Policies and Procedures

SECTION: **Administration**	*NO.* **2.4.48.**		
CHAPTER: **Information Technology**	*ISSUED:* 3/14/12	*REV. A*	*REV. B*
POLICY: **Configuration Standards**	*PAGE 1 OF 2*		

PURPOSE

Protect University data and information systems by ensuring a consistent, secure configuration across devices.

SCOPE

This policy applies to all information systems at Creighton University, including but not limited to, desktops/laptops, servers, network equipment, printers, mobile devices, and storage systems that store, process, or transmit University data.

POLICY

Information systems that process, transmit, or store University data must be configured in accordance with the applicable standard for that class of device or system. Standards must be written and maintained by the area or team responsible for the management of the system in conjunction with the Information Security Office.

Standard software deployments, such as a database or web server, should have a standard configuration maintained by the group responsible for managing the software.

Before being deployed into production, a system must be certified to meet the applicable configuration standard in accordance with the **Certification and Accreditation Procedures**.

DEFINITIONS

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

Configuration Standard
A document or collection of documents that describe how a device should be configured.

RESPONSIBILITIES

Device Managers are responsible for developing and publishing configuration standards for the devices over which they have primary responsibility.

The Information Security Office is responsible for reviewing and approving the standards in conjunction with the Device Managers.

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

Change Management Policy
Desktop configuration standard
Server configuration standard
Printer configuration standard
Network device configuration standard
Mobile device configuration standard

EXCEPTIONS

Any exception to this policy must be approved by the Information Security Office. Exceptions to applicable standards must be documented and maintained by the team responsible for the standards.

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.