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
September 9, 2024

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.

Level 3: Confidential	Information that is available only to authorized persons Information the disclosure or loss of which could seriously impede

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: 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