Policies and Procedures

SECTION: Administration

CHAPTER: Information Technology

POLICY: Risk Management Policy

PURPOSE

The purpose of this policy is to ensure that Creighton University is properly addressing the risks inherent in operating and maintaining information systems required for continued operations.

SCOPE

This policy covers all data and information systems owned, operated, leased, or in the care of Creighton University as well as those who utilize them.

POLICY

Creighton University must conduct a regular, accurate, and thorough assessment of the risks and vulnerabilities to its information systems and electronic resources. Security controls must be implemented for each system to reduce risks and vulnerabilities to a reasonable and appropriate level. Creighton University must also regularly evaluate these measures and safeguards to ensure their effectiveness.

Any new system must have a risk assessment performed prior to it promotion into production environments.

DEFINITIONS

Electronic Resources – All computer related equipment, computer systems, software, networks, facsimile machines, voicemail and other telecommunications facilities, as well as all information or data contained therein.

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

Security Controls - Mechanism, either technical or procedural, designed to reduce risk.

RESPONSIBILITIES

Information Security Office is responsible for development of a risk management program and for conducting risk analysis of University systems.

Device Managers are responsible for assisting the Information Security Office in the performance of the risk analysis and for implementing security measures and safeguards identified to mitigate risk.

Vice President for Information Technology is responsible for setting and defining the acceptable levels of risk for University systems.

Change Advisory Board will review all new systems to ensure an initial Risk Assessment has been conducted prior to moving new systems into production.
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

Risk Management Program
Change Advisory Board Operating Procedures

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.