UNIVERSITY OF CALGARY

University Policy
University Procedure
Operating Standard
Guideline/Form

Information Security Classification Standard

OSP Document Number IM010-03
Authorizing Unit University Legal Services Information Technologies
Approval Authority General Counsel Chief Information Officer
Implementation Authority General Counsel
Effective Date January 31, 2008
Last Revision January 1, 2015

Table of Contents

1 Purpose

The purpose of this operating standard is to establish a framework for:

a) classifying Information Assets based on Confidentiality; and
b) determining baseline security controls for the protection of Information Assets based on their Confidentiality.

2 Scope

This operating standard applies to Information Assets regardless of their location.

3 Definitions

In this operating standard:

a) "Confidentiality" defines an attribute of information. Confidential information is sensitive or secret information, or information whose unauthorized disclosure could be harmful or prejudicial.

b) "Data Custodian" means an employee who implements controls to ensure the security of Information Assets within their domain. The Data Custodian is accountable to the Data Trustee.

c) "Data Trustee" means a member of the Executive Leadership Team. The CIO and General Counsel collaborate with Data Trustees to define and approve data-related policies and standards.

d) "Information Assets" means Business Information Assets, Health Information Assets and Scholarly Information Assets as defined in the Information Asset Identification and Classification Policy

e) "University" means the University of Calgary.

4 Standard/Practice

Security Classification

4.1 Data Custodians will classify Information Assets with respect to their Confidentiality using one of the following four categories:

Classification	Definition	Examples
Level 1: Public	▪ Information deemed to be public by legislation and/or under University policy ▪ Information in the public domain	▪ names of employees and - business contact information - job profile - salary range - discretional benefits - relevant education ▪ names of registered students and - dates of registration - program of registration - degree awarded - convocation date ▪ annual reports ▪ public announcements ▪ telephone directory ▪ published research data
Level 2: Internal Use	▪ Information not approved for general circulation outside the University ▪ Information the disclosure or loss of which would inconvenience the University although it would unlikely result in financial loss or reputational damage	▪ internal memos sent to all members of a department ▪ minutes of department meetings that are circulated to all members of a department ▪ unpublished research data ▪ anonymized or de-identified human subject data ▪ library transactions and journals

Level 3: Confidential	▪ Information that is available only to authorized persons ▪ Information the disclosure or loss of which could seriously impede the University's operations ▪ Information the disclosure or loss of which may: - adversely affect the University's operation; or - cause reputational damage; and - obligate the University to report to the government or other regulating body and/or provide notice to affected individuals.	▪ faculty/staff employment applications, personnel files, date of birth, health information and personal contact information ▪ admission applications ▪ student enrollment status ▪ donor or prospective donor name and contact information ▪ information commonly used to establish identity such as a driver's license or passport ▪ contracts ▪ intellectual property ▪ authentication verifiers including: - passwords - shared Secrets - cryptographic private keys
Level 4: Restricted	▪ Information that is: - confidential; and - subject to specific privacy and security safeguards under law, policy or contractual agreement. ▪ Information the loss or disclosure of which could cause severe harm to individuals or the University ▪ Information the loss or disclosure of which may obligate the University to report to the government or other regulating body and/or provide notice to affected individuals	▪ payment card information including: - PAN - cardholder name - CVV2/CVC2/CID ▪ health information when it can be linked to an identifiable individual including: - information about health status - diagnostic, treatment or care information - payment for health care ▪ identifiable human subject research data ▪ information that is subject to special government requirements in the interests of national security

4.2 For convenience, Data Custodians may assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection includes a student's name, degree program and credit card number, the data should be classified as Restricted even though the student's name and degree program is public information.

4.3 If there is any ambiguity with respect to Confidentiality, the information will be classified as Confidential until it can be definitively classified at a lower level.

4.4 Data Custodians will reevaluate the classification of Information Assets on a periodic basis to ensure the assigned classification is still appropriate.

4.5 If a Data Custodian determines that the classification of certain Information Assets has changed, an analysis of security controls will be performed to determine whether existing controls are consistent with the new classification.

4.6 If gaps are found in existing security controls, the Data Custodian will work with relevant University departments to mitigate and/or correct the risk.

Information Asset Protection Requirements

4.7 Information Assets will be protected in accordance with the security classification.

4.8 Appendix A outlines the minimum protection requirements that are necessary at each security classification level.

4.9 Appendix A will be updated by the CIO as technology changes and new controls are introduced.

5 Appendices

Appendix A: Information Asset Access, Transmission and Storage Requirements

6 Related Policies

Information Asset Management Policy

7 History

January 31, 2008	Approved and Effective.
January 1, 2015	Revised.
June 26, 2015	Editorial Revision. Approved by General Counsel
July 30, 2015	Editorial Revision. Approved by General Counsel on the recommendation of Director, Information Technologies.
January 1, 2020	Editorial Revision. Updated format and links.

Appendix A: Information Asset Access, Transmission and Storage Requirements

Level	Labels	Access	Transmission	Storage
1	Public	READ ▪ no restrictions WRITE/EDIT ▪ limited to Data Trustee or delegate ACCESS CONTROLS ▪ none required	▪ no special safeguards required	▪ no special safeguards required
2	Internal Use	READ ▪ limited to employees and other authorized users who have a work-related need to access the information ▪ access privileges determined by the Data Trustee; and can be based on position or on role definition WRITE/EDIT ▪ limited to Data Trustee or delegate ACCESS CONTROLS ▪ access information through the local network or VPN ▪ password authentication required ▪ two-factor authentication recommended for remote access	▪ Encryption (or similar mechanism): - recommended when transmitting information via public networks (e.g. Internet) - encryption (or similar mechanism) optional when transmitting via local network	ELECTRONIC ▪ information must be stored within a controlled access system ▪ the server must be on a network that is not visible to public networks ▪ information may be stored on a server that is: - managed and monitored internally; OR - managed by a third party when the storage arrangement is approved by IT, University Legal Services, and the Trustee AND when a contract with the third party is in place ▪ Encryption (or similar mechanism): - optional when information is stored within the University data centre - recommended when information is stored outside the University data centre PAPER ▪ store records in a locked file cabinet ▪ access to the cabinet restricted to those authorized by the Data Trustee or designate

3	Confidential	READ ▪ limited to employees and other authorized users who have a work-related need to access the information ▪ access privileges determined by the Data Trustee; based on position or on role definition WRITE/EDIT ▪ limited to Data Trustee or delegate ACCESS CONTROLS ▪ access information through the Local Network or VPN ▪ password authentication required ▪ two-Factor Authentication required for remote access	▪ Encryption (or similar mechanism): - required when transmitting information via public networks (e.g. Internet) - recommended when transmitting via local network	ELECTRONIC ▪ information must be stored within a controlled access system ▪ the server must be on a network that is not visible to public networks ▪ information must be stored on a server that is: - managed and monitored internally; OR - managed by a third party when the storage arrangement is approved by IT, University Legal Services, and the Trustee AND when a contract with the third party is in place ▪ Encryption (or similar mechanism): - required when information is stored outside the University Data Centre - optional when information is stored on premise PAPER ▪ store records in a locked file cabinet ▪ access to the cabinet restricted to those authorized by the Data Trustee or designate
4	Restricted	READ ▪ as above for Level 3 WRITE/EDIT ▪ as above for Level 3 ACCESS CONTROLS ▪ as above for Level 3 unless additional controls are required under law or contract	▪ as above for level 3 unless encryption (or similar mechanism) is required under law or contract when transmitting via local network	ELECTRONIC ▪ as above for Level 3 unless additional controls are required under law or contract ▪ encryption (or similar mechanism): - as above for Level 3 unless encryption (or similar mechanism) is required under law or contract even when information is stored on premise PAPER ▪ store records in a locked file cabinet ▪ access to the cabinet restricted to those authorized by the Data Trustee or designate