



1
2
3
4

POLICY STATEMENT 126 INFORMATION TECHNOLOGY DATA ENCRYPTION

5
6

POLICY DIGEST

7
8
9
10
11
12

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

13

I. PURPOSE

14 As an institution of higher education, Louisiana State University at Eunice (“University” or “LSU
15 Eunice”) is charged with maintaining systems and data for administrative, academic, and
16 research purposes. While data is a critical business asset to the University, the management of
17 this data can present significant risk. Thus, it is essential that data is treated appropriately at all
18 levels of Data Governance. Beyond traditional security controls such as authentication and
19 authorization, encryption serves as an additional mechanism for further improving data security.

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

21

II. DEFINITIONS

22 **Data.** Any information residing on the University Information Technology Infrastructure or held
23 on any other IT Infrastructure on behalf of the University. This data includes files, documents,
24 messages in any format, including e-mail messages and posts made on any Social Media site
25 maintained by/for the University or its units. All data created and/or maintained by a User is also
26 subject to this Policy, even if the data is created and/or stored on the User’s own personal
27 computer, smartphone, or other personal device.

28 **Encryption.** Cryptographic transformation of data (called “plaintext”) into a form (called
29 “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If
30 the transformation is reversible, the corresponding reversal process is called “decryption”, which
31 is transformation that restores encrypted data to its original state.

32

III. POLICY STATEMENT

33

A. A. Data Encryption

- 34
35
36
37
38
39
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

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

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

44 **IV. STANDARDS**

45 A. The Encryption standards are outlined in [Standard LSU Eunice-ST-126-1](#).

46 **V. REVISION HISTORY**

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

47