



POLICY STATEMENT 124 DATA MANAGEMENT

Monitoring Unit: Information Technology Services
Initially Issued: July 21, 2023

PURPOSE

As an institution of higher education, the Louisiana State University A&M Baton Rouge Campus (“University” or “LSUAM”) is charged with maintaining systems and data for administrative, academic, and research purposes. These assets are critical to the mission of the University, and datasets must be managed with a formalized Data Management policy.

The purpose of this policy is to define the required processes and activities to support the classification, management, and security of data that is owned and/or maintained by the University.

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 LSUAM’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 University 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.

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

POLICY STATEMENT

A. Data Classification

1. LSUAM must establish and maintain a Data Governance Framework through a subcommittee under the purview of LSUAM IT Governance. The responsibilities of the subcommittee must be defined by IT Governance.
2. Datasets under the purview of LSUAM must be assigned a classification level based on sensitivity of the incorporated data elements.

B. Data Handling

1. LSUAM must identify administrative, technical, and physical security controls that need to be applied to restrict access and safeguard data, based on data classification, to ensure its confidentiality, integrity, and availability.
2. LSUAM shall identify critical datasets and implement appropriate measures to recover data fully in an event of a technology failure.
3. LSUAM shall define processes and procedures for disposal of data, as per data classification.

C. Data Storage

1. Data must be stored in a manner that complies with relevant regulations, contractual agreements, and/or data classification to maintain its confidentiality, integrity, and availability.

D. Data Privacy

1. LSUAM must implement processes and/or procedures to support privacy of personal information which is collected, used, processed, and/or stored for business purposes.
2. LSUAM must implement processes and procedures to improve user awareness as it pertains to the privacy of their personal information.
3. LSUAM must implement processes and procedures to support compliance with privacy regulations at local, state, national, and/or international level.

STANDARDS

- A. [The data classification standards are outlined in Standard PS-124-ST-1.](#)
- B. [The data handling standards are outlined in Standard PS-124-ST-2.](#)
- C. [The data storage standards are outlined in Standard PS-124-ST-3.](#)
- D. [The data privacy standards are outlined in Standard PS-124-ST-4.](#)

EXCEPTIONS AND NON-COMPLIANCE

- Please refer PS-120-ST-4 for additional information related to exceptions.
- Please refer PS-120 for additional information related to Policies and Standards non-compliance.

REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	7/21/2023	Initial Draft	Information Technology Services