University Policy
University Procedure
Operating Standard
Guideline/Form

Effective Date	
Last Revision	

1 Purpose

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.

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 e icq231.3 TJETQ1.59 85 TJET (e)-3 (m71.3 T9 (d t)2.6 ET (e)-nd/85 42.6 (i)5.1 (o)1. un(o)	

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 rm item 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 i abi ab c0 1 Tf (bl)5.1 (atTf-.1 (r)1.

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

[redacted]

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