



Information Security Classification Standard

OSP Document Number IM010-03	Table of Contents 1 Purpose 1 2 Scope 1 3 Definitions 1 4 Standard/Practice 2 5 Appendices 4 6 Related Policies 4 7 History 4
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	

- 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 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.
		September 9, 2024	Editorial Revision.

Appendix A: Information Asset Access, Transmission and Storage Requirements

Level	Labels	Access	Transmission	Storage
1	Public	<p>READ no restrictions</p> <p>WRITE/EDIT limited to Data Trustee or delegate</p> <p>ACCESS CONTROLS none required</p>	no special safeguards required	no special safeguards required
2	Internal Use	<p>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</p> <p>WRITE/EDIT limited to Data Trustee or delegate</p> <p>ACCESS CONTROLS access information through the local network or VPN password authentication required two-factor authentication recommended for remote access</p>	<p>Encryption (or similar mechanism):</p> <ul style="list-style-type: none"> - recommended when transmitting information via public networks (e.g. Internet) - encryption (or similar mechanism) optional when transmitting via local network 	<p>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:</p> <ul style="list-style-type: none"> - 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 <p>Encryption (or similar mechanism):</p> <ul style="list-style-type: none"> - optional when information is stored within the University data centre - recommended when information is stored outside the University data centre <p>PAPER store records in a locked file cabinet access to the cabinet restricted to those authorized by the Data Trustee or designate</p>

- 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