POLICY STATEMENT 121
ACCEPTABLE USE

Monitoring Unit: Information Technology Services
Initially Issued: July 21, 2023

PURPOSE

As an institution of higher education, the Louisiana State University A&M Baton Rouge Campus (“University” or “LSUAM”) is charged with maintaining systems and data for administrative, academic, and research 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 IT assets provided at, for, and by and/or through LSUAM, regardless of location of the IT asset.

DEFINITIONS

Bring Your Own Device (BYOD) – BYOD refers to the 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.

POLICY STATEMENT

A. Network Acceptable Use
   1. LSUAM shall define acceptable use standards for all network related assets, configurations, and activities including, but not limited to:
      a. Legal Compliance (e.g., DMCA)
      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. LSUAM shall define acceptable use standards 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. LSUAM shall define acceptable use standards for all applications-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.)

STANDARDS

A. The network acceptable use standards are outlined in Standard PS-121-ST-1.
B. The system acceptable use standards are outlined in Standard PS-121-ST-2.
C. The application acceptable use standards are outlined in Standard PS-121-ST-3.

EXCEPTIONS AND NON-COMPLIANCE

- Please refer PS-120-ST-4 for additional information related to exceptions.
- Please refer PS-120 for additional information related to Policies and Standards non-compliance.

REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	7/21/2023	Initial Draft	Information Technology Services