| *SECTION:* **Information Technology** | *NO.* | | |
|---|---|---|---|
| *CHAPTER:* **General** | *ISSUED:* **3/13/13** | *REV. A* | *REV. B* |
| *POLICY:* **Data Classification Policy** | Page **1** of **5** | | |

## PURPOSE

The purpose of this policy is to ensure the appropriate level of protection is applied to University data and enable those who handle data to be able to easily make decisions when managing the data.

## SCOPE

This policy applies to all data generated, accessed, modified, transmitted, stored, or used by the University, irrespective of the medium on which the data resides (paper, hard drive, CD/DVD, etc.), or the format of the data (text, graphics, video, voice, etc.).

All University faculty, staff, agents, and contractors must abide by the required security controls defined for each classification level.

## POLICY

All University data must be classified into one of three sensitivity levels by the appropriate Data Owner: Confidential, Private, or Public. A document, file, or information system is classified according to the most sensitive level of data contained therein and should be labeled in accordance with the **Data Labeling Standard**.

**A. Confidential (High Sensitivity)**
Data should be classified as Confidential if its unauthorized disclosure could result in significant legal, financial, reputational, or other adverse impact upon the University, due to legal or regulatory requirements, University policies or agreements to which the University is a party, or because of the sensitivity of the information. Examples of Confidential data can be found in Appendix A.

**B. Private (Medium Sensitivity)**
Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in harm to the University's image or reputation, or could undermine the confidentiality of University business or processes, but would not necessarily violate existing federal or local laws, University policies, or University contracts. Data in this category are not routinely distributed outside the University, and distributed within the University on a need-to-know basis. Examples of Private data can be found in Appendix A.

**C. Public (Low Sensitivity)**
Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. Public data has no legal or other restrictions on access or usage and may be open to the University community and the general public. Examples of Public data can be found in Appendix A.

## DEFINITIONS

**Data Owners** – Those who generate data or those to whom data are entrusted. Data owners assign the classification categories to their data, and have the primary responsibility for ensuring the appropriate use and security of the data. "Data Owners" is used as a term of art for the purpose of this and related University policies, and does not refer to the actual legal ownership of particular data.

## RESPONSIBILITIES

**Data Owners** are responsible for classifying data under this policy.

## ADMINISTRATION AND INTERPRETATIONS

This policy shall be administered by Information Security. Questions regarding this policy should be directed to the Information Security Officer.

## AMENDMENT/TERMINATION OF THIS POLICY

The University reserves the right to modify, amend or terminate this policy at any time. This policy does not constitute a contract between the University and its faculty or employees.

## REFERENCES TO APPLICABLE POLICIES

Data Handling Policy
Data Labeling Standard
Data Destruction Standard
Data Stewardship Policy

## EXCEPTIONS

None

## VIOLATIONS/ENFORCEMENT

Any known violations of this policy should be reported to the University's Information Security Officer at 402-280-2386 or via e-mail to infosec@creighton.edu.

Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with University procedures.

The University may advise law enforcement agencies when a criminal offense may have been committed.