POLICY STATEMENT 126
ENCRYPTION

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. While data is a critical business asset to the University, the management of this data can present significant risk. Thus, it is essential that data is treated appropriately at all levels of Data Governance. Beyond traditional security controls such as authentication and authorization, encryption serves as additional mechanism for further improving data security.

The purpose of this policy is to outline requirements for the encryption of data at LSUAM.

DEFINITIONS

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.

Encryption – Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. The corresponding reversal process is called "decryption", which is transformation that restores encrypted data to its original state.

POLICY STATEMENT

A. Data Encryption
    1. Data classified as confidential and/or private data, as per the Data Classification (PS-124-ST-1) must be encrypted-at-rest (e.g., stored on storage media such as, USB drives, external and internal hard drives, SSD drives, etc.), where applicable, and in motion (e.g., data transfer between devices, over the internal or external network, etc.) in accordance with PS-126-ST-1 (Encryption Standards).
    2. Wherever encryption is used:
        a. Encryption of data should only be carried out using National Institute of Standards and Technology (NIST) approved and/or commercially supported encryption algorithms.
        b. Encryption keys must be generated, stored, accessed, distributed, and destroyed in a controlled and secured manner as defined in PS-126-ST-1.
        c. Encryption keys must be periodically changed as defined in PS-126-ST-1.

STANDARDS

A. The Encryption standards are outlined in Standard PS-126-ST-1.

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