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 mustbe 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

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

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

III. STANDARDS

A. Data Management

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

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

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

B. Public Data

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

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

C. Private and Confidential Data

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

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

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

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

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

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

D. Data storage and sharing

1. Sensitive information must only be stored on authorized systems and applications, and electronic copies, including backups, must be kept at a minimum.

2. Sharing of sensitive information must be carried out using secure means including, but not limited to, secure file transfer, encrypted e-mails, etc. Sensitive information must not be shared internally and externally through unencrypted channels (see Appendix A for additional information).

3. When sensitive data is shared, the recipient must be informed of its data classification and the need to maintain confidentiality and integrity of such data.

4. LSU Eunice must establish processes and procedures to include relevant information in contracts and agreements with third parties for data security when sensitive information will be involved.

5. If data is to be shared in a physical manner than appropriate measures must be taken to secure sensitive information including, but not limited to, certified tracking, signature confirmation services, use of tamper-evident sealed package, etc.

E. Data Disposal

1. LSU Eunice must establish processes and procedures for secure disposal of sensitive information.

2. Any asset containing sensitive information must not be repurposed (including surplus), and/or discarded, without following established processes and procedures for secure disposal.

3. All physical materials containing sensitive information must only be discarded using University provided shredders.

APPENDIX A

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)

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

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

IV. REVISION HISTORY

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