



POLICY STATEMENT 132 SYSTEM SECURITY

POLICY DIGEST

Monitoring Unit: Office of Information Technology
Initially Issued: June 20, 2023
Last Revised: None

I. PURPOSE

As an institution of higher education, the Louisiana State University at Eunice Campus (“University” or “LSU Eunice”) 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.

II. 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)

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

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

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

47 **III. POLICY STATEMENT**

48 A. Endpoint Protection

- 49 1. LSU Eunice shall identify and implement solutions for endpoint protection.
- 50 2. LSU Eunice shall define and implement processes for identifying, containing, and
51 remediating compromised systems.

52 B. Host Based Network Protection

- 53 1. LSU Eunice shall define processes and procedures for configuring, updating, and
54 maintaining host-based network protection for all institution owned devices.
- 55 2. LSU Eunice shall define host-based firewall requirements for all institution owned
56 devices.

57 C. Removable and Physical Media

- 58 1. LSU Eunice shall define general usage requirements for removable and physical
59 media.
- 60 2. LSU Eunice shall define requirements for removable and physical media containing
61 sensitive/confidential data.

62 D. File Integrity Monitoring

- 63 1. LSU Eunice shall identify and implement solution(s) for file integrity monitoring.
- 64 2. LSU Eunice shall establish processes and procedures for management of alerts
65 related to file integrity monitoring.

66 E. Mobile Device Management (MDM) and Bring Your Own Device (BYOD)

- 67 1. LSU Eunice shall define security requirements for management of LSU owned
68 devices through an MDM product.
- 69 2. LSU Eunice shall define security requirements for management of personally owned
70 devices connected to enterprise networks.

71 F. Endpoint Application Management

- 72 1. LSU Eunice shall define criteria for software installation on institution owned devices.

73 2. LSU Eunice shall define processes and procedures for management of applications
74 installed on institution owned devices.

75 G. Operating System Management

76 1. LSU Eunice shall define security requirements for operating systems utilized for
77 institution owned devices.

78 H. Web Application Management

79 1. LSU Eunice shall define security requirements for web applications designed and
80 implemented on institution owned devices.

81 I. Database Management

82 1. LSU Eunice shall define security configuration requirements for all databases utilized
83 for institution purposes.

84 **IV. STANDARDS**

85 A. The Endpoint Protection standards are outlined in [LSU Eunice Policy Statement 132](#)
86 [Standard 1](#).

87 B. The Host based Network Protection standards are outlined in [LSU Eunice Policy](#)
88 [Statement 132 Standard 2](#).

89 C. The Removable and Physical Media standards are outlined in [LSU Eunice Policy](#)
90 [Statement 132 Standard 3](#).

91 D. The File Integrity Monitoring are outlined in [LSU Eunice Policy Statement 132 Standard](#)
92 [4](#).

93 E. The MDM and BYOD standards are outlined in [LSU Eunice Policy Statement 132](#)
94 [Standard 5](#).

95 F. The Endpoint Application Management standards are outlined in [LSU Eunice Policy](#)
96 [Statement 132 Standard 6](#).

97 G. The Operating System Management standards are outlined in [LSU Eunice Policy](#)
98 [Statement 132 Standard 7](#).

99 H. The Web Application Management standards are outlined in [LSU Eunice Policy](#)
100 [Statement 132 Standard 8](#).

101 I. The Database Management standards are outlined in [LSU Eunice Policy Statement 132](#)
102 [Standard 9](#).

103 **V. REVISION HISTORY**

Version	Date	Change Description	Edited By
0.1	3/5/2023	Initial Draft	Office of Information Technology

104

--	--	--	--