Acceptable Use Policy

General Policy

Effective Date: January 8, 2009
Revised: November 21, 2013
Status:

__ Draft
__ Under Review
_X_ Approved
__ Obsolete

Responsible University Officer:
Vice President for Information Services, CIO

Responsible Coordinating Office:
Office of Information Services

Version 1.1

REVISION HISTORY

Draft: January 8th, 2009
Final Draft: November 21, 2013

OVERVIEW

Cardinal Stritch University requires that all individuals accessing University electronic resources or using University systems to access non-University electronic resources abide by the standards of acceptable use set forth in this policy.

The University cannot be held accountable for actions which an individual takes which are contrary to this or any other University policy, are contrary to the mission and goals of the University or are contrary to generally acceptable actions.

The University cannot be responsible for content or actions which originate on non-University systems.

The University reserves the right to change any portion of this policy at any time and to limit or restrict use of its electronic resources including but not limited to limiting or restricting access to non-University electronic resources accessed through University systems.

PURPOSE

The purpose of this policy is to outline acceptable use of computer and electronic resources at the University which is both reasonable and responsible. Responsible use of resources is necessary to ensure that resources are available to all when they are needed and that the individual and the University are protected from harm.
Acceptable Use Policy

SCOPE

This policy applies to all individuals who use, access or control University electronic resources. This includes but is not limited to students, faculty, staff, contractors, vendors, guests, visitors and any other user who uses University owned or controlled electronic resources.

POLICY

This policy sets forth general expectations regarding the use of University electronic resources, systems, data and information. This policy does not override applicable international, federal, state, local or other statutes. Individuals who access University resources are responsible for exercising good judgment regarding acceptable use.

General

- No University resource may be used in a manner or for a purpose that violates University policies or which is illegal or unethical.
- Use of University resources and systems for commercial purposes, except where explicitly approved, are strictly forbidden.
- Any action which would result in loss of data, corruption of data, loss of use or degradation of performance of any University resource or system or which in any way would have negative impact on other individuals or the University will not be tolerated.

Network

- Any device that attempts to circumvent security measures, mask the identity of the user, cause disruption of service, scan network ports, discover and/or exploit vulnerabilities of other devices on the network or capture or view data not intended for the recipient is strictly prohibited.
- The individual in control of any device connected to the network is responsible for the security of and traffic generated by that device regardless of origin. Any device which is generating unwanted traffic will be removed from the network and may not be reconnected to the network until all issues have been resolved.
- University networks may not be used to gain unauthorized access to non-University systems or to access systems or materials which are illegal or otherwise prohibited.

Computers

- University owned computers for student use are available in computer labs and public spaces throughout the University.
- Use of non-public University owned computers, including but not limited to staff computers, faculty computers, servers and control systems by non-authorized users is prohibited.
Acceptable Use Policy

• All computers which are connected to University networks or systems, including but not limited to student and privately owned computers, are required to have all current operating system and software patches installed, to have University approved anti-virus software installed and operating with the latest virus definitions and to be in good working condition.
• Loss, damage or theft of University owned equipment must be immediately reported to appropriate University staff.

Email

• Any activity which can be reasonably assumed to be offensive including but not limited to sending unsolicited email (SPAM, junk mail or Phishing Attempts), harassing or threatening email, creating or forwarding chain letters is prohibited.
• Unauthorized use or access of other users email, forging or manipulation of email headers or falsely representing the University or other individuals in any manner is forbidden.
• Sending or storing excessive amounts of email or emails of excessive size is not allowed.
• Extreme caution should be used when accessing email from unknown senders, particularly when there are attachments or links within the message. Messages such as these often contain viruses or other malicious code.
• Always be skeptical of offers that seem to be too good to be true and of requests for personal information. You should never provide account login information, passwords, social security numbers, bank account numbers or other highly confidential personal information via email or via web links from email.

Phone

• Use of University owned or controlled phone numbers to conduct non University business, including but not limited to solicitation of funds, sales and support is prohibited.
• Making non-emergency calls to 911 or other emergency services is strictly prohibited.
• Any call which may be deemed harassing or prank calls of any kind are prohibited.

FAX

• FAX machines must be setup to display the correct phone number of the FAX machine on all outgoing FAX.
• FAX machines cannot be used to transmit sensitive data, including but not limited to personally identifiable information.

Data

• Unauthorized access of University data is prohibited. Authorized use of data is covered in the Data Access Policy.
Acceptable Use Policy

- It is the responsibility of each user to protect their own data, including making local backups of critical files where central backups are not already being made; ensuring that systems are routinely scanned for virus, malware and other malicious programs; and ensuring that systems are up to date with relevant security patches and updates.
- Sensitive data, including but not limited to personally identifiable information may not be backed up or stored on local machines or media. See the Data Access Policy for further restrictions.
- Sensitive data, including but not limited to personally identifiable information may not be transmitted over insecure methods, including but not limited to FAX and unencrypted email.

Security and Privacy

- It is the responsibility of each individual to protect privacy and information.
- Passwords should be changed every six months and should be secure, easy to remember and hard to guess. Secure passwords are passwords that are at least 8 characters long which contain a combination of upper and lower case letters, numbers and special characters and which do not contain recognizable words, phrases, dates or other guessable combinations. Authorized users are responsible for the security of their passwords and accounts.
- Only authorized users will have administrative access on University machines.
- Attempts to access accounts for which you are not authorized is strictly prohibited. In the event that a system administrator needs to access private information or another account such activity will be documented and subject to review.

Copyright

- Copying, storing, displaying or distributing copyrighted material using University resources or systems without the express permission of the copyright owner, except as otherwise allowed under copyright laws, is prohibited.

ENFORCEMENT

Violations of these policies may result in the immediate suspension and possible revocation of access to University IT resources and systems. Serious violations will be referred directly to the appropriate University or outside authorities. Unauthorized use of University resources is a criminal offense. Penalties may range from suspension or dismissal from the University to civil or criminal prosecution.