Responsible Use of Information Technology Policy

Background

Access to IT resources is essential to the University at Albany's mission of teaching, learning and research and is integral in promoting the success of all students, faculty and staff. This responsible use policy was developed to provide the campus with a secure, reliable IT environment in support of the University's mission. Such an environment facilitates and encourages the exchange of ideas and information while protecting the freedom of expression of the campus community. This policy establishes basic rights for all users and defines expectations and behaviors to ensure appropriate use and protection of these resources.

General Principles

Access

Access to information technology is essential to the University's mission of providing students, faculty and staff with educational services of the highest quality. The pursuit and achievement of this mission requires access to campus IT resources and the Internet for all members of the University community.

Freedom of Expression and Academic Freedom

The University respects freedom of expression in all electronic forms on its computing and networking systems. While electronic speech has broad protections, the University community is expected to recognize that disseminating information electronically makes it accessible to a broad and diverse audience. All users are expected to respect the University's Community Rights and Responsibilities when sharing information using campus IT resources.

This policy supports the principle of academic freedom as outlined in the SUNY Policies of the Board of Trustees (Article XI, Title I).

Privacy

All members of the campus community will respect the privacy of individual users with regard to content in all electronic forms to the fullest extent possible under applicable policy and law. The University does not monitor content except under the limited circumstances outlined in this policy. Members of the campus community are expected to use only those resources they have access to, and to use them in the manner and to the extent they are authorized.

Aggregate traffic, not individual content, is monitored on the University network to measure and assure reliable performance. The University employs tools to identify and mitigate malicious traffic and reserves the right to take immediate action to protect and secure the IT environment and electronic assets in the event a threat is detected. This may include removal of devices from the University network and/or suspension of individual access. The protection of campus IT resources takes precedence over the rights of the individual to access them. See the section on Protecting the University Network and Technology Infrastructure in this policy and Connecting Devices to the University Network for more information.

All users are advised that computer networks are inherently insecure. While the University takes precautions to protect its IT environment, absolute privacy and security cannot be guaranteed.

Compliance

Use of University computing and network resources must comply with all applicable federal, state and other applicable laws and regulations; SUNY policies; this document and all other applicable University policies, protocols, standards, procedures and guidelines; and all applicable contracts and licenses, which includes the laws of copyright, libel, trademark and privacy.

All devices on campus networks, both University and personally owned, must comply with the University at Albany's Connecting Devices to the University Network policy and standards documents. The use of

any equipment or services that may limit access or performance for others may be restricted or prohibited. Any servers residing on the campus network must comply with Standards for Connecting Servers to the University Network.

Scope

This policy applies to all users of campus computing and network resources, including but not limited to, all students, faculty and staff, campus affiliates and University guests.

User Access and Responsibilities

As members of the University community, all students, faculty and staff are afforded the privilege of access to a variety of campus resources. The University's IT environment is one such resource.

Computing Accounts and Access

All members of the University receive an individual account providing access to IT resources for the duration of their association with the institution. Passwords for individual accounts must never be shared.

Access to campus IT resources is based on the principle of least privilege; people are granted access to electronic assets based on their current role at the University. Any time an individual's role changes, their access to campus IT resources must be reviewed and updated accordingly. See the University's Identity Management Policy (in draft) for more information about computing accounts and access.

Misuse of IT Resources

All members of the University are responsible for preserving the integrity of campus IT resources and using them in a manner consistent with this policy.

Improper use includes, but is not limited to: unauthorized access to or misuse of network or electronic data in any form; the use of another's computing account, circumventing network security measures; the use of University networks, computer resources or data for private, commercial or political purposes; harassment or defamation; the unauthorized alteration of electronic files; disruption or interference (hacking/spam/viral programs); software license or copyright violations; violations of federal or state law, or applicable SUNY or University at Albany policies.

Responsibility for the Protection of University Data

The University makes every effort to respect the privacy of an individual's electronic assets. All members of the campus community and users of its IT resources are expected to observe the privacy and integrity of others' files. No user should view, copy, alter or destroy another's electronic files without permission unless required to do so by law, policy or procedure.

University employees with network access to institutional data have responsibilities to safeguard and protect such data, particularly that information which is governed by law, policy or regulation. This includes, but is not limited to, personally identifiable information and educational, personnel, health and financial records. All employees with access to institutional data are expected to read, sign and act in accordance with the University's Employee Access Compliance Agreement. Employees may be subject to additional job-specific requirements to protect institutional data as part of their routine responsibilities.

Requests for access to protected information are reviewed by the Office of the CIO (OCIO) in consultation with the Office of General Counsel, Information Security Officer, University Controller and all other relevant parties to ensure that appropriate measures are taken to protect University data and carried out in compliance with all applicable laws, regulations and policies.

In the normal course of system maintenance, campus IT staff may have access to others' electronic files. Staff are required to maintain the confidentiality and privacy of information in such files unless required by law or University policy to disclose it. See specifically the section on the Employee Access Compliance Agreement for more information (note the "Sys Admin" section is in draft).

Security
All members of University community assume responsibility for ensuring that campus IT resources and information assets are handled in a manner consistent with the University's Information Security Policy and Information Security Domains, Supporting Protocols and Procedures.

Incidental Use of Information Technology
Campus IT resources are intended for academic and business purposes consistent with the University's mission. However, the University recognizes and acknowledges that incidental use of such resources may occur. Occasional, incidental use unrelated to the University's mission, such as personal email or document storage, is acceptable provided that:

- the University doesn't incur more than minimal costs
- the use does not interfere with official business
- it does not result in personal financial gain
- it is not in violation of any security/access rules

Protecting the University Network and Technology Infrastructure
The University takes reasonable and appropriate precautions to protect the integrity of its networks, equipment and all electronic assets. This includes measures to minimize and/or prevent hackers and other malicious attacks from harming campus IT resources in accordance with the University's Information Security Incident Response Protocol. The University does not guarantee against threat, loss, or damage. Users should be aware that campus computer systems and networks may be subject to unauthorized access, tampering or generation of fraudulent email messages. The University reserves the right to limit the use of campus IT resources based on institutional priorities, technical capacity and security and fiscal considerations.

While the University does not monitor the content of individual usage except under the limited circumstances outlined below, the normal operation and maintenance of computing resources require the backup and caching of data and communications, the logging of system activity, the scanning of systems and network ports for anomalies and vulnerabilities, and other such activities for the provision of service. If anomalies or unusual activity are identified in the course of monitoring aggregate network traffic, measures will be taken to protect the confidentiality, integrity and availability of IT resources. The University reserves the right to take any of the following actions if such anomalies or unusual activity is identified:

- Access computer systems and networks, including individual login sessions
- Limit or remove an individual's access to campus IT resources
- Limit or remove devices from the University network

In the event that the content of individual usage is in need of review, the OCIO shall consult with the Office of General Counsel and appropriate campus authorities to ascertain whether such monitoring is necessary and, if so, determine the scope of content which may be viewed. Such examinations are conducted by technical staff in the presence of the vice president or designee(s) of the division requesting access and are limited to those items specified by the scope of review. When possible, efforts will be made to notify individuals prior to reviewing the content of electronic files. However, the University may also monitor individual usage without prior notice under the following limited circumstances:

a. The user has given permission to do so;
b. It reasonably appears necessary to do so to protect the integrity, security or functionality of computing resources or protect the University from liability;
c. There is reason to believe the user has violated, or is violating, applicable law or policy;
d. The account appears to be engaged in unusual or excessive activity, as indicated by the monitoring of general activity and usage patterns; or

e. Is otherwise required or permitted by law

Any individual monitoring, other than that specified in (a), required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the OCIO in consultation with the Office of General Counsel and other appropriate campus authorities.

Responsibility and Authority

This policy may be supplemented with additional policies and related documents as deemed necessary by the OCIO. Additional requirements may be established by individual departments/units provided they are consistent with this policy. Responsibility and authority for this policy resides with the OCIO and its designees. Violations of this policy should be reported to the OCIO and may be subject to disciplinary and/or legal action. Enforcement resides with the OCIO.

Related Documents

- SUNY Policies of the Board of Trustees
- Community Rights and Responsibilities
- Identity Management Policy (in draft)
- Information Security Policy
- Information Security Domains, Supporting Protocols and Procedures
    - Access to Electronic Records Held in Accounts Subsequent to Termination, Departure or Death
- Employee Access and Compliance Agreement
- Internet Privacy Policy
- Connecting devices to the University Network
    - Standards for Connecting Devices to the University Network
    - Standards for Connecting Servers to the University Network
    - Network Equipment Standards
    - Class B Domain Space Standards
    - Wireless Standards
- Email as an Official Means of Communication with Students
- University Web Policy (in draft)