Policies and Procedures

SECTION: **Administration**	*NO.* **2.4.4.**		
CHAPTER: **Information Technology**	*ISSUED:* 4/7/06	*REV. A* 3/14/12	*REV. B*
POLICY: **Log Management Policy**	*PAGE 1 OF 2*		

PURPOSE

The purpose of this policy is to establish a requirement to enable and review logs on Creighton IT resources that store, access or transmit data classified by Creighton as Confidential or Private.

SCOPE

This policy covers all Creighton data which is available currently, or which may be created, used in the future. This policy applies to all individuals who maintain affected systems or data.

POLICY

IT resources that store, access or transmit data classified, by Creighton University, as Confidential or Private shall be electronically logged. Logging shall include system, application, database and file activity whenever available or deemed necessary.

- Logging shall include creation, access, modification and deletion activities.
- Log files shall be regularly examined for access control discrepancies, breaches, and policy violations.
- Data custodians or device managers are responsible for developing appropriate processes for monitoring and analyzing their logs.
- Individuals shall not be assigned to be the sole reviewers of their own user activity.
- System activity review cycles shall include review of audit logs minimally every 30 days and may include daily exception reporting.

DEFINITIONS

Confidential Data
A class of data whereby its unauthorized disclosure, alteration or destruction could result in significant risk to the mission, safety or integrity of the University and/or its constituents.

Private Data
A class of data whereby its unauthorized disclosure, alteration or destruction could result in moderate risk to the mission, safety or integrity of the University and/or its constituents.

Device Managers
Entity responsible for maintaining or managing a class of information systems.

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 are responsible for assigning the classifications categories to their data, and have the primary responsibility for ensuring the appropriate use and security of the data.

Date Custodians are responsible for identifying the systems that must be reviewed based on the classification assigned by the data owners, the information on these systems that must be reviewed, the types of access reports that are to be generated, and the individual(s) responsible for reviewing all logs and reports. The data custodians are also responsible for ensuring appropriate evidence of regular log review is happening in accordance with this policy.

Information Security Office is responsible for verifying that a review process has been implemented in an effective manner.

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 Classification 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.