The purpose of establishing a Data Security Classification is to provide a formal means of identifying information risks and classifying information according to sensitivity for the purpose of applying appropriate protective security measures.

The data collected, used and maintained by the University varies in sensitivity and format, therefore appropriate security measures must be in place to ensure compliance with business, legal and regulatory requirements. Sensitive data may include personal and personal health information or proprietary internal information related to, and under the custody and control of, the University and University community (including employees, faculty, students, researchers, contractors, associates, etc.).

Under The Freedom of Information and Protection of Privacy Act (FIPPA) and The Personal Health Information Act (PHIA), the University of Manitoba has certain obligations to ensure appropriate collection, maintenance, use and disposal of University records. These requirements must be applied equally to paper and electronic information systems and devices.

All data, regardless of format must be classified under this standard. All records, regardless of whether they constitute an official University record, contain data and must be classified under this standard.

This document is intended for:

- Enterprise system owners and stakeholders with responsibility for leading and implementing information technology and management process, procedures, and initiatives.
- Individuals with responsibility for maintaining the custody and control of University records.
- Individuals that use or access University systems containing personal or proprietary information, including University networks, databases, email systems, smartphones, etc.

**Definitions**

**Data:** Factual information, used as a basis for reasoning, discussion or calculation; representations of information or of concepts, in any form; raw information in its simplest form.

**Personal Information** means recorded information about an identifiable individual, including:

- the individual's name,
- the individual's home address, or home telephone, facsimile or e-mail number,
- information about the individual's age, sex, sexual orientation, marital or family status,
- information about the individual's ancestry, race, colour, nationality, or national or ethnic origin,
- information about 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,
- information about the individual's political belief, association or activity,
- information about the individual's education, employment or occupation, or educational, employment or occupational history,
- information about the individual's source of income or financial circumstances, activities or history
- information about 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 or opinions expressed about the individual by another person, and
- an identifying number, symbol or other particular assigned to the individual.
Personal Health Information is recorded information about an identifiable individual that relates to:

a) the individual’s health, or health care history, including genetic information about the individual,
b) the provision of health care to the individual, or
c) payment for health care provided to the individual, and includes
d) the Personal Health Information Number (“PHIN”) and any other identifying number, symbol or particular assigned to an individual, and
e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care;

Records: Information created, received and maintained as evidence and information by an organization or person in pursuance of legal obligations or in the transaction of business. Records contain evidential value, describing the context, content and structure of the data.

System (Electronic): A network of hardware and software used to collect, filter, process, create and distribute records and/or data.

Data Classification Framework

<table>
<thead>
<tr>
<th>Sensitivity</th>
<th>Definition</th>
<th>Protective Security Measures</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Restricted  | Information that is highly sensitive both externally and internally at the University. Unauthorized access could reasonably be expected to cause serious harm to individuals, businesses, other third parties or the University. | Extensive security measures, including: **Electronic media:** Encryption, security access controls, possible offline storage, potential physical controls such as maintaining equipment in secured areas. **Paper media:** Secure storage via locking cabinet and/or room that is accessible only to those with proper clearance. | Examples may include:
- Records containing sensitive personal health information
- Drafts of strategic plans, annual reports, and financial statements
- Legal files
- Payroll information and data
- Some security response plans
- Network system information
- Proprietary source code
- Patent applications, trademarks and trade secrets
- Research data and intellectual property |
| Protected   | Information that is sensitive externally and may be somewhat sensitive internally at the University. The inappropriate release of the information would reasonably be expected to cause minimal to moderate harm to individuals, businesses, other third parties or the University. | Moderate or baseline security measures, including employee identification, desktop tools, access controls (systems, applications, file/folder), site containers, network security monitoring, encryption, system audit functionality, physical storage in a secure cabinet or room, etc. | Examples may include:
- Vendor or service provider contracts
- Employment contracts
- Employee records
- Internal communications
- Donor or prospect information
- Applications for employment, resumes, reference letters
- Student applications
- Student records
- Planning documents |
| Public      | Information that is intended for or is available to the public. | Limited security measures, including (in some cases) use/edit controls, ensuring physical availability of official paper media. | Examples may include:
- University website
- Brochures, campus maps
- Calendar and course information
- Published marketing information
- Governing documents
- Published annual reports |
Implementing Data Classification

Information plays an integral role in the business of the University. Responsibility for classifying information for data protection therefore lies at the highest level of the business unit, in collaboration with Information Services and Technology (IST).

Data sensitivity is determined by the context within which the data exists. Sensitivity cannot be determined by subject (e.g. name, phone number, etc.), record type (e.g. application form, email, etc.), or record media (e.g. electronic, paper, etc.). Sensitivity is determined by the purpose and manner in which the information is collected and used. For example, an employee’s name and work contact information is not sensitive in the context of an address book or directory. However, if this information is in the context of disciplinary action, legal action or a human rights complaint, the same information may be highly sensitive.

Data classification itself should be carried out by the business-owner and according to established business, legal, regulatory and University-specific requirements.

Implementing data classification first requires an understanding of the business functions and processes in place within the organization. The business-owner is in the best position to articulate and make decisions about the business, legal and regulatory context of the data under its care. Implementing data classification requires:

- Documenting clearly the processes and activities which create and use records.
- Documenting legal, operational, policy, procedural and regulatory requirements of the business unit.
- Assessing the risks of confidentiality breaches.
- Organizing information assets in ways which allow them to be managed in groups, rather than at the individual or file level.
- Establishing the appropriate classification levels for data resulting from business processes.
- Establishing policies and procedures for managing, classifying and safeguarding data.
- Securing data according to established policies and procedures.

Once the business rules for managing information have been established by the business-owner, they must be communicated to IST so that appropriate security safeguards can be applied.

Information Managers (IST) are responsible for establishing and applying security safeguards in collaboration with business-owners.

Data Classification Checklist

- Roles and responsibilities for classifying and handling data have been clearly articulated.
- Business processes have been identified and documented.
- Risks to confidential information have been identified.
- Policies and procedures relating to classification of data have been established and communicated.
- Minimum security safeguards have been established for different levels of security.

For Further Information

- Contact the Access and Privacy Office, 233 Elizabeth Dafoe Library, 204.474.9462, fippa@umanitoba.ca
- Contact the IT Help Desk (204.474.8600) or Shared Services (204.474.8400)