TECHNOLOGY ACCEPTABLE USE - STUDENTS

Sponsor: Chief Information Officer
Contact: Information Technology Security Analyst
Category: Information Security and Technology
Number: 1000.003
Effective Date: 07/09/2003
Implementation History: Approved: April 14, 2002, Revised: July 9, 2003, February 2023
Keywords: Students, Computers, Computer lab, Account Access, Technology Access
Background Information: This policy replaces the “Computer Use Statement Policy-Students”. This policy amends and incorporates all policy statements from the preceding policy. This policy was drafted with the assistance of a third-party cyber security firm. The SUNY Empire “laptop loaner program” is acknowledged in this policy.

Purpose

SUNY Empire promotes student use of its online academic resources, online student support services and computing facilities located at centers and units, and seeks to improve the computer literacy of its students, faculty and staff. Every user is expected to adhere to the statements#that follow to further these goals.

The purpose of this Acceptable Use Policy is to clearly establish each member of the institution’s role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives will enable SUNY Empire to implement a comprehensive system-wide Information Security Program.

DEFINITIONS

None specific to this policy

STATEMENTS

SCOPE

This policy applies to all students with access to computing resources owned, managed or otherwise provided by SUNY Empire State (Empire). Individuals covered by this policy include, but are not limited to all students, matriculated or non-matriculated, with access to the institution’s computing resources and/or facilities. Computing resources include all SUNY Empire owned, licensed or managed hardware and software, email domains, and related services and any use of the institution’s network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

PRIVACY

SUNY Empire will make every reasonable effort to respect a user’s privacy. However, students do not acquire a right of privacy for communications transmitted or stored on the institution’s resources, including laptops loaned to students. In response to a judicial order or any other action required by law or permitted by official SUNY Empire policy, or if the institution has otherwise determined reasonable necessity to protect or promote the legitimate interests of the institution, the President or Chief Information Officer (CIO), may authorize a SUNY Empire official or other authorized agent, to access, review, monitor and/or disclose computer files associated with an individual’s account. Additionally, in response to a suspected violation of the Student Conduct Policy and/or violation of New York State Acceptable Use of Technology Information Technology Resources Policy, the Vice Provost for Student Success or the Executive Director for Student Success may require a student return a loaned laptop to SUNY Empire before the term has ended and may authorize an agent of the university to review the data and information on the laptop. Students are encouraged to review the Adherence to Family Education Rights and Privacy Act of 1974 Policy (https://www.sunyempire.edu/policies/?search=cid%3D37340) as well as the Student Conduct Policy (https://www.sunyempire.edu/policies/?search=cid%3D37969).

POLICY

Any use that disrupts the institution’s mission is prohibited. Using any Empire computer, account, computer resources or online resources for personal profit, or other purposes other than academic or university purposes is prohibited.

Following the same university policies on Affirmative Action, Non-Discrimination-Anti-Harassment, Sexual Harassment and Bias Related Crime, that protect the rights of individuals that study and interact with SUNY Empire, acceptable use of information technology resources generally respects all individuals’ privacy, but subject to the right of individuals to be free from intimidation, harassment, and unwarranted annoyance. All users of SUNY Empire’s computing resources must adhere to the requirements enumerated below.

The university reserves the right to monitor or restrict computing activity on SUNY Empire owned and operated systems, with the exception of laptops loaned to students from the official laptop loan program. The university is not responsible for loss of data or service interference resulting from efforts to maintain the university’s computing facilities.

Students creating personal webpages on the university’s servers must abide by the university’s Web Presence and Publishing Policy. (https://www.sunyempire.edu/policies/?search=cid%3D35655)

4.1 FRAUDULENT AND ILLEGAL USE

SUNY Empire explicitly prohibits the use of any information system for fraudulent and/or illegal purposes. While using any of the institution’s information systems or hardware, a user must not engage in any activity that is illegal under local, state, federal, and/or international law. As a part of this policy, users must not:

Violate the rights of any individual or company involving information protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by SUNY Empire.

Use in any way copyrighted material including, but not limited to, photographs, books, or other copyrighted sources, copyrighted music, and any copyrighted software for which the institution does not have a legal license or an appropriate license has been purchased by the user of a loaned device.

Export software, technical information, encryption software, or technology in violation of international or regional export control laws.

Issue statements about warranty, expressed or implied, unless it is a part of normal job duties, or make fraudulent offers of products, items, and/or services.

Any user that suspects or is aware of the occurrence of any activity described in this section, or any other activity they believe may be fraudulent or illegal, must notify the IT Service Desk (https://www.sunyempire.edu/service-desk/).

4.2 CONFIDENTIAL INFORMATION

SUNY Empire has both an ethical and legal responsibility for protecting confidential information in accordance with its Enterprise Data Classification Policy (https://www.sunyempire.edu/policies/?search=cid%3D104470).

4.3 HARASSMENT

SUNY Empire is committed to providing a safe and productive environment, free from harassment, for all employees and students. Harassment is defined and prohibited by the Student Conduct Policy (https://www.sunyempire.edu/policies/?search=cid%3D37969). For this reason, users may not:

Use institution information systems to harass any other person via e-mail, telephone, or any other means, or

Actively procure or transmit material that is in violation of sexual harassment or hostile workplace laws.

If a user feels he/she/they is being harassed through the use of the institution's information systems, the user shall reference the university's Discrimination Compliant Procedures (https://www.sunyempire.edu/policies/?search=cid%3D146277).

4.4 INCIDENT REPORTING

SUNY Empire is committed to responding to security incidents involving personnel, institution-owned information, or institution-owned information assets. As part of this policy:

The loss, theft or inappropriate use of information access credentials (e.g., passwords, or security tokens), assets (e.g., key cards, laptop, cell phones, tablets), or other information will be reported to the SUNY Empire IT Service Desk.

All incidents regarding SUNY Empire owned physical assets shall be reported to the IT Service Desk (https://www.sunyempire.edu/service-desk/).

Any device loaned through the Laptop Loan program should be reported to the program administrator, including damage, loss, and/or theft.

4.5 MALICIOUS ACTIVITY

SUNY Empire strictly prohibits the use of information systems for malicious activity against other users, the organization's information systems themselves, or the information assets of other parties.

4.5.1 DENIAL OF SERVICE

Users must not:

Perpetrate, cause, or in any way enable disruption of SUNY Empire's information systems or network communications by denial-of-service methods;

Knowingly introduce malicious programs, such as viruses, worms, and Trojan horses, to any information system; or

Intentionally develop or use programs to infiltrate a computer, computing system, or network, and/or damage or alter the software components of a computer, computing system, or network.

4.5.2 CONFIDENTIALITY

All encryption keys employed by users must be provided to Information Technology if requested, in order to perform functions required by this policy.

Users must not:

Perpetrate, cause, or in any way enable security breaches, including, but not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access;

Base passwords on something that can be easily guessed or obtained using personal information (e.g., names, favorite sports teams, etc.);

Facilitate use or access by non-authorized users, including sharing their password or other login credentials with anyone, including other users, family members, or friends;

Use the same password for SUNY Empire accounts as for other non-SUNY Empire access (for example, personal ISP account, social media, benefits, email, etc.);

Attempt to gain access to files and resources to which they have not been granted permission, whether or not such access is technically possible, including attempting to obtain, obtaining, and/or using another user's password;

Make copies of another user's files without that user's knowledge and consent.

4.5.3 IMPERSONATION

Users must not:

Circumvent the user authentication or security of any information system;

Add, remove, or modify any identifying network header information ("spoofing") or attempt to impersonate any person by using forged headers or other identifying information;

Create and/or use a proxy server of any kind, other than those provided by SUNY Empire, or otherwise redirect network traffic outside of normal routing with authorization; or

Use any type of technology designed to mask, hide, or modify their identity or activities electronically.

4.5.4 NETWORK DISCOVERY

Users must not:

Use a port scanning tool targeting either SUNY Empire's network or any other external network, unless this activity is a part of the user's normal job functions, such as a member of the Information Technology Services (ITS), conducting a vulnerability scan, and faculty utilizing tools in a controlled environment;

Use a network monitoring tool or perform any kind of network monitoring that will intercept data not intended for the users, unless this activity is a part of the user's normal job functions.

4.6 OBJECTIONABLE CONTENT

SUNY Empire strictly prohibits the use of organizational information systems for accessing or distributing content that other users may find objectionable. Users must not post, upload, download, or display messages, photos, images, sound files, text files, video files, newsletters, or related materials considered to be in violation of the Student Code of Conduct (https://www.sunyempire.edu/policies/?search=cid%3D37969), unless explicitly assigned by an instructor or mentor to do so as part of an academic exercise.

4.7 HARDWARE AND SOFTWARE

Specific university owned equipment managed by the Health and Wellness Program's Laptop Loan program may be used outside the university's network and have a less restrictive device and security settings. Users of the laptops are expected to adhere to all the above sections with acceptable use.

The laptops loaned are not restricted by the SUNY Empire State University's Information Technology Services, and users may install software they have legally purchased licenses or have access through the university (Office 365, etc.). However, a user should always protect their security and use sound judgment when using unsecured networks or trusted plug & play devices outside of the university or the student's residence.

The university is not responsible for loss of data or service interference resulting from individual use of devices loaned through the laptop loan program.

When using university owned equipment not governed by the Laptop Loan program, such as computer labs or other local devices, SUNY Empire strictly prohibits the use of any hardware or software that is not purchased, installed, configured, tracked, and managed by the institution. Users must not:

attach, connect or remove or disconnect, hardware of any kind, including wireless access points, storage devices, and peripherals, to any institutional information system without the knowledge and permission of ITS;

Download, install, disable, remove or uninstall software of any kind, including patches of existing software, to any institutional information system without the knowledge and permission of ITS;

Use personal flash drives, or other USB-based storage media, or

Take SUNY Empire equipment off-site without prior authorization from ITS.

4.8 MESSAGING

The organization provides a robust communication platform for users to fulfill its mission. Users must not:

Send unsolicited electronic messages, including "junk mail" or other advertising material to individuals who did not specifically request such material (spam);

Solicit electronic messages for any other digital identifier (e.g. e-mail address, social handle, etc.), other than that of the poster's account, with the intent to harass or to collect replies; or

Create or forward chain letters or messages, including those that promote "pyramid" schemes of any type.

4.9 OTHER

In addition to the other parts of this policy, users must not:

Use the institution's information systems for commercial use or personal gain.

ROLES AND RESPONSIBILITIES

SUNY Empire reserves the right to protect, repair, and maintain the institution's computing equipment and network integrity. In accomplishing this goal, SUNY Empire ITS personnel or their agents must do their utmost to maintain user privacy, including the content of personal files and Internet activities. Any information obtained by ITS personnel about a user through routine maintenance of the organization's computing equipment or network should remain confidential, unless the information pertains to activities that are not compliant with acceptable use of SUNY Empire's computing resources including the Student Conduct Policy (https://www.sunyempire.edu/policies/?search=cid%3D37969)

ENFORCEMENT

Enforcement is the responsibility of the institution's *President or Chief Information Officer (CIO).* The President or CIO may authorize a SUNY Empire official or an authorized agent. Users who violate this policy may be subject to the termination of their account. The institution may temporarily suspend or block access to an account when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the institution or other computing resources or to protect SUNY Empire from liability.#If a laptop that has been loaned to a student is requested to be returned to SUNY Empire due to a suspected violation and it is not returned, a hold will be placed on the student's record which will prevent registration for future courses.

EXCEPTIONS

Exceptions to the policy may be granted by the Chief Information Officer (CIO), or by his or her designee.#All exceptions must be reviewed annually.

APPLICABLE LEGISLATION AND REGULATIONS

The Gramm - Leach Bliley Act (GLBA)

Family Educational Rights and Privacy Act (FERPA)

General Data Protection Regulation (GDPR)

New York State Information Security Breach and Notification Act

New York State Acceptable Use of Information Technology Resources NYS-P14-001

NIST 800-171

FIPS-199

New York Civil Practice Law and Rules § 4509

Code of Ethics of the American Library Association

RELATED REFERENCES, POLICIES, PROCEDURES, FORMS AND APPENDICES

Student Conduct Policy (https://www.sunyempire.edu/policies/?search=cid%3D37969)

Adherence to the Family Educational Rights and Privacy Act of 1974 Policy (https://www.sunyempire.edu/policies/?search=cid%3D37340)

Enterprise Data Classification Policy (https://www.sunyempire.edu/policies/?search=cid%3D104470)

Student Email Communication Policy (https://www.sunyempire.edu/policies/?search=cid%3D147367)

Use of University Hosted Individual Web Spaces Policy (https://www.sunyempire.edu/policies/?search=cid%3D35762)