, and conduct themselves in a manner consistent with the Information Security Policy, Procedure or Standards;

(b) use Information Systems only for authorized purposes as defined by the University;

(c) comply with the terms of software licenses;

(d) comply with legal and regulatory obligations that apply to them including, but not limited to, *The Freedom of Information and Protection of Privacy Act* (FIPPA), *The Personal Health Information Act* (PHIA), and the *Copyright Act*;

(e) protect their userid (the unique identifier assigned to each user of the Information Systems by IST) password and system from unauthorized use. Users are responsible for all activities on their userid that originate from their system with their knowledge;

(f) participate in security awareness, training, and education sessions as appropriate to their job functions and as directed by their supervisors and/or management;

(g) promptly report lost or stolen University owned devices to the University's IST Service Desk;

(h) promptly report lost or stolen non-University owned devices used to connect to the University's network and Information Systems or for accessing University Information to the University's IST Service Desk;

(i) promptly notify the University's IST Service Desk or the Director of Information Security and Compliance of any known or suspected Information Security Breach, Cyber Attack, incident or issue;

(j) comply with all University policies regarding Intellectual Property;

(k) access only Information that is their own, that is publicly available or to which they have been explicitly granted access by the owner of the Information;

(l) ensure that systems under their control have current security updates and anti-virus software installed regardless of ownership of the equipment; and

(m) engage in ethical workplace behaviours when using University Information Systems reflecting:

(i) academic honesty;

(ii) acceptable language of discourse;

(iii) restraint in the consumption of shared Information System resources by refraining from monopolizing systems and/or overloading networks with excessive data or activity, degrading services, or wasting any other related resource(s);

(iv) respect for Intellectual Property and ownership of data; and

(v) respect for individual rights to privacy and freedom from harrassment in such forms as intimidating, disrespectful or obscene messages, jokes or images.

3.6 IST is responsible for:

(a) ensuring that information technology architecture components are designed and implemented to protect the Information they process in accordance with the Information Security Policy, Procedure or Standards;

(b) the safety, integrity and security of University owned and operated Information Systems and networks;

(c) defining, implementing, and testing disaster recovery plans and making contingency arrangements to manage the prolonged unavailability of Information or Information Systems, critical computer facilities, equipment, or communications services;

(d) coordinating the investigation of alleged unauthorized use of University computer systems and network under the authority of the Vice President (Administration);

(e) providing current security information and anti-virus updates to the University Community and where possible installing these updates on machines connected to the campus network automatically;

(f) periodically informing and reminding the University Community of current Information Security Standards to be followed to ensure the integrity of University computing and networking facilities;

(g) maintaining an accurate and up-to-date inventory of Information System hardware and software in use; and

(h) ensuring that all implementations, maintenance, enhancements, and other Business Processes within its purview are conducted in accordance with the Information Security Policy, Procedure or Standards.

3.7 External Parties must:

(a) comply with the Information security and data protection requirements of the contracts, service agreements, and non-disclosure agreements that govern their relationship with the University;

(b) exercise due care and caution when accessing Information and Information Systems; and

(c) ensure that the Confidentiality Protection, Integrity Protection and Availability Protection of University Information are in place and that Information and Information Systems are adequately safeguarded.

3.8 The Information Security and Compliance section is responsible for developing a University-wide Information security vision, strategy, program, and Standards. Information Security and Compliance must:

(a) perform oversight and governance functions for Information assurance and protection, Information risk management, security incident investigations, and disaster recovery across the entire University;

(b) work in cooperation with the Office of Legal Counsel, Access and Privacy Office, and Audit Services to interpret laws and regulations governing Information security and privacy and provide appropriate compliance oversight;

(c) produce and maintain University-wide Information Security Standards that specify required and recommended Information security measures and controls;

(d) develop methodologies and processes to help the University of Manitoba‘s Faculty and Administrative Units comply with Information Security Procedure and Standards in a consistent and effective manner;

(e) provide expertise and knowledge of current higher education trends in Information security and Business Processes to ensure parity with peer organizations and improve control processes across the University; and

(f) respond to, investigate, and report on Information Security Breaches.

Part IV
Authority to Approve Procedures

4.1 The Chief Information Officer may approve Procedures, if applicable, which are secondary to and comply with this Policy.

Part V
Review

5.1 Governing Document reviews shall be conducted every ten (10) years. The next scheduled review date for this Policy is February 3, 2030.

5.2 In the interim, this Policy may be revised or repealed if:

(a) the Chief Information Officer or the Approving Body deems it necessary or desirable to do so;

(b) the Policy is no longer legislatively or statutorily compliant; and/or

(c) the Policy is now in conflict with another Governing Document.

5.3 If this Policy is revised or repealed all Secondary Documents, if applicable, shall be reviewed as soon as possible in order that they:

(a) comply with the revised Policy; or

(b) are in turn repealed.

Part VI
Effect on Previous Statements

6.1 This Policy supersedes all of the following:

(a) all previous Board of Governors/Senate Governing Documents on the subject matter contained herein; and

(b) all previous Administration Governing Documents on the subject matter contained herein.

Part VII
Cross References

7.1 This Policy should be cross referenced to relevant Governing Documents, legislation and/or forms as follows:

(a) Information Security Procedure

(b) Use of Computer Facilities Policy

(c) Use of Computer Facilities Procedure

(d) Custody and Control of Electronic Devices and Media Policy

(e) Custody and Control of Electronic Devices and Media Procedure

(f) Records Management Policy

(g) Access and Privacy Policy

(h) Access and Privacy Procedure

(i) Data Security Classification

(j) Use of Copyright Protected Materials Policy