POLICY STATEMENT 121 STANDARD 2
SYSTEM ACCEPTABLE USE

POLICY DIGEST

Monitoring Unit: Office of Information Technology
Initially Issued: October 17, 2022
Last Revised: none

I. PURPOSE

As an institution of higher education, Louisiana State University at Eunice ("University" or "LSU Eunice") is charged with maintaining systems and data for administrative and academic purposes. These assets are critical to the mission of the University, and the security of these systems and datasets must be managed with a formalized Information Security Program.

A major element of protecting the University's Information Technology assets in maintaining acceptable usestandards that clearly define what is considered the acceptable uses of LSU Eunice network, systems, and applications.

The purpose of this standard is to describe acceptable use standards as they pertain to the University Information Technology systems.

II. DEFINITIONS

Bring Your Own Device (BYOD). BYOD refers to use of personal devices to connect to the organizational network and systems.

Biometric Authentication. Biometric authentication is a technology employed on devices that uses biometrics (body characteristics and calculations) to identify a user and enforce access control.

Encryption in transit. Encryption in transit is employed on data when it is transferred over a network.

Endpoint protection. Endpoint protection is a software or configurations implementedon computing endpoints to provide security from malware and unauthorized access.

Firmware. Firmware is a low-level type of computing software that interfaces with the device's hardware.

Jailbreaking. Jailbreaking is a process utilized to modify a smart device or other electronic device to remove restrictions imposed by the manufacturer or operator.

Least privilege. Least privilege is a principal that requires users and programs to only have the necessary privileges to complete their tasks.

III. STANDARDS

A. Access control

1. Users must properly log off and/or password protect any information system when leaving the immediate work area for any length of time.

2. Anonymous/automatic system logon features shall not be configured on the University owned information systems unless authorized by the Office of Information Technology (OIT).

3. Administrative access to any University owned information system shall be restricted to appropriate support personnel. The principal of least privilege shall always be enforced.

B. Data Storage

1. Data created on LSU Eunice information systems shall be deemed the property of the University unless otherwise stipulated by intellectual property agreements or other legal arrangements with the University.

2. All end user mobile computing devices must be encrypted in a manner consistent with the data stored on them and University encryption standards.

3. Users must store all sensitive/confidential University data on authorized and approved storage services, whether on premise or cloud.

C. Physical Security

1. Users must take appropriate measures to physically secure University owned devices regardless of location. These measures include, but are not limited to, keeping devices on person when travelling, not leaving devices in car where it is visible, etc.

D. Bring Your Own Device (BYOD)

1. BYOD is expected in the University environment; however, to maintain security of LSU Eunice network, systems, applications, and data, all BYOD devices must meet the following requirements:

   a. Must have latest firmware updates, patches, service packs, and/or operating system version.

   b. All devices must be secured with a password, biometrics, or other appropriate access controls.

   c. BYOD devices must not be configured in a manner to bypass security measures put in place by the manufacturer (e.g., jailbreaking).

   d. BYOD devices must have endpoint protection, anti-virus, and/or anti-malware application installed, configured, operational, and are up to date.

E. Usage Activity

1. All information contained within the University network, system, and applications are subject to examination by the University where:

   a. There is a suspicion of misconduct under the University policies, or suspicion of violation of state and federal laws.

   b. It is necessary to comply with or verify compliance with state or federal law including eDiscovery procedures.

2. LSU Eunice must implement processes and procedures for reviewing of usage activities including, but not limited to:

   a. List of individuals or entities that can review usage activity.

   b. List of individuals or entities that approve the review of usage activity.

   c. List of individuals or entities that can request a review of usage activity.

   d. List of conditions under which usage activity information can be disclosed to any party.

IV. REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	2/25/2022	Initial Draft	OIT