**Policies and Standards**

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

<table>
<thead>
<tr>
<th>CHAPTER:</th>
<th>ISSUED:</th>
<th>REV. A</th>
<th>REV. B</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**POLICY: Malicious Code Policy**

**PURPOSE**

Data has a value to Creighton University, and malicious program code has the ability to destroy or alter that data. Furthermore, the reputation of the University could be damaged if malicious software code is distributed through Creighton’s network. This document describes the University’s policy prohibiting malicious program code.

**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**

Members of the Creighton community are not permitted to use Creighton University resources to install, run, copy, store, distribute or develop any form of malicious software code intended to obtain, destroy, secretly install or modify information/data stored, run or used on any computer system.

Members of the Creighton community are not permitted to use Creighton University resources to run or manipulate software applications or programs to perform a malicious function which can obtain, destroy, secretly install or modify information/data stored, run or used on another computer system.

**DEFINITIONS**

None.

**RESPONSIBILITIES**

*System Users* are responsible for adhering to this policy.

**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 Governance Policy
Information Security Exception Policy
Malicious Code Prevention Policy
Malicious Code Prevention Standard

EXCEPTIONS

None.

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.