LONG ISLAND UNIVERSITY

COMPUTER SYSTEM ACCESS AND USAGE POLICY

PURPOSE

The purpose of this policy is to set guidelines for using and monitoring network or resource usage at the University.

STATEMENT OF POLICY

Employees and students should be aware that any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system may be subject to monitoring at any and all times by any lawful means.

To ensure the continued integrity of its information technology resources, facilities and controls, the University may audit, inspect and/or monitor network or resource usage, at any time, without notice. The University may limit or terminate the network access of any user who is in violation of any University or Information Technology (IT) policies.

Examples of improper use include, but are not limited to the following:

- Unauthorized access to network or electronic data in any form;
- The use of another's password or account;
- The use of University data, networks or IT resources for commercial or political purposes;
- The unauthorized alteration of electronic files, including any disruption or interference (hacking / spam / viral programs);
- Software license or intellectual property violations;
- The violation of any University policy, local, state or federal law; harassment or defamation.

Users with access to confidential, privileged or financial data protected by law or University policy must adhere to the following security requirements:

Desktop security: All computers must be secured and non-approved software removed. Only approved software may be installed. Individual users on administrative systems may not add or remove software without Information Technology involvement. USB ports will be disabled to prevent the transportation or misuse of confidential information.

Internet: Internet browsing will be limited to approved, business websites by unit Directors. Personal webmail such as Yahoo, Google, etc., is not allowed.

Passwords: Frequent password changes will be required using unique combinations of alphanumeric and character sets such as "#, !" and so forth. Staff must not share passwords.

Remote Access: Remote access will be limited to LIU-owned computers utilizing virtual Citrix software that prevents the accidental transfer of information. All remote access must be authorized for business operation continuity purposes and approved by a University Officer.

Laptop security: Laptop use is not authorized for persons with access to extremely privileged information due to the risk of loss and associated threat of security breach. When laptop usage cannot be avoided, strong data encryption must be applied.

The University may also restrict unlimited electronic access. If an imposed limitation interferes with a user's bona fide educational or research activities, the user may direct a written request for a waiver to his or her Department Chair, who, on approval, shall forward the request to the appropriate Dean for review. The University reserves the right to limit the use of information technology resources based on institutional priorities, technical capacity and fiscal considerations.

Article 156 of the New York State Penal Code and federal law (18 USC §§ 1030, 1302, 2252, 2501) impose criminal sanctions for certain offenses involving computers, software and computer data, including unauthorized use, fraud, computer trespass, computer tampering and unauthorized access to student records. Misuse of the University's information technology resources is subject to disciplinary and/or legal action.

These policies apply to all users of any University information technology resource, including students, staff, faculty and other authorized users, whether operating on campus or from a remote location. The University's information technology resources include, but are not limited to:

- Any network, communication system, computer equipment or media service provided by the University for educational, research, administrative, communication or related purposes;
- Information technology or data communications equipment owned, leased, or operated by the University;
- Any equipment connected to the University's data network, regardless of ownership;
- All messages, data files and programs stored in or transmitted by any University information technology resource;
- All data and information assets created with or stored on systems operated by or for the University.

Information technology resources are provided by the University to support its educational and research mission. Use of University information technology resources is a privilege. Accordingly, all users of the University's networks, systems and equipment are responsible for the proper use and protection of these resources, consistent with University policies and applicable law.

The Information Technology department supports the University's educational mission by providing access to the following systems and services:

- Systems using the University network for communication;
- University networks, computer systems, equipment, storage and supporting resources;
- Electronic mail accounts, point-to-point messaging, list server postings;
- The World Wide Web;
- Special-purpose software on University network computers;
- Administrative information Systems;

- Learning Management Systems;
- Library Management Systems;
- The My LIU Student Portal.

Terms of Use: Usage of the University's information technology systems and resources is a privilege granted to University students, faculty and staff, to support its educational mission. Passwords and account access may not be shared. Passwords are the frontline of protection for all user accounts. Persons using University information technology resources must safeguard their passwords. Select 'secure' passwords using letter, number and symbol combinations that cannot easily be 'cracked' by automated tools.

All users of the University's computer network must maintain the integrity of the information technology systems. Any user who detects a possible security concern on any University system or network must report it immediately to the IT system administrators. The University reserves the right to audit, inspect, limit, revoke or refuse to extend IT privileges or access to its computer systems and electronic resources, at any time, in its sole discretion.

Internet Content: The University does not control information available over the Internet and is not responsible for Internet content. Internet users should be aware that even sites accessed for legitimate educational or research purposes may contain offensive material. Workstations in open-access facilities, such as the University Computer Labs, shall be used in a fashion that is not offensive to the University community or violative of local, state or federal law.

Personal Use: The University is a non-profit, tax-exempt organization. As such, it is subject to federal and state laws that restrict the use of University property for matters unrelated to its Charter mission. As a recipient of state and federal funds, additional restrictions apply. To ensure compliance with applicable law and University policy, the use of the University's information technology resources for political or commercial purposes, is prohibited.

Physical Security: All computers, data storage media and storage repositories that contain confidential information must be secured against loss or tampering. Portable computing devices such as laptops, hand-held equipment (PDAs) and data storage media pose a unique and significant risk for exposure of protected information and potential access to the University's administrative systems. For these reasons, special care must be taken with these devices. The login should never be set for automated login, and all protected data stored on any portable device must be encrypted. Store all such devices in a secure location.

POLICY TYPE: OPERATIONS