Policies and Procedures

SECTION: **Administration**	***NO.*** **2.4.50.**		
CHAPTER: **Information Technology**	***ISSUED:*** 3/13/13	*REV. A*	*REV. B*
POLICY: **Data Handling Policy**	*PAGE 1 OF 4*		

PURPOSE

The purpose of this policy is to outline the appropriate mechanisms for safeguarding University data as it travels through the lifecycle of being created, received, transmitted, maintained, used, and destroyed.

SCOPE

This policy covers all data, electronic or otherwise, that is used, produced, owned and/or placed in the care of Creighton University and its affiliates.

POLICY

All University data must be associated with a Data Owner who is responsible for managing access to the data and that all standards and policies are followed for the duration of the data lifecycle. Data must be classified and labeled in accordance with the **Data Classification Policy** and the **Data Labeling Standard**. The handling and safeguards afforded to each classification level are as follows:

Confidential Data

Confidential Data must be protected at all times to the highest possible degree as is prudent or as is required by law. Guidelines for the protection of Confidential Data include, but are not limited to the following:

1. Collection/Creation
    a. Users should collect only the minimum necessary information required to perform business or academic functions.
2. Access
    a. Data Owners are responsible for defining which users or groups of users may have access to confidential data under their stewardship.
    b. Access to confidential data should be logged with sufficient detail to identify the individual who accessed the data and when.
    c. Where access to confidential data has been authorized, use of such data shall be limited to the purpose required to perform University business.
    d. Confidential data must not be disclosed to third parties outside the University without explicit authorization of the Data Owner.
3. Storage/Handling
    a. Confidential data must be maintained with sufficient controls to prevent access by unauthorized parties.
    b. Confidential data at rest must be protected in accordance to the **Data Storage Standard.**
    c. Entities entrusted with confidential data must go through annual data security training.
4. Transfer
    a. Confidential data must not be transmitted electronically without mechanisms to ensure the confidentiality and integrity of the transmitted data.
        i. For example, a file may be transferred using an encrypted transfer protocol such as SFTP to protect it while in transit.

        ii. Encryption levels must meet the minimum standard for confidential data as outlined in the **Data Encryption Standard**.

5. Destruction
    a. Once data has reached the end of its useful life at the University, as defined in the **Data Retention Policy**, it must be destroyed in accordance with the **Data Destruction Standard**.
    b. Confidential data must be sufficiently destroyed so that none of the original elements can be recovered, reused, or identified.

Private Data
A reasonable level of control should be applied to Private Data to prevent accidental or intentional disclosure to unauthorized parties. Guidelines for the protection of private data include, but are not limited to the following:

1. Collection/Creation
    a. Users should collect only the minimal amount of information required to perform business/academic functions.
2. Access
    a. Data Owners are responsible for defining which users or groups of users may have access to private data under their stewardship.
    b. Private data should not be openly shared outside of the University.

3. Storage/Handling
    a. Private data must be maintained with sufficient controls to prevent access by unauthorized parties.
    b. Private data at rest must be protected in accordance to the **Data Storage Standard**.

4. Transfer
    a. Private data should not be transmitted electronically without mechanisms to ensure the confidentially and integrity of the transmitted data.
    b. Encryption levels must meet the minimum standard for private data as outlined in the **Data Encryption Standard**.
5. Destruction
    a. Once data has reached the end of its useful life at the University, as defined in the **Data Retention Policy**, it must be destroyed in accordance with the **Data Destruction Standard**.

Public Data
A minimal level of control should be applied to Public Data to prevent unauthorized alterations or deletion. Guidelines for the protection of public data include, but are not limited to the following:

1. Collection/Creation
    a. Users should collect only the minimal amount of information required to perform business/academic functions.
2. Access
    a. Public Data is free to be accessed by any individual with no special provisions
    b. Care must be taken to prevent unauthorized modification or destruction of any data.

3. Storage/Handling
   a. No special restrictions exist on the storage or handling of public data other than those required to prevent unauthorized modification or destruction.
4. Transfer
   a. Public data may be transmitted in any available format or mechanism.
5. Destruction
   a. Once data has reached the end of its useful life at the University, as defined in the **Data Retention Policy**, it must be destroyed in accordance with the **Data Destruction Standard**.

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 data policies, and does not refer to the actual legal ownership of particular data.

Data Custodian
Those who are authorized by the Data Owner to use or manipulate data. Data Custodians have the responsibility to adhere to all policies applicable to the data entrusted to them.

RESPONSIBILITIES

Data Owners have the following responsibilities:

1. Ensure that access and protection requirements are consistent with University policies and the data classifications are in place and responsive to business needs.
2. Ensure the accuracy and quality of all data within their stewardship.
3. Communicate data protection requirements to the Data Custodians.
4. Annually review with appropriate Data Custodians the current set of data access authorizations and, as appropriate, update access granted to each user.
5. Ensure that authorized users of highly sensitive data are trained on their responsibilities associated with their approved access to that data.
6. Report any possible breach in security or illicit use of information systems to the Information Security Office.
7. Ensure that data is properly identified and labeled in accordance with applicable standards and policies.

Data Custodians have the following responsibilities:

1. Protect data in their possession from unauthorized disclosure, access, alteration, destruction, or usage.
2. Use information systems in a manner consistent with University policies and procedures.

ADMINISTRATION AND INTERPRETATIONS

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

Policies and Procedures

SECTION: **Administration**	***NO.*** **2.4.50.**		
CHAPTER: **Information Technology**	***ISSUED:*** 3/13/13	*REV. A*	*REV. B*
POLICY: **Data Handling Policy**	*PAGE 4 OF 4*		

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 Classification Policy
Data Retention Policy
Data Destruction Standard
Data Storage Standard
Data Encryption Standard
Data Labeling Standard

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.