# POLICY STATEMENT 126
# INFORMATION TECHNOLOGY DATA ENCRYPTION

**POLICY DIGEST**

**Monitoring Unit: Office of Information Technology**
**Initially Issued: January 6, 2023**
**Last Revised: January 6, 2023**

## 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, 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 an additional mechanism for further improving data security.

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

## II. DEFINITIONS

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

**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. If the transformation is reversible, the corresponding reversal process is called "decryption", which is transformation that restores encrypted data to its original state.

## III. POLICY STATEMENT

A. 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, where applicable, and in motion in accordance with Encryption Standards.

2. The use of proprietary data encryption methods, i.e., not commercially supported, must not be utilized.

3. Encryption keys must be generated, stored, accessed, distributed, and

destroyed in a controlled and secured manner as defined in Encryption Standards.

4. Encryption keys must be periodically change as defined in the Encryption Standards

## IV. STANDARDS

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

## V. REVISION HISTORY

| Version | Date | Change Description | Edited By |
|---|---|---|---|
| 0.1 | 07/18/2022 | Initial Draft | OIT |
| | | | |