POLICY STATEMENT 121
ACCEPTABLE USE FOR INFORMATION TECHNOLOGY SYSTEMS

POLICY DIGEST

Monitoring Unit: Office of Information Technology
Initially Issued: October 17, 2022
Last Revised: December 15, 2025

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 acceptable use of these systems and data sets must be managed with a formalized Acceptable Use Policy.

The purpose of this policy is to outline certain specific responsibilities that each user acknowledges, accepts, and agrees to follow when using Information Technology (IT) assets provided at, for, and by and/or through LSU Eunice, regardless of location of the IT asset.

II. DEFINITIONS

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

Digital Millennium Copyright Act (DMCA). DMCA is a 1998 United States copyright law that criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works.

Internet of Things (IoT). IoT is the interconnection via the network of computing devices embedded in everyday objects, enabling them to send and receive data

Packet Capture. Packet capture is a method of using a computer program or piece of hardware that can intercept and log traffic that passes over a digital network or part of a network.

Port scanning. Port scanning is a method of determining which ports/services on a network are open and could be receiving or sending data.

III. POLICY STATEMENT

A. Network Acceptable Use

1. LSU Eunice shall define acceptable use parameters for all network related assets, configurations, and activities including, but not limited to,

    a. Legal Compliance

b. Internet of Things (IoT)

c. Network analysis (e.g., packet captures, port scanning)

d. Network utilization (e.g., bandwidth monitoring)

e. Network peripherals (e.g., hubs, routers, switches)

f. Network access (e.g., device registration)

B. System Acceptable Use

1. LSU Eunice shall define acceptable use parameters for all system related assets, configurations, and activities, including but not limited to:

a. Access Controls (e.g., screen lock, logon/logoff procedures)

b. Data storage

c. Physical security (e.g., theft prevention, travel precautions)

d. BYOD security requirements

e. Usage activity auditing

C. Application Acceptable Use

1. LSU Eunice shall define acceptable use parameters for all application related configurations, and activities including, but not limited to:

a. Application permissions and credentials

b. Software installation, usage, and removal

c. Data transmission

d. Malicious software

e. Digital communication services (e.g., email, chat, conferencing, etc.)

D. Electronic Mail Acceptable Use

1. LSU Eunice shall define acceptable use parameters for electronic mail usage including, but not limited to:

a. Eligibility

b. Account retention procedures

c. Storage and retention

d. Privacy and applicability of laws and policies

E. Artificial Intelligence (AI) Acceptable Use

1. LSU Eunice shall define acceptable use standards for use of Artificial Intelligence including, but not limited to:

a. Procurement of AI products and services

b. Use of AI products and services

c. Data security

IV. STANDARDS

A. The network acceptable use standards are outlined in Standard LSU Eunice-ST-121-1.

B. The system acceptable use standards are outlined in Standard LSU Eunice-ST-121-2.

C. The application acceptable use standards are outlined in Standard LSU Eunice-ST-121-3.

D. The electronic mail acceptable use standards are outlined in Standard LSU Eunice-ST-121-4.

E. The artificial intelligence acceptable use standards are outlined in Standard LSU Eunice-ST-121-5.

V. REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	02/25/2022	Initial Draft	OIT
0.1	12/15/2025	Standard 5 added	OIT