

SYRACUSE UNIVERSITY POLICIES

Keyword Search Policy Home

Policy Categories

University Governance Ethics, Integrity, and Legal Compliance

Faculty, Teaching, and Research

Academic Rules, Student Responsibilities & Services

Employment, Workplace Rules, Benefits and Governmental Notices

Free Speech

Administrative and Financial

Information Technology

University Facilities, Equipment, and Property

Campus Safety and Emergency Services

Policy Process

Submitting a Proposed New or Revised Policy

Reporting Policy Violations

2015 Approved Policies

Mobile Device Acceptable Use Policy

Purchasing Policy - Printers, Copiers, Multifunction Devices

Office Supply Purchasing Policy

Travel Policy

GIFT POLICY

Other Authoritative Documents

Syracuse University Compact

Faculty Manual

Staff Employee Handbook

Student Handbook

Academic Rules

University Senate Bylaws

Free Speech

Information Technology Resources Acceptable Use Policy

I. General Policy Statement

This policy governs the ways in which all users of IT Resources, including but not limited to Syracuse University students, faculty, staff, trustees, agents, visitors, and guests may use the University's Information Technology (IT) Resources. This policy also sets forth the University's rights with respect to accessing data and other records contained in or on the University's IT Resources.

II. Reason for Policy/Purpose

This policy is established to ensure University IT Resources are used for their intended purpose and in compliance with law, regulations, University policies, and contractual obligations. This policy also aims to protect the confidentiality, integrity, security, availability and performance of University IT Resources.

III. Policy

A. Acceptable Use of IT Resources

IT Resources may be used to further the educational, research, scholarly, creative, and service mission of the University, within the bounds of applicable law and regulations, University policies, and contractual obligations. By extension, IT Resources may be used for the free exchange and expression of ideas within the limits of the law, including acquiring or sharing of copyrighted information in compliance with applicable copyright and other law.

B. Unacceptable Use of IT Resources

IT Resources are not to be used in a way that is unlawful, or inconsistent with the University's mission or policies, including:

1. Use that violates laws, regulations, any University policy or policy of external networks and resources, or contractual obligations;
2. Use that is contrary to the University's non-profit status (e.g., commercial use unrelated to the University and the University's mission; partisan political activities or lobbying that suggests University endorsement of political candidates, platforms, or positions);
3. Use that violates copyright, trademark, trade secret, patent or other intellectual property rights of others;
4. Use that obstructs University operations by consuming excessive amounts of network bandwidth or other IT Resources, or deliberately degrading performance of IT Resources;
5. Use for any type of commonly defined malicious Hacking activity which includes attempts to deny service to, gain information about, access to, control or use of any University or personally owned computing device or data without the owner's explicit permission;
6. Use to intimidate, harass, incite, threaten or otherwise do harm to others, beyond the bounds of protected free speech;
7. Use for the purpose of intercepting or monitoring data on IT Resources not intended for the user;
8. Allowing or enabling use by any unauthorized person;
9. Sharing University passwords and credentials with unauthorized persons;

Emergency Procedures Reference Guide

Campus and Governmental Notices

Policy Submission Flowchart

10. Impersonating others or committing fraudulent acts.

C. Violations of Policy

Violations of the policy may result in disciplinary action, including dismissal from employment, suspension or expulsion from further study, and termination or suspension of IT Resources privileges.

D. Privacy and Access

Syracuse University values the privacy of its students, faculty, and staff, especially with respect to scholarly, creative, and personal information. However, in limited circumstances, the University may need to access, copy or view data stored or transmitted on IT Resources. The limited circumstances include:

- When required by law, regulations, University policy, or contractual obligations, including but not limited to in order to comply with a validly issued subpoena;
- When required to protect the health or safety of individuals, the community, or the general public;
- When required to perform essential functions in furtherance of the University's mission and operations;
- When required to diagnose or fix problems with IT Resources, or to otherwise preserve the availability, integrity and confidentiality of IT Resources;
- When required to investigate suspected violations of law, University policy, or other misconduct; or
- When required in connection with the University's representation, claims or defenses in a lawsuit or regarding a legal claim.

In the event data must be accessed, the appropriate University Officer as defined in Section V, Appendix A *("Procedures")* must approve and make the request to the Office of the Chief Information Officer (CIO).

If a user suspects or knows that privacy laws, rules or regulations have been violated, including that Confidential Data has been lost or stolen from IT Resources, it is the user's responsibility to immediately notify the Information Security Officer.

IV. To Whom Does This Policy Apply

Students, Faculty, Staff, Visitors/General Public, Other: Third-Party Contractors

V. Appendices (as applicable)

A. Procedures

Data may be accessed in the limited circumstances set forth at Section III.D of this policy *("Privacy and Access")* only with the appropriate request and approval from the relevant University Officer to the Office of the CIO. The role of the requester is based on the need for the data and/or the role of individuals whose information may be accessed or provided.

Requirement	Request and approval must come from one of the following University Officer(s)
Subpoena or other legal need, including investigations or defense of a legal claim	President and Chancellor, or Senior Vice President and General Counsel
Health or safety need	President and Chancellor, Senior Vice President of Safety and Chief Law Enforcement Officer, Chief of the Department of Public Safety, or Senior Vice President and General Counsel
Essential functions need	President and Chancellor, Vice Chancellor for Academic Affairs and Provost, Vice President and Chief Financial Officer, Senior Vice President and Chief Human Resources

	Officer, or Senior Vice President and General Counsel
Fix or Maintain IT Resources	President and Chancellor, Vice President and Chief Information Officer, Information Security Officer, or Senior Vice President and General Counsel
Requests that involve University Officer(s) data	President and Chancellor, Vice Chancellor for Academic Affairs and Provost, or Senior Vice President and General Counsel

B. Definitions

"Confidential Data": See definition at ITS Information Security Standards page.

"Information Technology (IT) Resources": University owned, leased, operated or contracted technology systems, networks, equipment and facilities.

"Hacking": Includes but is not limited to activity that maliciously or without permission circumvents IT Resource security configurations, exploits system or software vulnerabilities, installs or deploys malware, generates excessive network traffic, performs social engineering, or attempts to access systems or data in an unauthorized manner.

C. Forms

none

D. Other Related Policies and Documents

- University Information Technology Policies
  - Email Policy
  - Security of and Secure Remote Access to Information Technology Systems and Resources
- Additional information
  - ITS Information Security Standards Page

E. Frequently Asked Questions

Q: What are some common examples of policy violations in addition to those listed in Section III(B) above?

A: Gaining access to a computer or other IT Resource without the proper permissions, e.g. trying to "hack" into a computer or an account, or using someone else's logon credentials to access information.

Using the University network or systems to attack any system on the Internet, not limited to only University owned and managed systems.

Illegally downloading and/or sharing copyrighted digital information such as music, movies, software, or digital books.

Intentionally and maliciously using any software tool or package with the intent of denying access to IT resources, commonly known as a Denial of Service (DoS) attack.

Maliciously "phishing" other users both on and off campus from an IT resource by trying to trick them into providing credentials, clicking on a link, or installing malware.

Attempting to intercept traffic on the University network without specific permission with the intent to gain access to information that you could not normally access.

Q: In Section III.D. of the policy on access, what does "When required to perform essential functions in furtherance of the University's mission and operations" mean?

A: The "essential functions" standard is meant to be used as a last resort in unusual circumstances where access to user data is necessary to effective operation of the University or University program(s).

F. Policy Administration

Information Technology Services/CIO

Date: Created: 10/21/16
Updated: 12/13/16

© 1995 - 2008 Syracuse University, Syracuse, NY 13244 (315) 443-1870

For technical assistance contact supolicy@syr.edu