Acceptable Use Policy

Policy Title:
Acceptable Use Policy

Responsible Executive(s):
Jim Pardonek, 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 individuals who access or use the University's computing, networking, telecommunication, and information resources. This includes students, faculty, staff, contractors, and any other individuals granted access in accordance with University agreements and resource availability.

This policy applies to all computing, networking, telecommunication, and information resources that are procured, operated, or contracted by the University. These resources include computer systems, hardware, software, databases, support services and personnel, physical facilities, communication systems, and any devices connected to the University's telecommunications infrastructure—including all Internet of Things (IoT) devices.

II. Definitions

Telecommunications

III. Policy

Computing, networking, telecommunications, 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, 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.

Use of computing, networking, telecommunication, and information resources must not disrupt the University's instructional, research, or public service missions, and should

align with the user's academic, professional, or operational responsibilities within the University.

Users of University computing, networking, telecommunication, and information resources must take reasonable steps to protect system integrity and ensure accessibility for others, while supporting a productive environment aligned with the University's mission.

Responsibilities regarding system and resource use

The following guidelines apply to individuals who access and use university computing, networking, telecommunication, and information resources:

- Respect the rights of others by complying with all applicable University policies, including those related to intellectual property, privacy, academic freedom, and by avoiding behavior that is intimidating, harassing, or disruptive to others' academic or professional activities.
- Follow data classification policies when handling confidential or sensitive information in electronic formats.
- Use generative AI responsibly, ensuring outputs are ethical, lawful, and do not expose protected, confidential, or personally identifiable information. Avoid uploading sensitive data and ensure all AI use complies with data protection regulations such as FERPA and HIPAA. Institutional data may only be processed using approved tools.
- Use systems and resources responsibly to avoid disrupting normal operations or interfering with others' authorized access and use.
- Protect the security and integrity of University computing and networking systems, including safeguarding access credentials and stored information.
- Do not attempt unauthorized access to external networks or computer systems using University network resources.
- Do not install or distribute malicious software, including viruses, worms, or Trojan horses, that could damage systems or replicate without authorization.
- Comply with specific policies governing the systems and networks you access.
- Do not misuse University resources to imply endorsement of personal, commercial, or political views, or to participate in political campaigns. University names, logos, and resources must not be used for unauthorized purposes.
- You are responsible for your account. Do not share your credentials, use another person's account, or attempt to bypass authentication or security measures. 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.

System and Network Administration Responsibilities

- System and network administrators are responsible for protecting users' rights by establishing and communicating policies that align with University standards. They are authorized to restrict or deny access to individuals who violate these policies or compromise the rights of others and must notify affected individuals of any such actions.
- Administrators are empowered to take reasonable actions to maintain the availability, security, and integrity of University systems and data. This includes responding to malfunctions, abuse, malware, or other threats by deactivating accounts, revoking access, stopping processes, deleting compromised files, or disabling access to computing, networking, telecommunications, and information resources as needed.
- Devices within the PCI (Payment Card Industry) environment must be documented with clearly defined acceptable uses, approved network locations, and a list of authorized products. Each device within the PCI environment must also be labeled with the owner's name, contact information, and its intended purpose.
- In cases where demand for technology resources exceeds availability, priority should be given to activities that are most essential to the University's mission, including instruction, research, and public service.

Access to University Technology Resources

Access to University computing, networking, telecommunications, and information resources is granted to enable individuals to perform their roles effectively, with permissions limited to what is necessary for their responsibilities. These resources are intended to support the University's core missions of instruction, research, and public service, and may not be used for commercial purposes without prior authorization from the Vice President for Information Services.

For guidance on protecting information when accessing University systems, please refer to the following policies:

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

Appeals and Enforcement of Technology Use Policies

Individuals who disagree with an administrative decision regarding the use of University technology resources may appeal to the appropriate manager or system administrator.

- Students may escalate appeals to the Dean of Students.
- Faculty may appeal through their department administration to the Provost.

- Staff may appeal through their management chain to the Vice President for Human Resources.

All appeals must follow the procedures established by system or component administrators.

Noncompliance and Sanctions

University units may define specific "conditions of acceptable use" for the facilities and resources they manage. These conditions must align with the University's general policy and clearly outline enforcement mechanisms. Where no specific enforcement process exists, the procedures outlined in the applicable University standards of conduct will apply:

- Student Handbook (students)
- Faculty Handbook (faculty)
- Employee Handbook and Personnel Policies (staff)

Violations of policies governing the access and use of computing, networking, telecommunications, and information resources may result in the suspension or revocation of access privileges by system administrators. Such violations may also lead to disciplinary action under the relevant University conduct standards and, when appropriate, may be referred for civil or criminal proceedings under applicable laws.

Related Documents and Forms

Not applicable.

IV. Roles and Responsibilities

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

V. Related Policies

Please see below for additional related policies:

- Rights and Responsibilities for the Access and Use of University Computing, Networking, Telecommunications 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 9, 2025

Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu