POLICY STATEMENT 121 STANDARD 1
NETWORK ACCEPTBLE 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 use standards 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 LSU Eunice network.

II. DEFINITIONS

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.

Domain Name Services (DNS). DNS is a service responsible for translating device domain names into Internet Protocol (IP) addresses.

Dynamic Host Configuration Protocol (DHCP). DHCP is a service responsible for the assignment of IP addresses to devices on a network.

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.

Network Proxy Service. Network Proxy Service is a system that acts as a gateway between a local segmented network and a larger-scale network such as the internet.

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. STANDARDS

A. Legal Compliance

1. University network resources must not be utilized to access and/or transmit any digital media that violates local, state, or federal law.

2. University network resources must not be utilized in any form to harass, intimidate, or threaten other persons.

3. LSU Eunice must ensure appropriate processes and procedures are in effect to respond to incidents involving unauthorized use and distribution of copyrighted materials.

4. LSU Eunice must ensure appropriate processes and procedures as in effect, as well as technical infrastructure is implemented to provide network activity information to support investigations and/or respond to legal requests.

B. Internet of Things (IoT)

1. Appropriate processes and procedures must be implemented to allow users of LSU Eunice network to connect IoT devices.

2. All IoT devices connected to the network (wired or wireless) must be proactively managed, updated, and patched by the owner of the device.

C. Network Analysis

1. Users of LSU Eunice network are not authorized to conduct network analysis practices, such as port scanning, vulnerability scans, etc., These activities can lead to network degradation or malfunction.

2. Network packet capturing/sniffing are strictly prohibited. There may be a need to conduct such activities for troubleshooting purposes and as such, any requirements to conduct such activities must be coordinated with the Office of Information Technology (OIT).

D. Network Utilization

1. Users are not authorized to monopolize or disproportionately use shared network resources or degrade network services in any manner that interferes with authorized use. The LSU Eunice Office of Information Technology (OIT) reserves the right to remove any device from the network that impacts the performance of the University's network.

2. Users are not authorized to leverage the University's network to interfere with any third-party network.

E. Network Infrastructure

1. Unauthorized extension of the University network by way of network hardware such

as hubs, switches, routers, wireless access points, etc., is strictly prohibited.

2. Users are not authorized to remove and/or disable University network infrastructure.

3. Infrastructure services such as DNS, DHCP, and/or network proxy services must be offered centrally by OIT. Users are not authorized to create, maintain, and/or offer network infrastructure services on the University network.

F. Network Access

1. All devices on the network must be registered in the systems providing network infrastructure services.

2. All remote access to networks owned and/or managed by the University must be accomplished using remote access method reviewed and approved by OIT.

3. OIT reserves the right to remove any device from the university network if the device is involved in data transmission which is harmful to the operation of the network and/or ifappropriate processes have not been followed for review and approval.

IV. REVISION HISTORY

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