Policies and Standards

SECTION: Security
CHAPTER: General

POLICY: Network Security Standard

PURPOSE

This Standard supports the Network Security Policy and identifies additional detail for the implementation of the policy. This Standard provides an overview of the applicable uses of the Creighton Network.

SCOPE

This standard 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 standard.

STANDARD

Security Patches

All devices connected to Creighton’s network must maintain reasonable current patch levels.

- The owner of any computing device that is connected to the Creighton Network is responsible for maintaining the security of the device. This responsibility requires that you maintain patches, hotfixes, updates, BIOS updates, ROM pack updates, etc. in an effort to prevent known vulnerabilities from degrading the Network.
- Personal computers running Microsoft Windows should routinely (at least weekly) run the Windows Update function and download and install applicable security patches that are identified as Critical Updates.
- Non Windows based personal computers are also required to maintain security patch levels.
- Non PC devices like PDA, game units, etc are the owners responsibility, and must be maintained in a manner that does not negatively impact overall Network performance.
- If users are not willing to accept security responsibility for network connected devices, they should not be connected to Creighton’s Network.
- Failure to maintain network connected devices in a secure manner force the Information Security Department or Creighton’s IT department to remove access to these devices. Repeated violations may lead to revocation of all network privileges for the applicable device owner.

Virus/Worm Infection

See the Malicious Code Policy and Malicious Code Prevention Standard for more information.
Unauthorized Devices

No users may connect devices to the network which may negatively impact other users’ ability to use the network. Such devices include, but are not limited to:

- Wireless Access Points
- DHCP servers or any device that acts as a DHCP server
- Any device that consumes an disproportionate amount of network bandwidth

Routine Network Scans

Creighton University will routinely scan Creighton’s Network for devices vulnerable to known security weaknesses, computers not running Creighton’s antivirus software, and devices which could negatively impact the performance of the overall network. No single device is more important than the network as a whole, therefore:

- Any device connected to the Creighton Network which is vulnerable to attack may be removed from the network until the owner can prove the device has been properly patched.
- Any computer connected to the Creighton Network which is infected with a virus or not running Creighton’s antivirus software may be removed from the network until the owner can prove the virus has been removed and Creighton's antivirus software is installed.
- Any computer connected to the Creighton Network which has the Creighton antivirus software installed but is not reasonable current on virus definition files may be removed from the network until the owner can prove current virus definition files are installed.
- Any device determined to have weak passwords on Administrative accounts may be removed from the network.
- Any device connected to the Creighton Network which degrades the performance of the network may be removed from the network.

DEFINITIONS

Network Connected 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.

Security Vulnerabilities
A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to compromise the system’s confidentiality, integrity, or availability.

Patched
**Policies and Standards**

<table>
<thead>
<tr>
<th>SECTION</th>
<th>NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>CHAPTER:</td>
<td></td>
</tr>
<tr>
<td>General</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>POLICY:</th>
<th>PAGE 3 OF 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security Standard</td>
<td></td>
</tr>
</tbody>
</table>

The process of finding, testing, and installing a modification (patch) to software that fixes an error in an application already installed on a system, patches are generally supplied by the vendor of the software.

**RESPONSIBILITIES**

**Creighton Network Users** are responsible to ensure all networked devices under their control are properly patched against known security vulnerabilities, protected against virus/worm infections, and do not impact other users use of the network.

**Systems Administrators** are responsible for taking all reasonable action to contain the effects of any system that is infected with a virus or other malicious software.

**Information Security Officer** is responsible for ensuring network users adhere to this standard.

**ADMINISTRATION AND INTERPRETATIONS**

This standard 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 standard at any time. This standard does not constitute a contract between the University and its faculty or employees.

**REFERENCES TO APPLICABLE STANDARDS**

- [Information Security Philosophy](#)
- [Information Security Governance Policy](#)
- [Information Security Exception Policy](#)
- [Malicious Code Prevention Policy](#)
- [Malicious Code Prevention Standard](#)
- [Network Security Policy](#)

**EXCEPTIONS**

Requests for an exception to this standard 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 standard 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 standard 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.