DATA SECURITY CLASSIFICATION

Data Security Classification provides a formal means of identifying information risks and classifying information according to its sensitivity for the purpose of applying appropriate security measures.

Data collected, used and maintained by the University varies in sensitivity and format. Appropriate security measures must be in place to ensure compliance with business, legal and regulatory requirements. Sensitive data may include personal information and personal health information or confidential business or administration 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 or not they constitute an official University record, contain data and must be classified under this standard. This includes analogue (paper) and digital records. Digital records include, but are not limited to memos, reports, written documents, audio and video recording, photographs, X-rays.

Information systems, such as databases software platforms, Software-as-a-Service (SaaS or “cloud” services) and email that contain data should be classified at a system level in accordance with the highest classification level applicable to the data.

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 and managing the custody and control of University records.
- Individuals that use or access University systems containing personal information, personal health information or confidential business information, including University networks, databases, email systems, authorized SaaS products and tools, smartphones, etc.

DATA CLASSIFICATION RANKINGS

Definition	Protective Security Measures	Examples
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 a 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, files/folders), 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 ▪ Donor or prospect information ▪ Applications for employment, resumes, reference letters ▪ Student applications ▪ Student records ▪ Planning documents ▪ Building floor plans including details about lab materials or secured facilities ▪ Aggregated or de-identified datasets

INTERNAL		
Information that is relevant to an internal audience. This information would not cause harm to the University if it was made public, but it is not content that needs to be actively shared with an external audience. This type of information would commonly be held in an intranet.	Limited security measures, including (in some cases) use/edit controls, ensuring the physical availability of official paper media.	Examples may include: ▪ Internal Newsletters and communications ▪ Internal Mailing lists (all staff, or subsets of staff) ▪ Human Resources blank forms ▪ Staff pension and benefits information ▪ Financial Services blank forms ▪ Training and support materials for Financial Systems
PUBLIC		
Information that is regularly shared or made available to the public.	Limited security measures, including (in some cases) use/edit controls, ensuring the 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

For Further Information

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

Produced by the Access and Privacy Office,
Updated August 2020