Policy Title:

Information Security Procedures

University Classification & Procedure 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 these Procedures. The Chief Information Officer is responsible for the operational administration of these Procedures.

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

1.0 Procedure Purpose

1.01 These Procedures outline the specific actions necessary to implement the Information Security Policy at The University of Winnipeg.

2.0 Definitions

2.01 All Definitions in the Information Security Policy are incorporated into these Procedures and shall apply as fully as if they had been set out verbatim herein.

3.0 Procedure Elements

3.01 Data Classifications

3.01.01 The University has developed a classification system to categorize University Data based on the potential harm arising from unauthorized access to, or improper use or alteration of, University Data.

3.01.02 In escalating order of potential harm, the data classifications are (see Appendix A):

a) Public;

b) Internal;

c) Sensitive; and

d) Highly Sensitive.

3.01.03 Appendix A of these Procedures outlines secure handling requirements for University Data by classification. All University Data shall be secured in accordance with its appropriate classification. Additional information security requirements may be communicated from time to time by the ISWG.

3.01.04 After reviewing Appendix A and any additional secure handling requirements communicated by the ISWG, if a University Community Member is uncertain of the appropriate data classification for any University Data or suspects the incorrect handling of classified data, the ISWG shall be consulted. Where a document, database, or other data resource contains University Data of two or more data classifications, the secure handling requirements of the most stringent data classification shall be applied.

3.01.05 If a University Community Member must apply specific information security requirements imposed by an external body to University Data, such as those established by a research funder, the University Community Member may apply these external requirements instead of the relevant secure handling requirements outlined in this Policy provided that the application of the external requirements does not result in less protection for University Data.

3.01.06 The secure handling requirements outlined in Appendix A are minimum standards that may be exceeded.

3.01.07 Any variance to the secure handling requirements associated with a data classification must be approved in advance by the ISWG.

3.02 Privacy and Security Review

3.02.01 The ISWG shall be notified to determine the requirements for a privacy and security review when a University Community Member is planning to:

a) introduce a new product or service;

b) significantly alter an existing product or service; or

c) acquire, extend, or renew a software license

that involves Sensitive or Highly Sensitive University Data, excepting where the ISWG has indicated that no such notification or review is required.

3.02.02 In respect of academic research projects that require a human research ethics application, the UHREB will determine whether the project must undergo a privacy and security review.

3.02.03 Should the ISWG or the UHREB determine that a privacy and security review is required, the University Community Member shall cooperate with the ISWG to complete the review in advance of implementation of the product, service, software, or research project.

4.0 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)

5.0 Related Policies, Procedures and Institutional Documents

- Acceptable Use of Information Technology Policy
- Conflict of Interest Policy
- Copyright Policy
- Information Security Policy
- 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

Appendix A:

1. Classification Definitions

Public: University Data that is freely disclosed to the public or would cause no harm if so disclosed.

Internal: University Data that is not protected by law, agreement, or industry regulation, but may cause minor harm to the University or others if disclosed indiscriminately or beyond a need-to-know basis.

Sensitive: University Data that

- must be protected by law, agreement, research protocol, or industry regulation;
- exposes non-public details of a University system; or
- may cause moderate harm to the University or others if disclosed to unauthorized individuals.

Highly Sensitive: University Data that

- must receive a high degree of protection by law, agreement, research protocol, or industry regulation;
- exposes non-public details of a critical University system; or
- may cause considerable harm to the University or others if disclosed to unauthorized individuals.

2. Types of University Data by Classification (Not Exhaustive)

Public	• Advertising and job postings;
	• Course and program descriptions, rates, and fees;
	• Employee:
	  ○ first and last names;
	  ○ titles;
	  ○ generic office email addresses, e.g., communications@uwinnipeg.ca; and
	  ○ office mailing addresses and office phone numbers;
	• Office locations;
	• Public-facing University Data on websites; and
	• Research University Data made available to the public.

Internal	• University Data intended for the sole use of the University, e.g.:
	  ○ budget and accounting figures;
	  ○ office procedures and manuals;
	  ○ building plans;
	  ○ work cell phone numbers; and
	  ○ employee-specific email addresses, e.g., j.doe@uwinnipeg.ca.

Sensitive	• Anonymous, anonymized, or coded human research data that is deemed sensitive (as defined above); • Appeals, grievances, and investigations; • Confidential 3rd party business information; • Information protected by solicitor-client privilege; • Information regarding ongoing litigation; • Personal Information that is not classified as Highly Sensitive; • Security camera footage.

Highly Sensitive	• Authentication credentials;
	• Credit card numbers;
	• Closed Board of Regents and Senate information;
	• Directly or indirectly identifying human research information;
	• Highly sensitive Personal Information, e.g.:
	  ○ Personal Health Information;
	  ○ accessibility and counselling information;
	  ○ social insurance number;
	  ○ driver's license number;
	  ○ passport number;
	  ○ personal financial accounts and information;
	  ○ biometric identifiers including finger and voice prints and full-face images;
	  ○ race or ethnic origin, political/religious beliefs or membership, genetic information, sexual orientation or sex life;
	  ○ criminal records checks;
	• Non-public information about a University system, e.g.:
	  ○ passwords;
	  ○ access codes;
	  ○ certificate / license numbers;
	• Research University Data that is Highly Sensitive (as defined above).

3. Security Handling Requirements by Classification

Public	• Any existing controls to govern access and integrity remain in place; • No policy requirements for access, transmission, storage, or destruction; and • Use standard operating system utilities to delete files.

Internal	• Access:
	  ○ need-to-know basis and revoked when leaving the unit;
	• Storage:
	  ○ storage on a University approved network or cloud storage system;
	  ○ for paper records, secure in a locked room or cabinet;
	• Transmission:
	  ○ no requirements when transmitted over a secure network;
	  ○ encryption recommended over unsecure networks;
	  ○ for paper records, protect against incidental reading; and
	• Destruction:
	  ○ delete using an approved deletion program; and
	  ○ shred.

Sensitive	• Access:
	  ○ need-to-know basis and revoked when leaving the unit;
	• Storage:
	  ○ storage on secure network required;
	  ○ encryption required;
	  ○ for paper records, secure in a locked room or cabinet;
	• Transmission:
	  ○ encryption recommended over secure networks;
	  ○ encryption required over public networks;
	  ○ for paper records, send in sealed envelope with “confidential” label; and
	• Destruction:
	  ○ delete using an approved deletion program; and
	  ○ shred.

Highly Sensitive	• Access:
	  ○ must be approved by the Responsible Administrator;
	  ○ limited to specific named users or positions;
	  ○ need-to-know / least privilege basis;
	  ○ revoked immediately when leaving the unit;
	• Storage:
	  ○ controlled access system required (password protected file or file system);
	  ○ secure network required;

	○ encryption required; ○ for paper records, double locking required (e.g., locked room and locked cabinet); ○ clean desk policy required; • Transmission: ○ encryption required over secure networks; ○ encryption required over public networks; ○ for paper records, send in sealed envelope with “confidential” label; ○ trackable mail/courier recommended; and • Destruction: ○ delete using an approved deletion program; and ○ shred.