Acceptable Usage Policy

Policy Title:
Acceptable Usage Policy

Responsible Executive(s):
Jim Pardonek, Associate Director and Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This policy applies to all persons accessing and using computing, networking, telephoning, and information resources through any facility of the University. These persons include students, faculty, staff, persons retained to perform University work, and any other person extended access and use privileges by the University given the availability of these resources and services, and in accordance with university contractual agreements and obligations.

This policy covers all computing, networking, telephoning, and information resources procured through, operated, or contracted by the University. Such resources include computing and networking systems including those that connect to the University telecommunications infrastructure, other computer hardware, software, data bases, support personnel and services, physical facilities, and communications systems and services. In addition, please note that this policy covers all IoT devices.

II. Definitions

Not applicable.

III. Policy

Computing, networking, telephoning, and information resources at the University, including access to local, national, and international networks, are available to support students, faculty, and staff as they carry out the University's instructional, research, health care, administration, and public service missions. Therefore, the University encourages and promotes the access and use of these resources by the University community. However, access and use which do not support the University mission are subject to regulation and restriction to ensure that they do not interfere with this legitimate work.

Any access and use of computing, networking, telephoning, and information resources must not interfere with the University's instructional, research, health care and public service missions and should be consistent with the person's educational, scholarly, research, service, operational or management activities within the University.

Those who access and use University computing, networking, telephoning, and information resources are to take reasonable and necessary measures to safeguard the operating integrity of the systems and their accessibility by others, while acting to maintain a working environment conducive to carrying out the mission of the University efficiently and productively.

Responsibilities regarding system and resource use

Persons who access and use university computing, networking, telephoning, and information resources are responsible for:

- Respecting the rights of other individuals, including compliance with other university policies for students, faculty, and staff -- these rights include but are not limited to intellectual property, privacy, academic freedom, intimidation, insulting or harassing others, interfering unreasonably with an individual's work or educational performance, or the creation of an intimidating, hostile or offensive working/learning environment.
- Exercising caution when committing confidential information to electronic media.
- Using systems and resources in ways that do not interfere with or disrupt the normal operation of computing systems, nor interfere with the access and use of these systems and resources by others allowed to do so.
- Protecting the security of access to university computing and networking systems and the confidentiality and integrity of information stored on university computing and networking systems.
- Use of University network resources to gain or attempt to gain unauthorized access to remote networks, including remote computer systems.
- Installation on any of the University computer systems, a program which is intended to and likely to result in the eventual damage to a file or computer system and/or the reproduction of itself. This is directed towards, but not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.
- Knowing and obeying the specific policies established for the system and networks they access.
- Members of the University community with access to University electronic resources may not use these resources in a way that implies that the University is actually or implicitly espousing a particular view, or endorsing any person, organization, product, service or belief; similarly, they may not use the name, logos, facilities or resources of the University for any personal, commercial or similar purposes, or to participate in or intervene in (including the publishing or distribution of statements) any political campaign on behalf of, or in opposition to, any candidate for public office.

- You are responsible for the use of your account. You may not give anyone else access to your account. You must not use a Loyola network account that was not assigned to you. You may not try in any way to obtain a password or access code for another person's network account. You may not attempt to disguise the identity of the account or machine you are using. You must not attempt to circumvent access and use authentication, data protection schemes or exploit security loopholes without authorization.

Under no circumstances may individuals give others access to any system they do not administer or exploit or fail to promptly report any security loopholes. Individuals must act to maintain a working environment conducive to carrying out the mission of the University efficiently and productively. You are responsible for the security of your passwords and access codes. This includes changing them on a regular basis and keeping it confidential.

Individuals may not under any circumstances deliberately circumvent or attempt to circumvent data protection schemes or uninstall or disable any software installed by the university for the purpose of protecting the university from the intentional or unintentional disclosure of information.

Systems and network administration, and facilities management

Administrators of systems and networks are responsible for protecting users' rights, setting policies consistent with them, and publicizing them to their users. They have authority to control or to refuse access to anyone who violates these policies or threatens the rights of other users. They have the responsibility to notify those individuals affected by decisions they have made.

Administrators of systems and networks are empowered to take reasonable steps necessary to preserve the availability and integrity of the system, to restore the integrity of the system in case of malfunction, abuse, virus, and other similar situations, and to protect the integrity of university data and other assets. These steps may include deactivating accounts, access codes or security clearances, stopping processes, deleting affected files, and disabling access to computing, networking, telephony, and information resources.

All devices deployed in the PCI environment must be documented listing Acceptable uses for the technology, Acceptable network locations for the technology, along with a list of company approved products. Additionally, all devices within the PCI environment must be labeled containing the owner, contact information, and purpose of the device.

Demand for computing, networking, telephoning, and information resources may occasionally exceed available resources. Priorities should be established for allocating such resources, giving a higher priority to activities that are more essential to the mission of the University.

Access

Access to University computing resources is granted to ensure that all who use these resources are given sufficient access rights to fully perform their tasks without restriction,

but no more. University computing, networking, telephony and information resources are provided to support the University's missions in instruction, research, health care and public service. These resources may not be used for commercial purposes without authorization from the Vice President for Information Services. Please review the following policies for details of protecting information when accessing University computing resources:

- Access Control Policy
- Vendor Access to Internal Systems Policy
- Password Standards

Appeal of an administrative decision

Individuals who disagree with an administrative decision may appeal it to the appropriate resource manager or systems administrator. From there, a student may submit an appeal to the Dean of Students, a faculty member through their department administration either to the Provost or to the Vice President for the Health Sciences, and a staff member through their management to the Vice President for Human Resources. Individuals must submit these appeals according to any rules and procedures issued by system administrators or component administrators.

Noncompliance and sanctions

Individual units within the University may define "conditions of acceptable use" for facilities and resources under their control. These statements must be consistent with this general policy but may provide additional detail, guidelines, and restrictions. Such "conditions of acceptable use" should indicate the enforcement mechanism. Where no enforcement mechanisms exist, the procedures defined in the applicable University's standards of conduct, i.e., Student Handbook (students), Faculty Handbook (faculty), and Employee Handbook and Personnel Policies (staff), will apply.

Disregarding policies and procedures concerning access and use of computing, networking, telephoning, and information resources may result in the denial or removal of access privileges by administrators of systems and networks and may lead to disciplinary action under the applicable University's standards of conduct, as cited above. Additionally, such disregard may be referred to other authorities for civil litigation and criminal prosecution under applicable state and federal statutes.

Appeal of an administrative decision

Individuals who disagree with an administrative decision may submit an appeal to their manager or administrator. Students may submit an appeal to the Dean of Students, faculty through their department administration to the Provost, and a staff member through their management to the Vice President for Human Resources. Individuals must submit these appeals according to any rules and procedures issued by system administrators or component administrators.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Acceptable Usage Policy at the University by setting the necessary requirements

VI. Related Policies

Please see below for additional related policies:

- Rights and Responsibilities for the Access and Use of University Computing, Networking, Telephony and Information Resources
- Access and Acceptable Use of Public Access Computing and Networking Facilities and Services

Approval Authority:	ITESC	**Approval Date:**	April 19, 2017
Review Authority:	Jim Pardonek	**Review Date:**	July 16, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu