PURPOSE

This policy ensures Creighton adhere to all applicable federal laws and regulations, and maintains a security infrastructure that adequately protects sensitive information.

Regular reviews of Creighton’s security infrastructure against industry standards, best practices, and federal laws will help ensure Creighton complies with laws and regulations, Creighton University polices and standards. This certification process will demonstrate and document that Creighton’s computer systems and networks meet basic security criteria.

SCOPE

This policy applies to the Information Technology infrastructure at Creighton University.

POLICY

Creighton’s security infrastructure must be evaluated, on a regular basis, to determine that technical security controls are implemented and comply with industry standards.

DEFINITIONS

Evaluation
Evaluation is the process of determining whether technical security controls are implemented and comply with specified criteria

RESPONSIBILITIES

Information Security Office is responsible for ensuring an evaluation is performed on a regular basis.

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 STANDARDS

Information Security Philosophy
EXCEPTIONS

Requests for an exception to this Policy must be submitted via the Policy Exception Request Form. All exception requests will be handled in accordance with the Information Security Exception Policy and Standard.

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.