University of Illinois
University Administration

Acceptable Use of Computing and Network Resources Policy

Issue Date: February 1, 2008

PURPOSE

This policy describes the acceptable use of computing and network resources at the University of Illinois, University Administration (UA). It is based on University policies which were developed to comply with all applicable laws and regulations and is intended to protect UA employees and the University from damaging actions including lawsuits, virus attacks, and the compromise of network systems and services. This policy is not intended to impose undue restrictions that are contrary to University of Illinois' established culture of openness, trust, and integrity.

APPLICABILITY

This policy applies to all employees, contractors, consultants, temporaries, and other individuals assigned to UA ("User"). This policy covers computer equipment and related software owned or leased by the University of Illinois, including but not limited to computers, application software, operating systems, data files, storage media, network accounts providing electronic mail, Internet browsing, FTP, login accounts and passwords.

Maintaining a secure and responsive network environment is a team effort involving the participation and support of every User of University technology resources. It is the responsibility of every technology User to know this policy and to conduct their activities accordingly. *Users must also comply with, and are subject to, the campus security and computer use policies of their primary campus location as well as other University policies.* Failure to comply with these policies could be cause for disciplinary action up to and including dismissal.

POLICY

1. Equipment and data stored on University computing resources are the property of the University of Illinois and intended to be used for University purposes.

   University supplied equipment, software and data remain the property of the University of Illinois. All items assigned to a User must be promptly returned when separation from the University occurs or is requested by the UA unit.

   University computing resources are to be used for University purposes. Employees' family members and friends are not permitted to use University assigned equipment.

   Information stored on UA systems is generally presumed to be a public record and UA cannot guarantee the confidentiality of such information. Authorized individuals may monitor, and access, equipment, systems, information and network traffic at any time in accordance with applicable laws and policies.

2. Equipment and data must be adequately secured to protect University resources.

   Users are responsible to secure their passwords and follow established practices for creating and changing passwords. Passwords must be changed at least annually. Effective passwords include combinations of letters, numbers, special characters with varying capitalization that are difficult for others to guess. Accounts, passwords, dynamic password token cards and smart cards must never be shared with others, including coworkers and family members.

Users must log off or software lock workstations if they will be left unattended, even for a short period of time. A password-protected screensaver should also be set to 30 minutes or less (15 minutes or less in areas that view sensitive data).

High risk or confidential data should not be stored on local storage devices (laptops, workstations, flash drives, CDs, etc.) Temporary local storage of these types of data is acceptable if the data are needed for offline work and the files are encrypted. Files containing sensitive data, such as passwords, UINs, equipment or system configuration information, and proprietary program source code (including information stored in local Outlook or Exchange folders) must also be encrypted on local storage devices. UA requires all Users to comply with the University of Illinois' Data Classification Policy, which is part of the University Information Security Policy.

All computers connected to the University network (including remote connections) must have current virus protection software executing on the machine. Users must not disable virus protection software. Users must exercise extreme caution before opening email attachments received from unknown senders.

Users must promptly follow appropriate security incident procedures to report any damage to or loss of computer hardware, software, or compromise of confidential and restricted data. To access the security incident procedures, please see https://nessie.uihr.uillinois.edu/pdf/policy/ua/SecurityBreachIncidents.pdf.

3. Remote computing must be authorized, used for University business, and conducted via secure network communications.

Remote computing is any connection made to the University of Illinois network from a non-University site including access from home, hotels, conferences and public WiFi hotspots. University owned and/or personal equipment must comply with this policy. All University policies also apply to remote computing devices.

Users must annually obtain approval from their UA unit Director to access the University network remotely. This approval can be gained through completion of the Remote Computing Access Form, which can be found online at https://nessie.uihr.uillinois.edu/pdf/policy/ua/RemoteComputingForm.pdf. Access will only be granted to Users who demonstrate a need to perform University business remotely. Remote connections to the University network are intended only for University business purposes.

Use of personal equipment on the University network must be approved by the UA unit Director and AITS Security. Personal equipment must meet the same security protection standards as University provided equipment. In addition, remote computing equipment must be protected by approved firewall software.

Remote Users must connect securely to the University network using a University VPN connection. Users must not allow another computer to share the VPN connection on their machine (Internet sharing).

Public web applications requiring user authentication (e.g., Outlook webmail, NESSIE, CITRIX, etc.) may be accessed from publicly available equipment without using a VPN connection. Users must take the following precautions when using public equipment to access University web applications:

- Do not exchange files between public equipment and University systems.
- Completely close all browser sessions and log out of all University applications and return equipment to its appropriate login prompt to ensure that the next User will not have access to University services or data.
- Never leave the workstation while logged in or with any open browser session.
- Ensure that high risk information is not viewable by others who may be in the vicinity of the equipment.

4. Unacceptable Use

Any illegal activity under local, state, federal or international law is strictly prohibited when using UA equipment or connected to the University network.

The following lists are not exhaustive, but provide examples of unacceptable use of University computing resources.

Unacceptable System Activities

- Revealing your University supplied account password to others or allowing others use of your account.
- Circumventing user authentication or security to any University computing resource.
- Installation, copying or distribution of software products that are not appropriately licensed for use by the University of Illinois.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.
- Exchanging files through a peer-to-peer connection.
- Using University computing resources to procure or transmit material that is in violation of sexual harassment or hostile workplace laws or University policies.
- Using University computing resources to access or store sexually explicit material when there is no legitimate University purpose for such use.
- Making intentionally fraudulent statements of any kind originating from any University of Illinois account.

Unacceptable Network Activities

- Port scanning or security scanning.
- Executing any form of network monitoring which intercepts data not intended for the User's computer.
- Effecting security breaches or disruptions of network services. This includes, but is not limited to, accessing data for which the User is not an intended recipient, logging into a server or account that the User is not expressly authorized to access, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Note: Network monitoring activities, required for the normal performance of their duties, shall be permitted for system administrators, auditors and other certain technical staff.

Unacceptable Email and Communications Activities

- Posting the same or similar non-University-related messages to large numbers of newsgroups (newsgroup spam).
- Participating in "chain letters" or "pyramid" schemes of any type.
- Intercepting, eavesdropping, recording or altering another person's electronic message.
- Adopting the identity of another person in any message.
- Sending a message that violates University ethical practices, including but not limited to sending racially or sexually explicit or harassing messages and/or files.
- Using electronic communication systems for any non-University of Illinois commercial purpose.
- Violating copyright or other intellectual property laws.
- Using electronic communication systems for purposes of political lobbying or campaigning.

5. Exceptions

Exceptions to this policy must be approved by the University Vice President and Chief Financial Officer and will be communicated to AITS Security.

Appendix A
University and Campus Policies Related to University Administration
Acceptable Use of University Computing and Network Resources Policy

Office of Business and Financial Services – ***Business and Financial Policies and Procedures Manual***

- Section 19.5 - Information Security Policy – The University of Illinois (http://www.obfs.uillinois.edu/manual/central_p/sec19-5.html)

- Section 19.8 - Software Copyright Compliance (http://www.obfs.uillinois.edu/manual/central_p/sec19-8.html)

University Ethics

- State Officials and Employees Ethics Act (5 ILCS 430) (http://ethics.uillinois.edu/policies/soeea.html)

- *University Code of Conduct* (http://ethics.uillinois.edu/policies/code.html)

- *Good Ethical Practice: A Handbook for Faculty and Staff at the University of Illinois* (http://ethics.uillinois.edu/resources/handbook.html)

Campus Computer Use Policies

- Chicago Campus - Acceptable Use Policy (http://www.uic.edu/depts/accc/policies/uicpol.html)

- Springfield Campus – Acceptable Use of Information Technology Resources (http://www.uis.edu/its/about/policies.html)

- Urbana Campus - Policy on Appropriate Use of Computers and Network Systems at the University of Illinois at Urbana-Champaign (http://www.fs.uiuc.edu/cam/CAM/viii/viii-1.1.html)