Policies and Standards

Policies and Standards

SECTION: Security

CHAPTER: General

POLICY: Data Classification Policy

PAGE 1 OF 2

PURPOSE

The purpose of this policy is to provide all members of the Creighton community with information to guide their security-related handling of University data. All data, regardless of its classification, will be protected from unauthorized alteration; this policy provides guidance on the proper handling of data.

SCOPE

This policy applies to all members of the Creighton University community (staff, faculty, students, contractors, consultants, temporaries, visitors, etc.) while using Creighton’s computing or networking resources. All users are expected to be familiar with and comply with this policy.

POLICY

All Creighton University data and data entrusted to Creighton University falls within one of three sensitivity classifications. The three sensitivity classes are: Confidential, Internal Use Only, and Public.

If not designated, the default classification is Internal Use Only.

All data must be maintained in accordance with the Data Classification Standard.

Departments may adopt departmental policies that create classifications with greater restrictions that those outlined within.

DEFINITIONS

Confidential
Access to this information shall be tightly restricted based on the concept of need-to-know. Disclosure requires the information custodian's approval and, in the case of third parties, a signed confidentiality agreement. Examples include employee performance reviews, patient identifiable information, research data, etc.

Internal Use Only
This information shall only be disclosed to third parties if a confidentiality agreement has been signed. Disclosure is not expected to cause serious harm to the University, and access is provided freely to all members of the Creighton Community. Examples include student telephone and address lists, policies and standards, network diagrams, etc.

Public
This information is suitable for public dissemination. Examples include, course listings, press releases, marketing brochures, etc.
Responsibilities

**Information Custodian** is responsible for ensuring the information under their control adheres to this policy and the Data Classification Standard.

**Information Security Officer** is responsible for maintaining the policy and ensuring the infrastructure exists to support 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 Standards

- Information Security Philosophy
- Information Security Governance Policy
- Data Classification Standard
- Information Security Exception Policy

Exceptions

Requests for an exception to this Policy must be submitted via the Policy Exception Request Form. All exception requests will be handled in accordance with the Information Security Exception Policy and Standard.

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.