# Interim Policy on Appropriate Use of Computers and Network Systems at the University of Illinois at Urbana-Champaign

December18, 2001

Senate IT Committee version

## Table of Contents

## 1. Purpose

The University of Illinois at Urbana-Champaign provides extensive computing and network communications services. These services, known collectively as UIUCnet, are part of the campus infrastructure, and their purpose is to support the University's teaching, research, and service missions. Unless explicitly noted, these policies apply to all computing and network communications equipment in all units.

This document[1] addresses issues specific to University of Illinois computing and network usage. Sections 1 through 6 articulate policies regarding individual users of computers and networks; sections 7 and following summarize administrative protocols for computing and network administrators and should not be construed as creating additional rights for individual users. Other university and campus policies that address specific activities and behaviors, some of which are cited later in this policy, continue to apply to computing and network use. Individuals using campus computing and networking services should be particularly aware of policies that apply to discrimination, harassment, the use of copyrighted materials, and those that apply to the appropriate use of university resources. Many major policy documents can be found on the web site *Looking Up Campus Information* (LUCI) at: http://www.admin.uiuc.edu/luci/.

Computing and network communications are changing rapidly both in terms of technology and application, and the University reserves the right to amend this policy at any time. The version posted on the web (at http://www.admin.uiuc.edu/cam/) is the governing policy.

All members of the campus community are given notice of this policy by virtue of its publication, and are subject to it on the same basis. Ignorance of this policy does not relieve anyone of his or her responsibilities under it.

## 2. Underlying Principles

a) The principles of academic freedom[2] apply in full to electronic communications.

b) The use of computing and network services provided by the campus is subject to all applicable state and federal laws, as well as general University and campus policies.

c) All standards of behavior, courtesy, and etiquette that govern vocal and written communications also extend to electronic communications.

---

[1] Earlier versions of this policy document were entitled *UIUCnet Computing and Networking Policy.*

[2] The University's Statutes recognize prevailing standards for academic freedom. For a discussion of these concepts in our environment, please see the Website of the Office of Academic Human Resources at http://webster.uihr.uiuc.edu/ahrhandbook/chap3/resource_offc.html.

d) When the Office of the CIO[2] becomes aware of any use of UIUCnet that violates provisions of University policy, presents a security risk, or degrades services to others, it may suspend or terminate network access and use and/or notify appropriate disciplinary and/or legal authorities. Where possible, the Office of the CIO will provide prior notification of actions that affect network use and access. In all cases, the CIO or designee will provide timely notification of the reasons for said actions and will document the appeal process available to those affected. The responsibilities of the Office of the CIO include:

   i) The choice of protocols supported by the network,
   ii) The definition of campus standards necessary for efficient operation of the network and for the security of transmitted data and networked computers,
   iii) Application of network management policies adopted by the campus to ensure inter-operability of departmental local area networks (LANs),
   iv) Monitoring the overall system to ensure the reliability, robustness and security of the campus network infrastructure, and
   v) Serving as the campus representative to the Internet community and ensuring that the campus is a responsible member of that community.

## 3. Computers and Network Systems: UIUCnet Defined

The term *UIUCnet* is used here to denote the campus computer and data communications infrastructure at the University of Illinois at Urbana-Champaign. It includes the campus backbone and local area networks, all equipment connected to those networks (independent of ownership), and all equipment registered to any domain name owned by the University.

## 4. Proper and Authorized Use of UIUCnet

The Office of the CIO, through CCSO, is charged with ensuring the integrity of UIUCnet computers and communications. CCSO takes active steps to ensure the physical integrity of the infrastructure, including routine monitoring of performance and reliability. While neither CCSO nor the CIO Security Office routinely monitors appropriate use of UIUCnet by individuals, the CIO Security Office will respond to complaints or other notifications of inappropriate use. Units that provide access to UIUCnet are responsible for ensuring that use is limited to legitimate users and is consistent with University policies and contractual obligations that govern the software and services offered on UIUCnet. Use of UIUCnet is a privilege, not a right, and such use may be suspended or terminated at the direction of the CIO Security Office when, in its judgment, this policy has been violated by the user. The CIO or designee will provide timely notification of the reasons for suspension or termination and will document the appropriate appeals process.

---

[2] The Office of the Chief Information Officer (CIO) includes CCSO, which is responsible for the design, operation, and management of the computing and network communications services provided at the campus level, and the CIO Security Office, responsible for coordinating with members of the community on security issues and establishing security best practices.

a) **Purpose of UIUCnet, the campus computing and communications infrastructure:** UIUCnet exists to support the educational, research, and public service missions of the University, and its use should be limited to those purposes.

b) **Authorized Users:** The document *Authorized Users at the University of Illinois at Urbana-Champaign*, also available at (http://www.cio.uiuc.edu/policies.html), defines who may use UIUCnet, the types of accounts available, and the duration of access.

c) **Appropriate Use of UIUCnet:** No individual may use UIUCnet resources for commercial or profit-making purposes or other purposes unrelated to the mission of the University. As with all University computing and network facilities, UIUCnet may not be used for improper or illegal purposes, such as unauthorized use of licensed software, intentional efforts to breach security, sending unauthorized mass mailings, or the transmission of computer viruses.

   i) **Ownership of Network Identifiers:** University-supplied network identifiers (network IDs), University identification numbers, and computer sign-ons are the property of the University. The University may revoke these identifiers or sign-ons at any time.

   ii) **Responsibility to Maintain Privacy of Passwords:** Passwords associated with an individual's network IDs and computer sign-ons should not be shared without authorization. Compromised passwords may affect not only the individual, but also other users on campus or on the Internet.

   iii) **Proper Identity Required:** Electronic mail and other forms of electronic communication must carry the proper identity of the sender at all times. Information servers (e.g., Web servers) must display the email address and identity of the unit or person responsible for maintaining the information.

   iv) **Appropriate Use of Bandwidth:** As described in Section 10 below, bandwidth both within campus and connecting to the Internet is a shared, finite resource. Users of UIUCnet must make reasonable efforts to use this resource in ways that do not negatively affect others. Units may set guidelines on bandwidth utilization for purposes of resource allocation.

d) **Use by Faculty and Staff:** Use of UIUCnet by faculty and staff is also governed by the University's Standards and Ethics Handbook (see http://ethics.uillinois.edu/Handbook.htm).

i) **Passwords and University Units:** Faculty and staff, including student employees, must not under most circumstances share their passwords with others, even with supervisors. However, when limited access to university-related documents or files is required specifically and solely for the proper operation of University units *and* where available technical alternatives are not feasible, exceptions are allowed under an articulated unit policy that is available to all affected unit personnel. Each such policy must be reviewed by the unit executive officer and submitted to the CIO for approval.

ii) **Use Unrelated to University Positions:** Use by University employees unrelated to their University positions must be limited in both time and resources and must not interfere in any way with University functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.

e) **Use by Students**: Use of UIUCnet by students is also governed by the Code of Policies and Regulations Applying to All Students, available at: http://www.uiuc.edu/admin_manual/code/code_contents.html (See, for example, Rule 11.E.12).

i) **Responsibility for Passwords:** Students must not share their passwords with others, even with friends. Students are responsible for ensuring that their computers are secure from unauthorized use. When working as employees, students are covered under section d) above.

f) **Use by Non-University Users:** Non-University individuals and organizations may not use UIUCnet, except as specified by written University contract. It is the responsibility of the contracting unit to ensure that content and usage of UIUCnet adhere to all general University policies and that resources are provided in a secure manner. For purposes of this policy, a contracting organization shall be deemed to be a unit of the University, and designated officials of the organization may exercise the responsibilities of University administrators as described in this policy, except that the contracting organization may not exercise or supercede the authority of the CIO.

i) **Limited to University-related activities:** Legitimate non-University users may use their University-provided accounts and Internet access only in conjunction with their authorized University-related activities.

ii) **Authorized Organizations:** UIUCnet resources may be used in support of organizations identified in Authorized Users at the University of Illinois at Urbana-Champaign ( http://www.cio.uiuc.edu/policies.html). While it is appropriate for the home pages of these organizations to provide some information about external organizations, clubs, commercial entities, etc., UIUCnet-connected equipment may not be the primary repository for that information.

iii) **University-sponsored External Entities:** Any University program that, in the interest of collaboration, wishes to provide an external entity with Internet access or to host non-University materials on a UIUCnet-connected server must first consult with CCSO about alternatives and secure approval from the Office of the CIO.

iv) **Network Services Limited to Authorized Users at the University of Illinois at Urbana-Champaign:** Except as indicated here, unless permission has been granted in an Allied Agency agreement or otherwise obtained in writing from the CIO or designee, a system connected to UIUCnet must not be used to provide network services or access to any person

or organization not identified in the University of Illinois at Urbana-Champaign Authorized Users (see above).

## 5. Web Policy Statement

The campus is currently developing a Web policy, which will be included here when complete.

# 6. Protection of Information in Electronic Media

### 6.1 Status of Information in Electronic Media

Information and data maintained in electronic media on University computer systems are protected by the same laws and policies, and are subject to the same limitations, as information and communications in other media. Before storing or sending confidential or personal information, campus users should understand that most materials on University systems are, *by definition,* public records. As such, they are subject to laws and policies that may compel the University to disclose them. The privacy of materials kept in electronic data storage and electronic mail is neither a right nor is it guaranteed.

### 6.2 Examination of Contents of Electronic Messages and Files

Unless required by law or by authorized administrative approval to do otherwise, campus and unit-level system administrators will not examine the contents of electronic messages and files and will make every reasonable effort to protect them from unauthorized inspection, subject to the following:

a) **Contents of Email:** a system administrator in the course of routine maintenance or in order to dispose of undeliverable messages might see the contents of electronic messages. In addition, electronic mail systems store messages in files (e.g., the file containing a user's inbound mail.) These files are copied in the course of system backups, and these backup copies may be kept long after original messages were deleted.

b) **System Files and Logs:** In the course of resolving system performance or security problems, system administrators may examine the contents of files that control the flow of tasks through the system or that grant unauthenticated access to other systems. This includes systems logs that document some activities of users.

c) **File and Directory Names:** File names and directory names are treated as public information and are not protected.

### 6.3 Process for Requesting Disclosure of Contents of Messages and Files

a) **Requesting Disclosure:** Requests for disclosure must be made in writing through regular reporting channels, consistent with the guidelines below. Requests for disclosure are made to the

campus Chief Information Officer (CIO), who is assigned the responsibility for implementing this policy and ensuring that the scope of the disclosure is limited to a legitimate University purpose. The CIO carries out these responsibilities in consultation with Legal Counsel and other appropriate offices. The CIO may designate an individual to act on his or her behalf in fulfilling these responsibilities. All authorizations by the CIO or designee will include specifications for the form and timing of notification to the person whose information is accessed or disclosed.

b) **Action While a Request is Pending:** While a request consistent with this process is pending or under consideration, the requesting unit executive officer may ask computer system administrators to take reasonable, necessary steps to maintain, store, or otherwise prevent the deletion or modification of the information being sought. This must be done in such a way as to maintain the privacy of said information until the requested disclosure is reviewed. The Office of the CIO may be able to advise units on appropriate procedures.

c) **Notification of Affected Individual(s):** When the CIO or a designated authorized unit administrator provides access to, and disclosure of, email messages and/or file content under provisions of external laws, regulations or applications of this University policy, the requesting administrator will normally notify *in advance* the individual(s) whose information is to be released, indicating the information to be released and the law, regulation or policy that governs the release. If individuals are not notified in advance, the CIO will be responsible for determining when notification is appropriate and for ensuring that such notification is carried out. Circumstances in which notification may be delayed include, but are not limited to, (1) the presentation by legal bodies of subpoenas or other instruments prohibiting advance notification, (2) situations where the safety of individuals is involved, or (3) investigations or inquiries conducted under published University policies.

d) **Conditions for Disclosure:** In the absence of legally compelled access or disclosure, the CIO is authorized to grant access to a user's file contents or electronic mail messages, or to give copies of them to any third party *within* the University only if *all* the guidelines below are met:
   i) The access or disclosure is requested in writing through regular University reporting channels, including the unit executive officer of the individual whose information is being disclosed and the next administrator in that reporting chain.
   ii) The reason for the requested disclosure serves a legitimate University purpose.
   iii) The disclosure is not invasive of legitimate privacy interests or unreasonable under the circumstances, e.g., in light of alternative means of acquiring the information or achieving the requester's purpose.
   iv) The nature and scope of the disclosure is submitted in writing to and approved by the CIO. This request is normally submitted by the approving executive officer indicated above.
   v) The affected individuals are notified in a timely manner in writing of any access or disclosure, consistent with section 6.3c above.

**6.4 Review of Disclosure:** UIUCnet users whose information is accessed or disclosed under the above provisions should use existing University complaint and/or grievance procedures when concerned about the application of this policy.

## 7. Responsibilities in Managing UIUCnet

This section outlines responsibilities in managing UIUCnet that may affect units and individuals.

a) **Network Design:** CCSO will work with any unit to develop or modify a network to meet unit needs. Needs directly related to the University's education, research, or public service missions have first claim on resources. Networks serving the Residence Halls, Certified Student Housing and other housing are unusual because of their high density and unique environment. Consistent with University policy, CCSO may require special restrictions on their use, if needed to protect the quality of service to those who share these networks.

b) **News Services**: CCSO offers news services, which may include news groups originating on- and off-campus, including commercially provided groups of interest to the campus community. CCSO will not review in advance or censor the content of the groups provided. However, if the presence of a news group is likely to impact campus services adversely or if a posting is in violation of law, CCSO may elect not to distribute that news group or may elect to remove that posting. Examples might include news postings that violate copyright law or news groups that generate burdensome amounts of traffic on the network or campus computers.

   i) Which news groups are provided and the retention period for news postings will be at the discretion of CCSO or the unit providing the service, based on input from the campus community and the availability of resources.
   ii) Professors have the right to moderate their class newsgroups.
   iii) A posting that falsifies the identity of the individual making the post constitutes impersonation and thus violates University policy, as well as potentially violating laws and regulations. Members of the community using University resources are expected to identify themselves using their campus network ID.

## 8. Network Design

CCSO is responsible for the design or approval of departmental local area networks (LANs) that are connected to the campus network and their connections to the campus backbone. The following subsections document policies and procedures relevant to these areas. The term LAN as used here refers to the routers, switches, repeaters, cabling and patch panels, but excludes servers and other computers.

a) **UIUCnet Address Space:** Only CCSO-approved domains may be operated within UIUCnet address space. Publicly accessible Domain Name Servers must be approved by CCSO before they are placed in service.

b) **Responsibility for Telecommunications Wiring:** CCSO is responsible for the telecommunications wiring system on the University of Illinois at Urbana-Champaign campus. If portions of this system are used in the construction of a LAN, all such use must conform to campus standards.

c) **Local Network Policies:** Network administrators and the owners of local networks may develop their own network policies, as long as they are not in conflict with campus or University policies. Unit-level policies may not restrict access to campus services, except where specific security concerns require it, and may not contravene policies stated here.

d) **Responsibility of Units:** Units are responsible for the uses of their local area networks and servers. In particular, units are responsible for ensuring that materials published electronically or otherwise placed on their servers are relevant and appropriate to the unit's mission.

e) **Licensing and other Restrictions:** Some servers connected to UIUCnet provide services or software that are restricted by licensing agreements to use by University students, faculty, and staff. Some licenses may further limit use to campus, one or more colleges or particular units. Servers must be configured so that restricted services or software are accessible only to those who are eligible.

f) **LAN Administrators:** Each LAN must have at least one designated administrator who is responsible for its administration and management, and whom CCSO may contact if it detects a problem.

## 9. Network Security

The security functions of commonly used desktops, servers, and communications technologies are often vulnerable, allowing unauthorized access to or viewing of system resources. A security violation on one machine may threaten security of other systems on the network, allowing unauthorized users to disrupt or damage interconnected systems. Because of this, each individual and unit has certain responsibilities to ensure that their systems are reasonably secure. This section describes security-related roles and responsibilities. It also describes circumstances under which UIUCnet user data can be collected and examined by an individual managing a LAN, server, or system.

a) **Responsibilities of Network Administrators:** It is the responsibility of every network administrator to have expertise sufficient to maintain appropriate levels of security and system integrity on local LANs. The CIO Security Office will document best practices and procedures for maintaining network security and integrity, in consultation with the campus community and peers nationally. CCSO provides training, consulting, and general support to network administrators.

b) **Ensuring Integrity of UIUCnet:** In the event that the CIO Security Office judges a LAN to present an immediate risk to the integrity of UIUCnet equipment, software, or data, or presents a risk to the external network (resulting in potential liability for the University), it may terminate or restrict the LAN's network connection without notice. If there is no immediate risk, the CIO Security Office will bring the matter to the attention of the LAN's network administrator. If unable to resolve the problem at this level, the Security Office will contact the unit executive officer or the next level administrator. In addition, if an individual system administrator of a multi-user system determines that an account presents an immediate security risk, he or she may inactivate the computer account without prior notice. The administrator must contact the CIO

Security Office in a timely manner to report and discuss the situation. In the course of ensuring the integrity of UIUCnet and local LANs, the CIO Security Office/CCSO and system administrators, respectively, may use tools, monitoring hardware and software, and log information as indicated here:

1) **Security Tools:** The CIO Security Office may use tools designed to locate security flaws in equipment connected to the campus network and will take appropriate steps to protect the privacy of data (as provided by this policy) in the process. When the CIO Security Office documents risks to security or network integrity, units are responsible for immediate responses to mitigate or remove the risk. Whether so notified or not, units are responsible for appropriate security with respect to equipment within their LAN.
2) **Network Monitoring Tools:** In order to solve network problems, campus and unit system administrators may employ software or hardware devices from time to time that capture contents of packets traversing the network, including email, Web, and other services. These monitoring tools will be used to monitor and improve the performance or integrity of the network. They will not be used to monitor or track any individual's network activity except under the special authorizations provided for under Section 6.
3) **System Log Files:** Managers of campus or unit systems and network services may log connections to their machines and services made via dialup or UIUCnet. The information recorded may include the source and destination for a connection, and session start and end times. Operators of multi-user systems may keep logs of activities on their systems. The logs may include login name, timestamps and commands issued. Network administrators may **not** monitor individual users' data or files except under special authorizations provided for under Section 6.

## 10. Bandwidth Guidelines

UIUCnet and its connections to the Internet are a shared, finite resource. While every effort is made to provide adequate bandwidth for University purposes, bandwidth may not be available for every use.

a) **New Applications:** Extensive use of new applications that require very large amounts of bandwidth on the campus backbone must be discussed with CCSO beforehand, so that appropriate planning can take place.

b) **Degrading Network Performance:** If use of a computing or network service by a project or individual seriously degrades network service to others, CCSO will try to help the project or individual obtain the needed service in a way that does not seriously impact others. If a network upgrade is required, the unit or user may be asked to pay all or part of the cost.

c) **Responsibilities of Network Administrators:** Network administrators are responsible for monitoring and managing traffic on their LANs to protect the quality of service from adverse impact by users whose applications require substantial bandwidth or other network resources.