Policies and Standards

SECTION: Security

CHAPTER: General

POLICY: Information Security Governance Policy

PURPOSE

Creighton University strives to protect all of its resources, one of which is its information, regardless of the format or media used to generate, store, display or manipulate it. It is essential that all system users adhere to all Creighton security policies when using Creighton’s network. The purpose of this policy is to outline Creighton’s requirements to which all system users must adhere when using Creighton’s network.

SCOPE

This policy applies to all members of the Creighton University community (staff, faculty, students, contractors, consultants, temporaries, visitors, etc.) while using Creighton’s computing or networking resources. All users are expected to be familiar with and comply with this policy.

POLICY

By connecting to Creighton University’s network, all individuals agree to the appropriate use of all university resources, including university, patient, and student information and supporting systems and infrastructure, as defined in the specific security policies, standards and guidelines.

Such documents outline user responsibilities with respect to passwords, personal computer security, anti-virus protection, personal firewalls for offsite computing, data confidentiality and encryption, Internet use, unauthorized or illegal access, and use of malicious code. References to the policies, standards and guidelines are provided below:

- Acceptable Use Policy
- Strong Password Construction Standard
- Access Control Policy
- User ID Policy
- Remote Access Policy
- Malicious Code Prevention Policy
- Malicious Code Policy
- Data Classification Policy
- Cryptography Policy
- Server Registration
- Encryption Standard
- Network Security Policy
- Physical Security Policy
- Computer Security Policy
DEFINITIONS

Creighton University's network
The “network” is defined as any device connected, either wired or wireless, to Creighton’s IT infrastructure. Creighton University’s network is also referred to as JayNet.

Information Security
The Information Security Department is a subset of the University’s Information Technology organization. The Information Security Department is made up of the University’s Information Security Officer and an Information Security Engineer. The Information Security Department has sole responsibility of the security of the Creighton University network.

RESPONSIBILITIES

Network Users are ultimately responsible for adhering to this policy, regardless of their level or capacity. Additionally, Creighton supervisors must ensure that all personnel reporting to them are aware of, understand, and comply with this policy.

Information Security has the sole authority to update, communicate and enforce this policy as necessary, which includes the granting of any exceptions.

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
Information Security Exception Policy

EXCEPTIONS

None.

VIOLATIONS/ENFORCEMENT

Internal Use Only
DRAFT
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.