PURPOSE

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Creighton University. Effective implementation of this standard will minimize unauthorized access to Creighton confidential information and technology.

SCOPE

This policy applies to server equipment owned and/or operated by Creighton University, or server equipment physically connected to Creighton’s network. Desktop machines and lab machines are not relevant to the scope of this policy.

STANDARD

Ownership and Responsibilities
All internal servers deployed at Creighton University must be owned by an operational group that is responsible for system administration.

- Servers must be registered within the University’s Network Registration Database (NetReg). At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
  - Information in NetReg must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

General Configuration Guidelines
- Operating System configuration should be in accordance with approved Information Security guidelines.
- Services and applications that will not be used must be disabled where practical.
- All patches/hot-fixes recommended by the equipment and software vendor must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. System Administrator must have processes in place to stay current on appropriate patches/hotfixes.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
Policies and Standards

SECTION: Security

CHAPTER: General

POLICY: Server Security Standard

• Servers should be physically located in an access-controlled environment.

• Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Logging

• All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  o All security related logs will be kept online for a minimum of 1 week.
  o Daily incremental tape backups will be retained for at least 1 month.
  o Weekly full tape backups of logs will be retained for at least 1 month.
  o Monthly full backups will be retained for a minimum of 2 years.

• Security-related events will be reported to the Information Security Officer, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
  o Port-scan attacks
  o Evidence of unauthorized access to privileged accounts
  o Anomalous occurrences that are not related to specific applications on the host.

Compliance

• Audits will be performed on a regular basis by Information Security or Creighton University’s Internal Audit Department.

DEFINITIONS

Server
A server is a computer that provides services to other computer or users.

RESPONSIBILITIES

Systems Administrators are responsible to ensure all networked devices under their control adhere to this standard.

Information Security Officer is responsible for ensuring all servers adhere to this standard.

REFERENCES TO APPLICABLE STANDARDS

Information Security Philosophy
Information Security Governance Policy
Information Security Exception Policy
Network Security Policy

EXCEPTIONS

Internal Use Only
DRAFT
Requests for an exception to this standard must be submitted via the [Policy Exception Request Form](mailto:infosec@creighton.edu). All exception requests will be handled in accordance with the Information Security Exception Policy and Standard.

**VIOLATIONS/ENFORCEMENT**

Any known violations of this standard should be reported to the University's Information Security Officer at 402-280-2386 or via e-mail to [infosec@creighton.edu](mailto:infosec@creighton.edu).

Violations of this standard can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with University policies.

The University may advise law enforcement agencies when a criminal offense may have been committed.