



## POLICY STATEMENT 124 STANDARD 2 DATA HANDLING

### POLICY DIGEST

Monitoring Unit: Office of Information Technology  
Initially Issued: December 12, 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 acceptable use of these systems and data sets must be managed with a formalized Data Management policy.

A major element of protecting the University’s Information Technology (IT) assets is ensuring that all University data is handled in a manner that sustains its confidentiality, integrity, and availability.

The purpose of this standard is to describe processes and procedures that should be followed for data handling at LSU Eunice.

### 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 LSU Eunice’s ability to continue business.

**Data.** Any information residing on the University 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.

**Data Custodian.** Information technology staff with day-to-day responsibilities for the capture, maintenance, and dissemination of data.

**Data Functional Owner.** Organizational representatives who have planning and decision-making responsibilities for data, related to their functional area. They are members of the academic or functional areas of the University (e.g., Registrar, Director, Associate Director, Assistant Director, Associate/Assistant Dean, or equivalent) and are appointed by Data Trustees, i.e., University Administration Officials.

**Data Stewards.** Operational managers in a functional area with day-to-day responsibilities for

42 managing business processes and establishing business rules for production transaction  
43 systems and associated datasets.

44 **User.** Any individual or entity that utilizes an asset. A user can be an individual, application,  
45 information system, network, etc.

### 46 **III. STANDARDS**

#### 47 A. Data Management

48 1. Under the purview of IT Governance, Data Governance subcommittee must  
49 establish data governance framework that outline data access requirements through  
50 a Master Access Plan (MAP).

51 2. MAP must be established using the principles of least privilege and need-to-know,  
52 i.e., access is only granted to users to support their daily tasks and responsibilities.

53 3. Data Governance subcommittee must establish criteria for maintaining  
54 confidentiality, integrity, and availability of defined data elements and their  
55 classification.

#### 56 B. Public Data

57 1. Data Stewards and Data Custodians must review data classified as Public Data and  
58 the assets the data is stored on to maintain its integrity and availability as per the  
59 criteria defined by Data Governance.

60 2. LSU Eunice must establish processes and procedures to disclose public data and  
61 the means through which disclosure can happen.

#### 62 C. Private and Confidential Data

63 1. Data Stewards and Data Custodians must not engage in collection of private and  
64 confidential data unless a business need exists to collect such data.

65 2. LSU Eunice must establish processes and procedures to maintain an inventory of  
66 assets where private and confidential data exists.

67 3. Data Stewards must authorize a user's access to private and confidential data and  
68 must maintain a signed confidentiality agreement on file based on risk assessment of  
69 the asset where the data is stored.

70 4. LSU Eunice must establish processes and procedures to make users aware of their  
71 responsibilities as it relates to data handling of sensitive information (i.e., private, and  
72 confidential data).

73 5. Users are not authorized to access sensitive information beyond the need of their  
74 responsibilities and tasks associated with them. Any unauthorized access will result  
75 in disciplinary action, up to and including termination.

76 6. Users are not authorized to maintain unauthorized copies of sensitive information.

- 77 D. Data storage and sharing
- 78 1. Sensitive information must only be stored on authorized systems and applications,  
79 and electronic copies, including backups, must be kept at a minimum.
- 80 2. Sharing of sensitive information must be carried out using secure means including,  
81 but not limited to, secure file transfer, encrypted e-mails, etc. Sensitive information  
82 must not be shared internally and externally through unencrypted channels (see  
83 Appendix A for additional information).
- 84 3. When sensitive data is shared, the recipient must be informed of its data  
85 classification and the need to maintain confidentiality and integrity of such data.
- 86 4. LSU Eunice must establish processes and procedures to include relevant information  
87 in contracts and agreements with third parties for data security when sensitive  
88 information will be involved.
- 89 5. If data is to be shared in a physical manner than appropriate measures must be  
90 taken to secure sensitive information including, but not limited to, certified tracking,  
91 signature confirmation services, use of tamper-evident sealed package, etc.
- 92 E. Data Disposal
- 93 1. LSU Eunice must establish processes and procedures for secure disposal of  
94 sensitive information.
- 95 2. Any asset containing sensitive information must not be repurposed (including  
96 surplus), and/or discarded, without following established processes and procedures  
97 for secure disposal.
- 98 3. All physical materials containing sensitive information must only be discarded using  
99 University provided shredders.

100

## APPENDIX A

101 Overview of methods for secure/insecure data transfers:

Approved Storage Locations	Approved Secure Sharing Methods	Insecure storage/sharing Methods
LSU Eunice Microsoft 365 environment	Encrypted Email	Regular email
OIT Datacenter	LSU Files-to-Geaux	Instant Messaging
For physical material: - Locked filing cabinet, desk, or locked rooms with limited access	Office365 services* (OneDrive, Teams [Internal])	Personal email
	Secure File Transfer Protocols, such as SFTP, HTTPS, FTPS, etc.	Computing devices – Personal or LSU Eunice owned (Laptops, Desktops, smartphones, tablets, etc.)
	OIT offered integration services	Unencrypted removable media**
		Personal Cloud storage services (Dropbox, Box, Google Drive, OneDrive)

102

103 \*Office365 services cannot be utilized to store health information, criminal justice information  
104 systems data, Payment Card Industry (PCI) data.

105 \*\*Removable media should only be utilized for data storage/sharing when other means are not  
106 available.

### 107 IV. REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	04/20/2022	Initial Draft	OIT

108