TITLE: ACCEPTABLE USE OF TECHNOLOGY RESOURCES

Purpose: Create an environment where users of university technology resources understand their responsibilities, duties, and obligations. This document contains specific rules for appropriate utilization and conduct.

Policy and Procedure:

1. University technology resources are provided to support the mission of the University and are not to be used for purposes considered inappropriate by the University. By utilizing university technology resources, you agree that you are in compliance with all local, state, national, and international laws and related university policies. Furthermore, you agree to compensate, exonerate, and protect the University (and its representatives) for any claim, damage or cost related to your use of university technology resources.

2. All users of university technology resources are covered by Policy 6.1, including those who individually own, lease, or rent resources connected to university technology resources. Users and university technology resources include, but are not limited to:
    a. Users:
        i. Students
        ii. Employees
        iii. Volunteers
        iv. Contractors
        v. Guests
    b. Resources:
        i. Office desktop computers
        ii. Portable computing devices (laptops, tablets, smart devices, etc.)
        iii. Printers, Copiers, and Scanners
        iv. Servers and data center equipment (Physical and Virtual resources)
        v. Desk and common area phones
        vi. Network equipment and services (switches, wireless access, firewalls, etc.)
        vii. Cloud resources (e-Mail and communication platforms, Learning Management System, Student Information System, Finance and Operations, Event Management, etc.)

3. Operational security of university technology resources and information systems is based on physical security and adherence to compliance, regulatory, and industry standards. Technology Advancement maintains the authority for the establishment and enforcement of standards for account management, administrative programming code, device access, program and information access, and maintenance of aforementioned physical and virtual resources. Real-time and cumulative reporting of utilization and violations across all university technology resources and connected resources is maintained and reports are referred to appropriate functional areas for analysis, remediation, and enforcement activities:

a. Account credentials will not be shared
b. No unauthorized devices will be connected to university technology resources
c. Devices accessing university data will be configured with protections leveraging credential and timeout controls
d. No action will be taken which will or could circumvent or compromise security
e. No action will be taken which will or could impair the appropriate access to university technology resources
f. No unapproved software, equipment, or services will be used with university technology resources
g. No viruses, malware, spyware, or similar malicious software will be knowingly used or circulated
h. No student or protected data will be stored, processed, transmitted, or otherwise interacted with outside of approved methods
i. Employees, volunteers, student workers, contractors, etc. will complete cybersecurity training at least annually
j. Student cybersecurity training is provided through academic courses and ad-hoc sessions

4. Appropriate use of university technology resources includes:
    a. University technology resources will only be utilized for LCU related purposes
    b. Passwords on accounts comply with complexity requirements
    c. Report unauthorized use of accounts immediately
    d. When release of protected data is authorized, employees are responsible for transmitting only requisite information in the most secure environment possible
    e. Treat transmissions via university technology resources as tangible documents
    f. Store and process data only within approved and proscribed systems and processes
    g. Apply system and security updates to all university technology resources and connected resources
    h. Requisition analysis and approval for any new software, equipment, or services associated with university technology resources

5. Inappropriate use of university technology resources includes, but is not limited to:
    a. Accessing, storing, or transmitting illicit (such as threatening, obscene, discriminating, harassing, offensive, or conflicting in any way with the values of the University) material
    b. Accessing, storing, or transmitting credentials and/or access methods belonging to other users or systems
    c. Accessing data without explicit authorization
    d. Interfering with the university technology resource security, monitoring, and operations
    e. Utilization or installation of unauthorized software, equipment, or services
    f. Copying and/or distributing software or data owned by the University

g. Creation, alteration, and/or destruction of university data and records. Examples can be found in LCU Policy 7.23.1 Retention of Records Schedule
h. Leveraging university technology resources to obtain unauthorized access to other computing systems
i. Conducting business unrelated to the University, such as personal advertisements, solicitations and promotions, or for reproduction of political or commercial material
j. Unauthorized transmission of data: Sharing protected student, employee, or other information in violation of applicable laws or regulations (including but not limited to FERPA, HIPAA, COPPA, GDRR, FSA, FTC Safeguards, or other state and federal regulations).
k. Unsecured transmission of data: Sharing or transmitting protected data by unsecured means that compromise privacy or data security.

6. Management and maintenance standards of university technology resources are set by Technology Advancement according to compliance, regulatory, and industry standards. These standards include, but are not limited to:
    a. Firmware and software update cycles and requirements
    b. Analysis and approval of new university technology resources (hardware, equipment, software, services, etc.)
    c. Technology documentation processes for compliance with local, state, national, and international standards for data protection
    d. Network security and integrity configurations and monitoring
    e. Deployment and maintenance of hardware, software, and services necessary for job functions
    f. Asset and inventory management, depreciation tracking, retirement and replacement scheduling and processing of university technology resources

7. Technology Advancement reserves the right and has the responsibility to examine files, directories, logs, communications, and processes associated with university technology resources. Causes for examination include, but are not limited to:
    a. Security or integrity of university technology resources is or may be threatened
    b. Detrimental, prohibited, and/or unlawful practices
    c. Backup and testing processes
    d. Upgrade and maintenance processes
    e. Diagnostic and troubleshooting processes
    f. Cybersecurity mitigation and training
    g. Inappropriate processing and/or dissemination of protected data
    h. Suspected violations of policy or applicable law

8. Access to university technology resources is for authorized personnel, students, and guests only. Users are responsible for resources in their purview and will not access resources to

which they have not been granted authorization. Access is granted by Technology Advancement based upon a given user's role with the University.

9. Violations of policy will be collected, analyzed and processed in accordance with this policy, the University Student Handbook, Employee handbook, and any related policies and/or applicable regulation and law:
    a. Report suspected or witnessed violations immediately to the University via ChapDesk and/or Data Security
    b. Access will be restricted as first step in collecting and analyzing suspected violations
    c. Investigation and remediation will involve interview processes with the Vice President of Technological Advancement and appropriate leadership in the context of the violation
    d. Pending the results of the investigation, referrals to appropriate enforcement groups or agencies will be carried out

10. Cancellation of access to university technology resources can occur as a result of termination of enrollment, employment or violations of policy and standards:
    a. Student access will automatically terminate no later than 90 days after their enrollment ends
    b. Employee access will automatically terminate with conclusion of employment at the University unless granted an exception by the Assistant Vice President of Human Resources and the Vice President for Technological Advancement
    c. Third party access will be cancelled at the completion of approved work
    d. Access will be cancelled immediately on determination of policy, standards, or applicable law violations

OFFICE RESPONSIBLE FOR THIS POLICY: Vice President for Technological Advancement

RELATED DOCUMENTS, POLICIES, PROCEDURES, and FORMS:

- LCU Handbook 2.1 Employee Handbook
- LCU Handbook 3.1 Financial Handbook
- LCU Handbook 4.1 Faculty Handbook
- LCU Policy 4.10 Instructional Technology
- LCU Policy 6.2 Written Information Security Plan (WISP)
- LCU Policy 6.3 Information Management Systems
- LCU Policy 6.4 Use of Electronic and Social Media
- LCU Policy 7.2 Privacy of Student Records
- LCU Policy 7.10 Intellectual Property Policy
- LCU Policy 7.11 Student Academic Records
- LCU Policy 7.19 Students with Disabilities
- LCU Policy 7.23 and 7.23.1 Retention and Disposition of Records

POLICY HISTORY:

- Prior Revision: 07-08-20
- Revised to modernize the policy according to compliance, regulatory, and industry best practices and improve accessibility