**Policies and Standards**

**SECTION:** Security  
**CHAPTER:** General  
**POLICY:** Network Registration Policy

**PURPOSE**

Creighton University must protect its network from internal and external interference and possible attack. Many divisions/departments have varying degrees of expertise and varying perspectives on the risk associated with connecting networked devices to Creighton’s network. Networked devices that are not properly configured, patched, or maintained add unnecessary risk to Creighton. In addition, Creighton’s security infrastructure restricts certain services on different segments of the network.

In order to provide for consistent, professional matching of risks to controls and to ensure networked devices function as intended, it is necessary for all devices to be known to the Information Technology Division and Information Security Office.

**SCOPE**

This policy applies to all devices connected to Creighton’s network.

**POLICY**

Each networked device, no matter its location on the Creighton network, must be registered with the Information Technology Division.

**DEFINITIONS**

**Networked Device**
A networked device is any piece of equipment that directly connects to Creighton’s network, either via wired or wireless connection; such as personal computers, laptops, servers, network printers, wireless access points, switches, routers, etc.

**RESPONSIBILITIES**

- **Systems Administrators** are responsible to ensure all networked devices under their control are properly registered in the central database.
- **Information Security Officer** is responsible of the maintenance and administration of the device database.

**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**

Internal Use Only
DRAFT
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 Governance Policy

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.