ADMINISTRATIVE PROCEDURE

Information Governance: Information Classification

Procedure Contents
- **Related Policy**
- **Purpose**
- **Applicability**
- **Procedure**
- **Related Information**
- **History**

Effective Date: 22 October 2012
Last Updated: 15 July 2021
Responsible University Officer:
VP Technology/CIO
Owner:
Senior Director, Information Governance
Contact:
Brad Stone

RELATED POLICY: Information Use, Privacy, and Security Policy

Purpose

Identifying, defining, and classifying university information is essential for ensuring that the appropriate degree of protection is applied. This procedure describes how the University classifies information.

Applicability

This administrative procedure applies to all university departments, faculty, staff, employees, consultants, and third-party service providers who have responsibility for classifying, providing access to, or using University information.

Procedure

Responsibility for Classification:

Information Stewards are responsible for classifying the information in their academic or administrative units into one of the four categories defined below. Information Stewards may appoint Glossary Editors to assist them. Classifications are to be determined in consultation with appropriate Information Trustees and are then used to govern access and security requirements. In addition, Information Stewards are responsible for periodically evaluating the classifications assigned and for providing information concerning access or availability of information within their stewardship.

Information Classifications:

Information is classified into one of the following four categories according to its use, sensitivity, risk, and importance to the university and in compliance with university policy, state and federal regulations, and other obligations regarding privacy and confidentiality of information.

Public

Information approved for public release that should be protected against loss or change.
(Examples: Course catalog, University calendar dates, University department names and department contact information)

Internal

Moderately sensitive information which is generally accessible within the University to those with a legitimate university purpose and is not intended for entities or persons outside the University.
(Examples: Student records, Employee contact information, Organization charts)

Confidential

Highly sensitive information where an inappropriate loss, changes, or disclosure could have substantial consequences to the University.

Substantial consequences include:

- Information disclosure that may be used to steal money from the University.
- Disclosure of personal information that could lead to identity theft or monetary loss for a small set of individuals, representing a breach of professional expectations by the University.
- Serious violation of regulatory requirements.

(Examples: Employee salary or performance information, Employment action reasons, Credit cardholder name and contact information**)**

Restricted

Information of the highest sensitivity where inappropriate loss, changes, or disclosure could have grave consequences to the University.

Grave consequences include:

- Information disclosure that may be used to steal money from others who have entrusted the University with their information, including students, donors, employees, and other patrons.
- Exposure of a significantly large amount of personal information that may result in significant fines or regulatory violations.
- Disclosure of information that would put the school, employees, students, alumni, other patrons, or their families in physical danger.

(Examples: Social Security Number, Credit card number, Personal medical records)

Considerations when Classifying Information:

Default Classification

All information is considered non-public and classified as **"Confidential"** until classified otherwise.

Aggregated or Combined Data

Some information may have little or no sensitivity in isolation but may be highly sensitive when combined with other data. For that reason, Information Stewards may classify aggregated or combined datasets with a more restrictive classification.

Approvals

All information classifications are subject to final approval by the Information Trustees.

Related Information

- Church Education System Information Classifications
- Access to Student Records Policy
- Access to Student Records Procedure
- Appropriate Use of Information Technology Resources Policy

History

Effective:

2 October 2012

Superseded:

14 April 2017

15 July 2021