POLICY STATEMENT 121 STANDARD 3
APPLICATIONS 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 (IT) 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 the University Information Technology applications.

II. DEFINITIONS

Digital Communication Services (DCS). DCS is any digital service/application that allows two or more people to communicate via text, audio, video, or any combination of these. Examples include, but are not limited to, email, instant messaging, IRC, video conferencing, etc.

Malicious Software (Malware). Malware is any software intentionally designed to cause damage to a computer or computer network.

Voice over Internet Protocol (VoIP). VoIP is the method and technologies used for delivery of voice communications and multimedia sessions over the Internet.

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

III. STANDARDS

A. Application permissions and credentials

1. All users must access University provided applications they are authorized to access and only for the purposes of which the access was intended.

2. All University applications must be configured to utilize University provided

credentials and where possible leverage Single Sign On services.

3. Users are required to maintain their credentials and credentials for any other accounts they are entrusted with in a secure manner. Credentials must not be shared and/or divulged to unauthorized individuals.

4. Users will be responsible for all actions carried out with their accounts and/or by accounts entrusted to them.

B. Software installation, usage, and removal

1. Any software, regardless of type (freeware, licensed, and/or open source), must not be installed without appropriate review and approval as outlined in the University processes for Software Acquisition.

2. Users must not disable or uninstall endpoint protection software on any system owned by the University.

3. All software installed on any University owned systems or devices must be for and/or related to the University business.

C. Data Transmission

1. All transmission of data via applications (e.g., e-mail, websites, cloud storage solutions, etc.) must be carried out using secure means such as, encryption.

2. All transmission of sensitive/confidential data must be conducted via mechanisms that have been reviewed and approved by LSU Eunice Office of Information Technology.

D. Malicious Software (Malware)

1. Users must not knowingly install Malware on University owned technology resources.

2. In the event of BYOD, users are responsible for ensuring their devices are not infected with malware.

E. Digital Communication Services (DCS)

1. Use of Digital Communication Services are subject to all University policies.

2. Users must utilize University provided and/or approved Digital Communication Services for all University business. This includes, but is not limited to, applications/platforms for e-mail, chat, video conferencing,VoIP, etc.

3. Users must not utilize DCS to access, create, transmit, print, or download material that is defamatory, obscene, fraudulent, harassing (including uninvited amorous or sexual messages), threatening, incites violence, or contains slurs, epithets, or anything that may be reasonably construed as harassment or disparagement based on race, color, national origin, gender, sexual orientation, age, disability, or religion or to access, send, receive, or solicit sexually oriented messages or images or any other communication prohibited by law or other University policies or directives.

4. Users must not intentionally obscure their identity when communicating via the University provided DCS.

IV. REVISION HISTORY

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