



1
2
3
4
5
6
7
8
9
10
11
12
13

POLICY STATEMENT 131 INFORMATION TECHNOLOGY NETWORK SECURITY

POLICY DIGEST

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

I. PURPOSE

14 As an institution of higher education, the Louisiana State University at Eunice Campus
15 (“University” or “LSU Eunice”) is charged with maintaining systems and data for administrative,
16 academic, and research purposes. All systems and applications rely on a robust network
17 infrastructure. Security of the network infrastructure is paramount and thus must be managed
18 with a formalized Network Security Policy.

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

II. DEFINITIONS

22 **Firewall.** A device or program that controls the flow of network traffic between networks or hosts
23 that employ differing security posture.

24 **Intrusion Detection Systems (IDS).** A security service that monitors and analyzes network or
25 system events for the purpose of finding, and providing real-time or near real-time warning of,
26 attempts to access system resources in an unauthorized manner.

27 **Intrusion Prevention Systems (IPS).** System which can detect an intrusive activity and can
28 also attempt to stop the activity, ideally before it reaches its targets.

29 **Remote Access.** Access to an organizational asset by a user (or another asset) communicating
30 through an external, non-organization-controlled network (e.g., the Internet).

III. POLICY STATEMENT

A. Network Architecture

- 33 1. LSU Eunice shall implement processes and procedures for network design and
34 architecture that support redundancy and scalability.
- 35 2. LSU Eunice shall develop processes and procedures for management of network
36 configuration.
- 37 3. LSU Eunice shall develop processes and procedures for an asset’s placement on
38 enterprise network.

39 4. LSU Eunice shall define parameters/requirements for attaining access to the network.

40 B. Network Firewall Devices and Appliances

41 1. LSU Eunice shall implement firewall devices/appliances at identified locations within
42 a network based on a defined criterion.

43 2. LSU Eunice shall define and document default enterprise firewall configuration.

44 3. LSU Eunice shall conduct periodic reviews of enterprise firewall rulesets and
45 configurations.

46 C. IDS/IPS

47 1. LSU Eunice shall implement IDS/IPS services at appropriate network locations.

48 2. LSU Eunice shall define processes and procedures for IDS/IPS related alerts.

49 D. Remote Access

50 1. LSU Eunice shall identify and implement appropriate technologies that support
51 remote access to enterprise network.

52 2. LSU Eunice shall develop processes and procedures that support remote access to
53 enterprise network.

54 E. Wireless

55 1. LSU Eunice shall define parameters for wireless network use within the institution.

56 2. LSU Eunice shall define processes and procedures for supported wireless network
57 configuration.

58 F. Cloud Based Network

59 1. LSU Eunice shall define security requirements for cloud-based networks associated
60 with the institution.

61 **IV. STANDARDS**

62 A. The Network Architecture standards are outlined in [LSU Eunice-131 Policy Statement](#)
63 [131 Standard 1](#).

64 B. The Network Firewall Devices and Appliances standards are outlined in [LSU Eunice](#)
65 [Policy Statement 131 Standard 2](#).

66 C. The IDS/IPS standards are outlined in [LSU Eunice Policy Statement 131 Standard 3](#).

67 D. The Remote Access standards are outlined in [LSU Eunice Policy Statement 131](#)
68 [Standard 4](#).

69 E. The Wireless standards are outlined in [LSU Eunice Policy Statement 131 Standard 5](#).

70 F. The Cloud Based Network standards are outlined in [LSU Eunice Policy Statement 131](#)
71 [Standard 6](#).

72 **V. REVISION HISTORY**

73

Version	Date	Change Description	Edited By
0.1	12/08/2022	Initial Draft	Office of Information Technology

74