Acceptable Use Policy

1.0 Overview
Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Ohio Northern University. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Ohio Northern University employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose
The purpose of this policy is to outline the acceptable use of computer equipment at Ohio Northern University.

3.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other workers at Ohio Northern University, including all personnel affiliated with third parties.

4.0 Policy

4.1 General Use and Ownership
Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted.

For security and network maintenance purposes, authorized individuals within Ohio Northern University may monitor equipment, systems and network traffic at any time.

Ohio Northern University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information
The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

Because information contained on portable computers is especially vulnerable, special care should be exercised. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3 Unacceptable Use
Under no circumstances is an employee of Ohio Northern University authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Ohio Northern University-owned resources.
The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

**System and Network Activities**
The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
- Unauthorized copying of copyrighted material
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
- Introduction of malicious programs into the network or server
- Revealing your account password to others or allowing use of your account by others.
- Using a Ohio Northern University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Ohio Northern University account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication.
- Port scanning or security scanning is expressly prohibited unless prior notification is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Ohio Northern University employees to parties outside Ohio Northern University.

**Email and Communications Activities**

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Ohio Northern University's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Ohio Northern University or connected via Ohio Northern University's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

**5.0 Enforcement**
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**6.0 Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>Unauthorized and/or unsolicited electronic mass mailings.</td>
</tr>
</tbody>
</table>