Policy Title:

Information Security Policy

University Classification & Policy Number:
A-005-21

Approval Body:
University Administration

Responsible Designate:
The Vice-President, Finance and Administration, is responsible for the overall development, administration, and review of this Policy. The Chief Information Officer ("CIO") is responsible for the operational administration of this Policy.

Established:
2023
Revised:
Not applicable
Editorial Revisions:
Not applicable
Scheduled Review:
2028

1.0 Policy Purpose

1.01 The purpose of this Policy is to outline the principles related to protecting The University of Winnipeg ("University"), the University Community, and third parties against harm through classification and secure handling requirements for University Data.

1.02 While this Policy specifically addresses information classification and related handling requirements, the domain of information security is broad and ever-changing. Therefore, aspects of the Policy and its implications for the University Community will evolve over time as circumstances warrant.

2.0 Definitions

The following definitions apply to terms as they are used in this Policy:

2.01 Department: a University faculty, department, office, centre, or other unit.

2.02 Health Care: any care, service, or procedure provided:

- to diagnose, treat, or maintain an individual's physical or mental condition; or
- to prevent disease or injury or promote health; or
- that affects the structure or function of the body, and includes the sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription.

2.03 Information Security Working Group ("ISWG"): a working group established by the University focused on the security of University Data. At a minimum, the ISWG is comprised of the following individuals or their designate: Chief Information Officer (CIO, Chair); Chair of the University Human Research Ethics Board (UHREB); Executive Director, IT Planning and Governance; Senior Information and Privacy Officer; a faculty member chosen by the Vice-President, Research and Innovation; and the Cyber Security Officer.

2.04 Personal Health Information: Recorded Information about an identifiable individual that relates to:

- the individual's health, or health care history, including genetic information about the individual; or
- the provision of health care to the individual; or
- payment for health care provided to the individual; and includes
- the personal health identification number or any other identifying number, symbol, or other particular associated with an individual; or
- any identifying information about the individual that is collected during, and is incidental to, the provision of health care or payment for health care.

2.05 Personal Information: Recorded Information about an identifiable individual, including:

- the individual's name, home address, or home telephone, facsimile, or email;
- the individual's age, sex, sexual orientation, marital or family status;
- the individual's ancestry, race, colour, nationality, or national or ethnic origin;
- the individual's religion or creed, or religious belief, association, or activity;
- personal health information about the individual;
- the individual's blood type, fingerprints, or other hereditary characteristics;
- the individual's political belief, association, or activity;
- the individual's education, employment or occupation, or educational, employment, or occupational history;
- the individual's source of income or financial circumstances, activities, or history;
- the individual's criminal history, including regulatory offences;
- the individual's own personal views or opinions, except if they are about another person;
- the views and opinions expressed about the individual by another person; or
- any identifying number, symbol, or other particular assigned to the individual.

2.06 Responsible Administrator: department heads, including Vice-Presidents, Associate Vice-Presidents, Deans, Associate Deans, and Directors.

2.07 Recorded Information: 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.

2.08 UHREB: University Human Research Ethics Board.

2.09 University Business: activities in support of the academic, research, and service mandates of the University. For employees this includes all activities performed as part of their employment duties.

2.10 University Community: students, employees, anyone holding a University appointment, post-doctoral fellows, visiting scholars, contractors, authorized third parties, volunteers, members of the Board of Regents and Senate, and anyone who resides on University property.

2.11 University Data: any data, regardless of physical form and on any storage medium, in the custody or under the control of a University Community member that is created, received, or maintained to support and provide evidence of University Business. Data includes both raw material, such as facts and figures, as well as information, which is data that has been analyzed, organized, or otherwise processed.

3.0 Scope

3.01 This Policy applies to all University Community members who have access to University Data.

4.0 Policy Elements

4.01 Principles

4.01.01 University Data is a valuable asset that supports and documents University Business.

4.01.02 Unauthorized access to University Data, or improper use or alteration of University Data, may result in harm to the institution, members of the University Community, and third parties. The University is therefore committed to the security, proper handling, and integrity of all University Data.

4.01.03 The University respects academic freedom and its obligations under relevant collective agreements including articles on academic freedom and intellectual property, to foster a climate of freedom, responsibility and mutual respect in the pursuit of the University's purposes and objectives. The academic research data of University researchers is not generally in the University's custody or under its control under Manitoba's *The Freedom of Information and Protection of Privacy Act*. However, as the University is committed to safeguarding to a high degree the University, the University Community, and third parties against harm, the academic research data of University employees, post-doctoral fellows, visiting scholars, interns, and students is University Data for the purposes of this Policy.

4.02 Roles and Responsibilities

4.02.01 All members of the University Community with access to University Data shall adhere to this Policy and shall secure University Data in accordance with this Policy's related procedures.

4.02.02 The CIO is responsible for developing strategies for the proper handling and security of University Data. They shall also chair the ISWG.

4.02.03 The ISWG, established as of the effective date of this Policy, is responsible for:

a) creating data classifications and assigning secure handling requirements for University Data, and amending these as appropriate;
b) disseminating and educating the University Community on all relevant elements of this Policy; and
c) responding to any suspected or confirmed non-compliance of this Policy and taking appropriate action, including alerting the appropriate Responsible Administrator.

4.02.04 A Responsible Administrator is responsible for:

a) understanding this Policy and promoting it within their Department, including by ensuring that staff are given adequate time for training in the working of this Policy and the associated Procedures;
b) working collaboratively with the ISWG to ensure the University Data in their Department is compliant with this Policy; and
c) ensuring that any suspected or confirmed non-compliance of this Policy of which they are aware is immediately reported to the ISWG.

4.03 Policy Non-Compliance

4.03.01 If any individual breaches the provisions of this Policy and its related procedures, they may be subject to barring from campus spaces, disciplinary consequences up to and including dismissal or expulsion, and/or the termination of any contract in accordance with related institutional policies and collective agreements.

4.03.02 This Policy is designed to be used in coordination with other University Policies. If a breach of this Policy and/or its related procedures violates one or more additional University policy the decision on which policy or procedures to follow will be that of the Vice-President, Finance and Administration.

5.0 Relevant Legislation

- *The Freedom of Information and Protection of Privacy Act* (Manitoba)
- *The Personal Health Information Act* (Manitoba*)*
- The *Personal Information Protection and Electronic Documents Act* (Canada)

6.0 Related Policies, Procedures and Institutional Documents

- Acceptable Use of Information Technology Policy
- Conflict of Interest Policy
- Copyright Policy
- Information Security Procedures
- Privacy Policy
- Respectful Working and Learning Environment Policy & Procedures
- Responsible Conduct of Research and Scholarship Policy
- Sexual Violence Policy & Procedures
- Student Non-Academic Misconduct Policy
- Survey Policy
- University Records Policy & Procedures