Acceptable Use of Computational Resources

Policy Number: IT-9100-002

Policy Title: Acceptable Use of Computational Resources

Vice Chancellor/Associate Chancellor: Vice Chancellor for Innovation

Unit Responsible for Policy: Technology Solutions

Effective Date: March 4, 2022

Contacts: Chief Information Security and Privacy Officer

Policy Statement:

The University of Illinois Chicago ("university") is committed to a respectful, safe, and ethical environment for all members of the university community (“members”).

This policy applies to all academic, research, and administrative departments and offices at the University of Illinois Chicago; all university faculty, staff, students, alumni, applicants, visitors, contractors and affiliates (university “members’); and all resources in the university computing portfolio including: systems, network infrastructure, devices, facilities and applications (collectively referred to as “computational resources”), whether located on university property or accessed remotely.

Throughout this document, the physical network used to provide internal networking and Internet services at UIC will be referred to as the “UIC network." The term "LAN" will be used to refer to a subset of the UIC network, commonly known as a "subnet," or as a departmental local area network.

All users have a responsibility to use university computational resources in an efficient, ethical, and legal manner. Users of these resources are expected to abide by this policy, which is intended to preserve the utility and flexibility of computational resources, safeguard university data, protect the work of students, staff, and faculty, and preserve the ability to access network resources to which the university is connected.

Policy may exist at the system and university level that place additional restrictions on the permissible use of computational resources. Such policies take precedence when they are more restrictive.

Units may create policy that imposes additional restrictions on computational resources within their areas, but in instances where a unit policy is less restrictive, this policy applies.

Underlying Principles

The following general statements provide the basis for making the specific recommendations that appear here and for deriving answers to future policy questions.

1. Access to computational resources is a privilege and not a right.
2. The principles of academic freedom apply in full to electronic communications within the limits set within this and other university policies.
3. The use of computational resources provided by the university are subject to all applicable State and Federal laws and university policies.
4. Technology Solutions is responsible for the design, operation, and management of the computational resources provided to the university. This responsibility includes the choice of protocols supported by the network and the definition of campus standards necessary for efficient operation of the network or for the security of transmitted data and networked computers and is subject to change.
5. The standards of behavior expected of community members extend to the virtual environment as well.

Ownership

Computational resources are the property of the university and shall be used for legitimate university instructional, research, administrative, public service, and approved contract purposes.

University identifiers (NetIDs) and computer sign-ons are the property of the university. The university may revoke these identifiers or sign-ons at any time with due cause.

Individual Responsibility

All UIC members are assigned a university identifier (NetID) and are required to create a password associated with that NetID to access computational resources. Members may also be required to use a second form of authentication referred to as two factor authentication (2FA) through a device such as a phone app, SMS, or hardware token to access specific resources. Sharing of computational resources and passwords is prohibited and it is your responsibility to protect these access mechanisms by safeguarding your password and 2FA device.

Members may not attempt to disguise their identity, the identity of their account, or the device that they are using while accessing university resources. Use of software that masks the origin of network traffic when accessing non-university resources for privacy reasons is permissible. Members may not attempt to impersonate another person or organization. Members may likewise not misuse or appropriate the university's name, network names, or network address spaces.

Members are responsible for maintaining security controls that comply with university policy and standards on their personal equipment (laptops, mobile devices, etc.) that utilize university computational resources.

Acceptable Use

University computational resources are the property of the university and shall be used for legitimate university instructional, research, administrative, public service, and approved purposes.

Minimal personal use of computational resources may be permitted if it does not interfere with the university's or the employee's ability to carry out university business and does not violate the terms of this policy or university ethics rules, policies or guidelines. Members should keep in mind that sensitive personal information, other than that required for employment by the university, should never be transmitted or stored using computational resources.

Users of computational resources shall not violate any applicable law or ethics rules, policies or guidelines as a result of their use of such resources.

All users of computational resources must:

- Comply with copyright and trademark laws; this includes a prohibition on using the UIC network to illegally download or share copyrighted material such as software, movies, music, books, etc.
- Use only those computational resources they are authorized to use and use them only in the manner and to the extent authorized.
- Not share accounts and credentials with anyone. Account credentials are for use only by the individual to whom they are assigned.
- Refrain from unauthorized access, modification, or destruction of another person's computer files, communications, accounts, or other data.
- Refrain from installing or using unauthorized software, particularly software that may create security risks.
- Refrain from intentional access to or dissemination of pornographic material unless (1) such use is specific to work-related functions and has been approved a user's supervisor/unit manager or (2) such use is for scholarly or medical purposes.
- Refrain from unauthorized attempts to circumvent the security controls of any computational resource.
- Refrain from attempts to degrade system performance or capability, or attempts to damage systems, software, or intellectual property of others.
- Refrain from using computational resources for commercial purposes unrelated to the university, except as specifically authorized.
- Comply with all federal, state and other applicable laws, all applicable university rules and policies, and all applicable contracts and licenses. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
- Request supervisory direction regarding permitted personal use of computational resources.

Proper and Authorized Use of the UIC Network

Members may not extend or share the UIC network with the public or others beyond what has been configured by the Technology Solutions Network Infrastructure Team. Members are not permitted to connect any network devices or systems (e.g., switches, routers, wireless access points, VPNs, and firewalls) to the UIC Network without advance consultation and written permission from the Technology Solutions Network Infrastructure Team.

Devices connected to the UIC network may not route network traffic between a UIC network and an external network without written approval from the Technology Solutions Network Infrastructure group.

Only Technology Solutions-approved domains may be operated within UIC Network address space. Publicly accessible Domain Name Servers must be approved by Technology Solutions before they are placed in service.

If Technology Solutions determines that a LAN, or any portion thereof, presents an immediate security risk to other UIC computational resources, Technology Solutions may terminate or restrict the LAN's network connection without notice until the issue has been remediated. If there is no immediate risk, Technology Solutions will bring the matter to the attention of the LAN's network administrator and/or network security liaison.

Technology Solutions will occasionally perform network scans of computational resources connected to the UIC network for security vulnerabilities. If the Technology Solutions Information Security and Privacy Office becomes aware of high-severity security vulnerabilities either through the results of these scans or other means, the administrator is responsible for securing the system to the satisfaction of the Technology Solutions Information Security and Privacy Office in a timely manner. Failure to do so will result in the restriction of network access for the affected resource.

The system administrator of a computational resource is responsible for the security of that resource. UIC Network connected servers must require user authentication over an encrypted session before allowing access to non-public information. At minimum, this will require the connecting user to supply a NetID and associated password. The administrator must monitor and log access and keep other system logs useful for establishing the identities of individuals used in the event of a breach of security.

All devices connected to the UIC network must be registered with a Technology Solutions operated or approved domain name server. Devices found connected that are not properly registered will be considered security threats and will have their network access blocked.

Network vulnerability scanning of computational resources is restricted to authorized personnel using the university provided solution.

Software and hardware which permit the capture and examination of network packets (commonly known as sniffing), may only be used on the UIC network by authorized personnel.

1. These tools may only be used after consultation with and receiving written permission from the Technology Solutions Information Security and Privacy Office.

2. When using these tools, they must be configured to capture the minimum information needed to diagnose the problem (i.e. member data should not be captured unless needed to solve a problem).

3. All data collected must be securely deleted as soon as it has served its purpose.

4. All information collected by these tools must be considered high-risk as defined by the UIC IT Security Program.

Administrators of computational resources are required to log access to their devices. The log information may include the source and destination addresses, session start and end times as well as the NetID used to establish the session.

Computational resources on the UIC Network must not be used to provide email or email routing services for persons or organizations that are not UIC community members.

The following devices may not be installed on the UIC network unless written consent has been given by the Technology Solutions Network Infrastructure group. Unapproved devices are subject to network filtering and/or physical disconnection.

1. Hardware firewalls and/or NAT devices
2. Wireless access points
3. DHCP servers

Security and Monitoring

The university regularly monitors and records the activity on computational resources to evaluate system efficiency and to detect signs of intrusion and/or abuse. It is the practice of the university not to selectively monitor the usage of computational resources by individuals unless there is a legitimate business or security reason to do so. The university may further monitor and record the usage of individuals, including the disclosure of individual files when:

1. in accordance with generally accepted security, network, and system administration practices;
2. to prevent or investigate any actual or potential information security incident and/or misuse of computational resources;
3. it has reason to believe that activities are taking place contrary to this policy, or state or federal law;
4. necessary to respond to a court order, subpoena, to assist law enforcement, or in response to a request from a federal or state oversight agency;
5. necessary to respond to a request for discovery in the course of litigation;
6. necessary to retrieve information in emergency circumstances where there is a threat to health, safety, or university property involved.

The university, in consultation with its legal counsel, may contact local or federal law enforcement authorities to investigate any matter in its sole discretion.

Employees do not have an expectation of privacy in their use of university computational resources and should limit personal use of these resources to minimize any potential exposure of personal data.

To ensure business continuity units may, with proper authorization, request access to employee email and files upon termination of employment or an unanticipated leave of absence

Discipline

Failure to comply with this policy may put university information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Students who violate this policy may be referred to the Office of the Dean of Students. Contractors, vendors, and others who fail to adhere to this policy may face termination of their business relationships with the university.

Violation of this policy may also carry the risk of civil or criminal penalties.

Reason for Policy: Failure to comply with this policy may put university information assets at risk.

Minority Impact Statement: The policy does not have any disproportionate or unique impact on UIC's minority students, staff, or faculty.

Who Should Read the Policy: All students, faculty, staff, and administrators at UIC.

Definitions:

- ***Covered Individuals:*** The policy applies to all members of the university community, our partners and guests, which includes any entity using university computing devices or the university data network, including the UIC-Guest network and eduroam.
- ***Ownership of Resources:*** All technology resources owned by the university may be accessed only by authorized personnel. Digital identifiers assigned by the university (e.g. Netid) are the property of the university.
- ***Identity:*** Members of the university community must use their assigned identifiers and may not share credentials. Individuals may not disguise their identity or that of any technology equipment.
- ***Acceptable Use:*** Personal use of resources should be limited but may be permitted when it does not violate other policy or ethics guidelines. Resources may not be used for prohibited political activity or commercial activity unrelated to the business of the university. Individuals may not use resources to violate any applicable law or to transmit harassing or malicious content.
- ***Data Network:*** The campus data network is run solely by Technology Solutions in support of university functions. No individual may connect network devices or systems to the network, including wireless access points, firewalls, and routers, without the consent of Technology Solutions. Technology Solutions monitors network traffic and may shut down network access to investigate issues or mitigate threats.
- ***Discipline:*** Failure to comply with this policy may put university information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Students who fail to adhere to this policy may be referred to the Office of the Dean of Students. Contractors, vendors, and others who fail to adhere to this policy may face termination of their business relationships with the university. Violation of this policy may also carry the risk of civil or criminal penalties.

Procedures: None

Forms: None

Related Laws, Regulations, Statutes, and Policies:

- IT Security Program [http://policies.uic.edu/uic-policy-library/information-technology/uic-information-techology-security-program/]

Document History:

Approval date: February 17, 2022
Approved as: New policy