UNIVERSITY OF MANITOBA

UNIVERSITY OF MANITOBA
PROCEDURE

Procedure:	INFORMATION SECURITY
Parent Policy:	Information Security Policy
Effective Date:	February 3, 2020
Revised Date:	
Review Date:	February 3, 2030
Approving Body:	Chief Information Officer
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 Procedure

1.1 To enforce the responsibilities of Information Users to act in accordance with the Information Security Policy, Procedure and Standards.

1.2 To identify the Information Security Standards applying to all Information Users.

1.3 To identify the Information Security Standards that will be used for IST support. The details of these Information Security Standards will be available to IST support personnel only, or on request.

Part II
Procedural Content

2.1 The following terms have the following defined meanings for the purpose of this Procedure:

(a) **“Academic Information”** includes information and data that is retained on the University’s Information System for a research, scholarly or educational purpose, and exists in many forms including but not limited to written or printed on paper, stored electronically, recorded on magnetic disk /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 defined as protection to ensure that access to Information and Information Systems are 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 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, formally accepts 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) **“Information**” includes all records and data in the custody and/or control of the University 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.

(j) **“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.

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

(l) **“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 may involve Information, University Information, Academic Information or Intellectual Property.

(m) **“Information Security Decision”** is a decision of Executive Staff at the University to grant an Exception to the Information Security Policy, Procedure or Standards. Information Security Decisions are based on the contents of Information Security Decision Requests submitted by Information Owners and setting out the justification/purpose for the requested Exception.

(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 to perform 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) **"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.

(t) **"IT Support"** is defined as staff in a unit or faculty who are responsible for maintaining computer systems and hardware, and for making decisions pertaining to those systems.

(u) **"University Community"** is defined as 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/tape, or spoken in conversation.

2.2 Adherence to the Information Security Policy, Procedure and Standards is mandatory for the University Community.

Definition of **"Authorized Use"**

2.3 For the purposes of this Procedure, Authorized Use of University Information, Academic Information and Information Systems are defined as University purposes associated with:

(a) Teaching and learning support;

(b) University approved research including graduate theses;

(c) Community services further to or related to the above;

(d) Administration of the University; and

(e) Outside professional activity in accordance with University policy.

2.4 Information Users may use the University Information Systems for non-University matters except where such use would be prohibited by this or other University policy or where such use unreasonably interferes with academic uses, job performance, Business Processes, or system performance/operations.

Definition of **"Unauthorized Use"**

2.5 Unauthorized Use of University Information and Information Systems is defined as use of University Information and Information Systems in ways not associated with University purposes, including but not limited to:

(a) Failure to adhere to the Information Security Policy, Procedure and Standards when using the Information and Information Systems owned and operated by the University;

(b) Use of or access to another Information User's Information System, userid, password, files, email or other Information without that Information User's permission unless authorized by the Vice-President (Administration);

(c) Attempting to circumvent security controls on any Information System or failing to keep current security controls on University owned equipment or Information Systems;

(d) Engaging in any activity that may be purposefully harmful to Information Systems or to any Information stored thereof;

(e) Placing any destructive or nuisance programs such as viruses or worms into an Information System;

(f) Sending fraudulent, harassing, threatening or obscene messages using the University Information Systems;

(g) Transmitting commercial advertisements, solicitations or promotions for any other commercial purpose that is not permitted pursuant to the Commercial Advertising Policy, or authorized by the Vice-President (Administration);

(h) Intentionally accessing or collecting illegal material or material that violates University policies or procedures;

(i) Sending unauthorized bulk email (spam);

(j) Using the system to excess for non-University related activities;

(k) Unauthorized use of the “University” logo or name;

(l) Using the systems or networks for personal financial gain in a manner which purports to represent the University’s involvement without the University’s prior written approval, excluding outside professional activity as defined above; and

(m) Engaging in any other activity that does not comply with the Information Security Policy, Procedure and Standards.

Consequences of Unauthorized Use

2.6 Persons found to be not acting in accordance with the Information Security Policy, Procedure and/or Standards are subject to University discipline up to and including dismissal/expulsion and/or any other action in accordance with applicable University governing documents and collective agreements.

2.7 In cases of financial loss to the University, restitution may be sought.

2.8 The University may disconnect any machine connected to a University Information System, including, but not limited to, Academic Staff owned computing and networking equipment which does not have current security controls installed and in the opinion of the University could jeopardize the integrity and operation of the Information and/or Information Systems.

2.9 Lack of awareness of the Information Security Policy, Procedure and Standards is not an excuse for non-compliance.

2.10 Where an Unauthorized Use is alleged, IST shall be responsible for coordinating the investigation of the Unauthorized Use with other University Administrative Units including the Office of Legal Counsel, Access and Privacy, and Human Resources, under the authority of the Vice President (Administration). When non-compliance is suspected, you should contact the Information Security Team at infosec@umanitoba.ca.

Part III

Awareness and Education

3.1 The Director of Information Security and Compliance collaborates with the Marketing and Communications Office, Information Services and Technology Staff, the Office of Risk Management, and the Access and Privacy Office to develop and distribute security awareness and educational materials.

Exceptions

3.2 Any Information Owner engaging in Business Processes for a Faculty or Administrative Unit of the University that cannot comply with any portion of this Policy, Procedure or Standards must request an Exception and submit a written Information Security Decision Request to the Director of Information Security and Compliance for review.

3.3 Requests that, if granted, pose a high level of risk to the University Information System, or a generalized risk beyond the Information Owner's Faculty or Administrative Unit may be referred to Executive Staff of the University for an Information Security Decision.

3.4 Information Security Decision Requests must include the scope and duration of the Exception, the business purpose/justification for the Exception, and a committed remediation plan and time frame to achieve adherence to the Information Security Policy, Procedure and Standards.

Information Security Standards applicable to all University Community members

3.5 The following Information Security Standards apply to all University Community members. Revisions or additions to these Information Security Standards may be undertaken by Information Security and Compliance under the authority of the Chief Information Officer:

(a) Password Standard;

(b) Device Encryption Standard;

(c) Electronic Transmission of Data Standard; and

(d) Use of Non-University Owned Devices Standard.

Information Security Standards which apply to IT Support

3.6 The following Information Security Standards apply to IT Support. Revisions or additions to these Information Security Standards may be undertaken by Information Security and Compliance under the authority of the Director of Information Security and Compliance:

(a) Workstation Patch Management Standard;

(b) Server Patch Management Standard;

(c) Application Patch Management Standard;

(d) Backup Standard;

(e) Vulnerability Management Standard;

(f) Malware Protection Standard;

(g) Threat and Risk Assessment Standard;

(h) Security Incident Handling Standard; and

(i) Data Centre and Facilities Access Standard.

Part IV
Accountability

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

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

4.3 The University Community is responsible for complying with this Procedure.

Part V
Review

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

5.2 In the interim, this Procedure 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 Procedure is no longer legislatively or statutorily compliant;

(c) the Procedure is now in conflict with another Governing Document; and/or

(d) the Parent Policy is revised or repealed.

Part VI
Effect on Previous Statements

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

(a) Information Security Policy

(b) Password Standard

(c) Mobile Encryption Standard

(d) Electronic Transmission of Data Standard

(e) Use of Non-University Devices Standard

(f) Workstation Patch Management Standard

(g) Server Patch Management Standard

(h) Application Patch Management Standard

(i) Backup Standard

(j) Vulnerability Management Standard

(k) Malware Protection Standard

(l) Threat and Risk Assessment Standard

(m) Security Incident Handling Standard

(n) Data Centre and Facilities Access Standard

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

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

(q) Data Security Classification

(r) Commercial Advertising Policy

(s) Use of Computer Facilities Policy

(t) Use of Computer Facilities Procedure