



**POLICY STATEMENT 129**  
**INFORMATION TECHNOLOGY PHYSICAL SECURITY**

**POLICY DIGEST**

**Monitoring Unit:** Office of Information Technology  
**Initially Issued:** April 20, 2023  
**Last Revised:** April 20, 2023

**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. These assets are critical to the mission of the University, and the physical security of these systems and data sets must be managed with a formalized Physical Security Policy.

The purpose of this policy is to define the required processes and activities involved in the management of assets as it pertains to physical security.

**II. DEFINITIONS**

**Asset.** A resource, process, product, information infrastructure, etc. whose loss or compromise could intangibly affect its integrity, availability, or confidentiality, or it could have a tangible dollar value. The loss or compromise of an asset could also affect an entity’s ability to continue business. Examples of assets including, but are not limited to, equipment, software, algorithms, and data.

**Data.** Any information residing on the University Information Technology (IT) Infrastructure or held on any other IT Infrastructure on behalf of the University. This data includes files, documents, messages in any format, including e-mail messages and posts made on any Social Media site maintained by/for the University or its units. All data created and/or maintained by a User is also subject to this Policy, even if the data is created and/or stored on the User’s own personal computer, smartphone, or other personal device.

**Information Technology Asset.** IT Asset is a subset of Asset and specifically refers to hardware (laptops, desktops, servers/virtual servers, external storage devices, mobile devices, etc.) utilized to store, process, access, and/or handle Data.

**III. POLICY STATEMENT**

**A. Surveillance Cameras**

1. LSU Eunice shall establish processes and procedures for management of surveillance technology.
2. LSU Eunice must identify a department responsible for overseeing surveillance

- 41 technologies.
- 42 3. LSU Eunice shall define processes and procedures for reviewing and approving  
43 surveillance proposals.
- 44 4. LSU Eunice shall appropriately and clearly classify surveillance related data as well  
45 as data retention policies for such data.

46 B. Physical Access Controls

- 47 1. LSU Eunice shall define parameters to identify what constitute a secure area on  
48 campus as it relates to critical and/or sensitive IT assets.
- 49 2. LSU Eunice shall define a process for determining the elements involved in  
50 constructing a physical security perimeter to protect sensitive areas.
- 51 3. LSU Eunice shall define requirements to ensure that only authorized personnel are  
52 allowed access to controlled areas.

53 C. Facility Planning

- 54 1. LSU Eunice shall ensure aspects of physical security of IT assets to be held within a  
55 facility is included in the design for new facilities or upgrades to an existing one.
- 56 2. LSU Eunice shall ensure that requirements such as cooling, power, etc., are included  
57 in the design for new facilities or upgrades to an existing one.
- 58 3. LSU Eunice shall define guidelines for the fire protection of data centers containing  
59 enterprise information assets, as all as any other areas classified as data centers by  
60 the University or departments.

61 **IV. STANDARDS**

- 62 A. The Physical Access Controls standards are outlined in [Standard LSU Eunice-ST-129-1](#).
- 63 B. The Facility Planning standards are outlined in [Standard LSU Eunice-ST-129-2](#).
- 64 C. The Surveillance Cameras standards are outlined in [Standard LSU Eunice-ST-129-3](#).

65 **V. REVISION HISTORY**

66

Version	Date	Change Description	Edited By
0.1	11/14/2022	Initial Draft	OIT

67