Policies and Procedures

SECTION:	*NO.*		
Administration	**2.4.11.**		
CHAPTER:	*ISSUED:*	*REV. A*	*REV. B*
Information Technology	3/13/13		
POLICY:	*PAGE 1 OF 2*		
Data Classification Policy			

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.

APPENDIX A DATA CLASSIFICATION SNAPSHOT

	Confidential (High Sensitivity)	**Private** (Medium Sensitivity)	**Public** (Low Sensitivity)
Description	Data which is legally regulated; and data that would provide access to Confidential or Private data.	Data which the Data Owners have not decided to publish or make public; and data protected by certain contractual obligations.	Data for which there is no expectation for privacy or confidentiality.
Legal Requirements	Protection of data is required by law or contract.	Protection of data required by contract.	None. Protection of data is at the discretion of the Data Owner or Data Custodian.
Reputational Risk	High	Medium	Low
Data Access and Control	Legal, ethical, or other constraints prevent access without specific authorization. Data is accessible only to those individuals designated with approved access and signed non-disclosure agreements.	University privacy, ethical, and reputational concerns prevent access without specific authorization. Data is accessible only to those individuals designated with approved access and signed non-disclosure agreements.	No access restrictions. Data is available for public access.
Transmission	Transmission of Confidential data through any non-Creighton network is prohibited (e.g. Internet). Transmission through any electronic messaging system (e-mail, instant messaging, text messaging) is also prohibited.	Transmission of Private data through any non-Creighton network is strongly discouraged. Third party email services are not appropriate for transmitting Private data.	No encryption or other protection is required for public data; however, care should always be taken to use all University data appropriately.
Storage	Storage of Confidential data is prohibited on Individual-Use Electronic Devices and media unless approved by the Information Security Officer. If approved, additional protective measures, including encryption will be required.	Level of required protection of Private data is either pursuant to Creighton policy or at the discretion of the owner or custodian of the data. If appropriate level of protection is not known, check with Information Security Officer before storing Private data unencrypted.	No encryption or other protection is required for public data; however, care should always be taken to use all University data appropriately.
Documented Backup and Recovery Procedures	Documented backup and recovery procedures are required.	Documented backup and recovery procedures are not necessary, but strongly encouraged.	Documented Backup and Recovery Procedures are not necessary, but strongly encouraged.
Audit Controls	Data Owner and Data Custodians with responsibility for Confidential data must actively monitor and review their systems and procedures for potential misuse and/or unauthorized access.	Data Owners and Data Custodians with responsibility for Private data must periodically monitor and review their systems and procedures for potential misuse and/or unauthorized access.	No audit controls are required.
Examples	**Information resources with access to Confidential data (username and password).** Student Data not included in directory information. This includes: • Loan or scholarship information • Payment history • Student tuition bills • Student financial aid information	**Personal/Employee Data** • Payroll information • Personnel records, performance reviews, benefit information • Race, ethnicity, and/or nationality • Gender • Date and place of birth **Business/Financial Data** • Financial transactions which do not include confidential data	**Certain directory/contact information not designated by the owner as Private.** • Name • Addresses (campus and home) • Email address • Listed telephone number(s) • Degrees, honors and awards • Major field of study

	• Class lists or enrollment information • Transcripts; grade reports • Notes on class work • Disciplinary action • Athletics or department recruiting information **Personally Identifiable Information (PII): Last name, and first name or initial, with any one of following:** • Social Security Number • Driver's license • State ID card • Passport number • Financial account (checking, savings, brokerage, CD, etc.), credit card, or debit card numbers **Protected Health Information (PHI) *** • Health Status • Healthcare treatment • Healthcare payment **Personal/Employee Data** • Worker's compensation or disability claims **Business/Financial Data** • Credit card numbers with/without expiration **Research Data** • Research data that is protected by laws and regulations.	• Information covered by non-disclosure agreements • Contracts – that don't contain PII • Credit reports • Assets/Net Worth • Records on spending and borrowing **Academic / Research Information** • Library transactions (e.g., catalog, circulation, acquisitions) • Unpublished research or research details or results that are not regulated or considered confidential data • Non-anonymous faculty course evaluations • Private funding information **Anonymous Donor Information** Last name, first name or initial (and/or name of organization if applicable) with any of the following: • Gift information, including amount and purpose of commitment **Other Donor Information** Last name, first name or initial (and/or name of organization if applicable) with any of the following: • Telephone/fax numbers • E-Mail, URLs • Employment information • Family information (spouse(s)/partner/ guardian/children/ grandchildren, etc.) **Management Data** • Detailed annual budget information • Conflict of Interest Disclosures • University's investment information **Systems/Log Data** • Server Event Logs **Research Data** • Research data that is private but not protected by law.	• Dates of current employment, position(s) • ID card photographs for University use **Specific for students:** • Class year • Participation in campus activities and sports • Weight and height (athletics) • Dates of attendance • Status **Business Data** • Campus maps • Job postings • List of publications (published research)