Policies and Procedures

SECTION: **Administration**	*NO.* **2.4.3.**		
CHAPTER: **Information Technology**	*ISSUED:* 4/7/06	*REV. A* 3/14/12	*REV. B*
POLICY: **Sanction Policy**	*PAGE 1 OF 2*		

PURPOSE

The purpose of this policy is to outline Creighton University's procedures as it pertains to non-compliance with University's information technology policies.

SCOPE

This policy applies to all faculty, staff, students, residents, postdoctoral fellows, and non-employees (including visiting faculty, courtesy, affiliate, and adjunct faculty, industrial personnel, and others) who collect, maintain, use, or transmit Creighton's data in connection with activities at Creighton University (CU).

POLICY

Creighton University will appropriately discipline employees and other workforce members for any violation of information technology policy or procedure to a degree appropriate for the gravity of the violation. These sanctions include, but are not limited to, re-training, verbal and written warnings and other disciplinary action in accordance with University procedures.

In addition, workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of an individual's information are subject to criminal investigation and prosecution or civil monetary penalties.

Creighton University will investigate any security incidents or violations and mitigate to the extent possible any negative effects that the incident may have had in a timely manner.

Creighton University and its workforce members will not intimidate or retaliate against any workforce member or individual that reports the incident.

DEFINITIONS

Creighton Data
Any data owned or entrusted to Creighton University.

Security Incident
Any adverse event that affects the confidentiality, integrity, or availability of data or systems.

Workforce Member
Any faculty, staff, students, residents, postdoctoral fellows, and non-employees (including visiting faculty, courtesy, affiliate, and adjunct faculty, industrial personnel, and others) who collect, maintain, use, or transmit Creighton's data in connection with activities at Creighton University.

Sensitive Data
Data generated by or entrusted to Creighton University which meets the definitions of Confidential or Private data as defined by the Data Classification Policy of Creighton University.

RESPONSIBILITIES

All individuals identified in the scope of this policy are responsible for compliance with any sanction that is applied to them under this policy

Information Security Office is responsible for reviewing reported security incidents and violations of security policy and levying, based on the gravity of the breach, appropriate sanctions upon the workforce member

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.