POLICY STATEMENT 124 STANDARD 3
DATA STORAGE

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 stored in a manner that sustains its confidentiality, integrity, and availability.

The purpose of this standard is to describe security processes and procedures that should be followed for data storage 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.

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 Storage

1. LSU Eunice data must be stored in a manner that supports compliance with relevant regulations and/or contractual agreements and to maintain confidentiality, integrity, and availability of the data.

2. Sensitive information, i.e., private, and confidential data, must only be stored on authorized systems and applications, and electronic copies, including backups, must be kept at a minimum.

3. Any storage of sensitive information with a third party must require a contract which must include relevant information related to data security and privacy.

4. Any personal computing device (laptops, desktops, smartphones, tablets, etc.) that is utilized to access, store, and/or process sensitive information must utilize encryption-at-rest technology.

5. Any server/application/platform that is utilized to access, store, and/or process sensitive information must have appropriate encryption technology to encrypt sensitive information at-rest and in-motion (i.e., data transfer).

6. Access to sensitive information must be granted based on the defined Master Access Plan (MAP). Wherever possible, role-based access must be utilized to grant such access.

7. Storage of sensitive information on a user's personal asset is strictly prohibited.

8. Any unauthorized disclosure of and/or access to sensitive data must be reported immediately to LSU Eunice's Office of Information Technology as per defined Security Incident Response processes.

B. Backup and Recovery

1. LSU Eunice must establish processes and procedures to develop disaster recovery and business continuity plans (DR/BC plans) for all critical systems, applications, and platforms that handle, store, and/or process sensitive information.

2. All documented DR/BC plans must be tested at least annually. The testing must include validating restoration of identified system(s) and/or data from backups.

3. All critical systems and/or sensitive data must have appropriate backups, and the frequency of backups shall consider any regulatory, contractual, and/or business requirements.

4. All backups must be stored in a manner that complies with regulatory and compliance requirements.

IV. REVISION HISTORY

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