POLICY STATEMENT 132
SYSTEM SECURITY

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. Security and management of systems involved in daily operations is critical in supporting the University and thus must be managed with a formalized System Security Policy.

The purpose of this policy is to define the required processes and activities pertaining to system security.

DEFINITIONS

Bring Your Own Device (BYOD) - BYOD refers to the use of personal devices, for enterprise purposes to conduct University business, especially as it relates to connecting to technical resources provided by the enterprise entity.

Database – A repository of information or data, which may or may not be a traditional relational database system. For the purpose of these policies and standards, end user database applications, such as Microsoft Access, are not in scope.

Endpoint Application – Software packages that are installed on or executed directly from an endpoint to provide additional functionality to the endpoint.

Endpoint Protection - An application utilized to protect endpoints (laptops, desktops, servers, mobile devices, etc.) from malicious activities. This is commonly known as anti-virus/anti-malware software or endpoint detection and response/EDR solution.

Host-based Firewall – A software program/application installed directly on an endpoint device (physical or virtual), either as part of the Operating System or separately, to manage network traffic flow at the host level to support enhanced network security for the host.

Mobile Device Management (MDM) – The administration of mobile devices such as smartphones, tablets, computers, laptops, and desktop computers.

Physical media – A data storage medium that is typically attached internally to an endpoint. For example, Magnetic tapes, Solid State Drives (SSDs)

Operating System – A computer program, implemented in either software or firmware, which acts as an intermediary between users of a computer and the computer hardware.

Removable media – A portable data storage medium that can be added to or removed from a computing device or network. For example, CD, DVD, USB drive, thumb drive, etc.

Web Application – A network application hosted on a web server, typically accessed via client software or a web browser that provides specific functionality to end users.

POLICY STATEMENT

A. Endpoint Protection
    1. LSUAM shall identify and implement solutions for endpoint protection.
    2. LSUAM shall define and implement processes for identifying, containing, and remediating compromised systems.
B. Host Based Network Protection
    1. LSUAM shall define processes and procedures for configuring, updating, and maintaining host-based network protection for all institution owned devices.
    2. LSUAM shall define host-based firewall requirements for all institution owned devices.
C. Removable and Physical Media
    1. LSUAM shall define general usage requirements for removable and physical media.
    2. LSUAM shall define requirements for removable and physical media containing private and/or confidential data.
D. File Integrity Monitoring
    1. LSUAM shall identify and implement solution(s) for file integrity monitoring.
    2. LSUAM shall establish processes and procedures for management of alerts related to file integrity monitoring.
E. Mobile Device Management (MDM) and Bring Your Own Device (BYOD)
    1. LSUAM shall define security requirements for management of LSU owned devices through an MDM product.
    2. LSUAM shall define security requirements for management of personally owned devices connected to enterprise networks.
F. Endpoint Application Management
    1. LSUAM shall define criteria for software installation on institution owned devices.
    2. LSUAM shall define processes and procedures for management of applications installed on institution owned devices
G. Operating System Management
    1. LSUAM shall define security requirements for operating systems utilized for institution owned devices.

H. Web Application Management
    1. LSUAM shall define security requirements for web applications designed and implemented on institution owned devices.
I. Database Management
    1. LSUAM shall define security configuration requirements for all databases utilized for institution purposes.

STANDARDS

A. The Endpoint Protection standards are outlined in PS-132-ST-1.
B. The Host based Network Protection standards are outlined in Standard PS-132-ST-2.
C. The Removable and Physical Media standards are outlined in Standard PS-132-ST-3.
D. The File Integrity Monitoring are outlined in Standard PS-132-ST-4.
E. The MDM and BYOD standards are outlined in Standard PS-132-ST-5.
F. The Endpoint Application Management standards are outlined in Standard PS-132-ST-6.
G. The Operating System Management standards are outlined in Standard PS-132-ST-7.
H. The Web Application Management standards are outlined in Standard PS-132-ST-8.
I. The Database Management standards are outlined in Standard PS-132-ST-9.

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