



POLICY STATEMENT 126-ST-1 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 additional mechanism for further improving data security. Encryption is performed on data by means of algorithms and keys. While the algorithms are public and well known, the keys needed to encrypt/decrypt the data must be kept private and secret.

The purpose of this standard is to document practices and requirements for appropriate encryption management

II. DEFINITIONS

Asymmetric Encryption. A method of encryption that utilizes two different keys, public and private, for the purposes of encryption and decryption. The public key, as the name implies, is made publicly available and is used for encryption. The private key (which is uniquely associated with the public key) is known only to the party attempting to decrypt the message. Asymmetric encryption is also known as public-key cryptography.

Certificate Authority. Certificate Authority (CA) is an internal or third-party entity that creates, signs, and revokes digital certificates. Primarily, a CA certifies the ownership of public keys by binding them to identities.

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

Dual Control. The principle of dual control requires that separate tasks be completed simultaneously to achieve a larger goal.

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

46 **Key Custodian.** Individuals that manage activities associated with the lifecycle of encryption
47 keys.

48 **Key Managers.** Individuals that oversee key custodians and various key management
49 processes without participating in the activities themselves.

50 **Private Key.** Confidential half of the asymmetric key pair used in public-key cryptography. This
51 key should only be known to the recipient of the encrypted communication.

52 **Public Key.** Public half of the asymmetric key pair used in public-key cryptography. This key is
53 typically known to the senders of the encrypted communication.

54 **Secret Key.** Symmetric key used in symmetric encryption and is a secret shared between the
55 communicating parties. This key is not truly private.

56 **Split knowledge.** The principle of split knowledge aligns with segregation of duties where
57 individual tasks can be performed independently to achieve a larger goal.

58 **Symmetric Encryption.** A method of encryption where a single key is utilized by the sender and
59 recipient for the purpose of encryption and decryption.

60 **III. STANDARDS**

61 A. Encryption of data at rest

62 1. All user endpoints (laptops/desktops) must be encrypted using whole disk
63 encryption. Where applicable, centrally supported, and managed encryption services
64 must be utilized.

65 2. Any data classified as confidential and/or private shall be stored using encryption on
66 systems, databased, and/or portable media.

67 3. Encryption of confidential and/or private data in databases shall be encrypted using
68 either whole disk encryption or encrypting specific tables, columns, etc., using
69 encryption technologies within the database.

70 4. All backups containing confidential and/or private data must be encrypted.

71 5. Any system, application, and/or database that stores passwords/credentials, must
72 implement appropriate encryption methodologies as defined in this standard.

73 B. Encryption of data in motion

74 1. Any transmission of confidential and/or private data internally or externally must
75 occur via an encrypted method, e.g., encrypted email, encrypted file sharing
76 solutions, SFTP, FTPS, TLS, etc.)

- 77 2. Any implementation of secure network connection (e.g., point to point connectivity via
78 IPSec/VPN Tunnels) with third parties must leverage identified secure cryptographic
79 algorithms.
- 80 3. Confidential and/or private data must not be shared using Instant Messaging
81 applications, regular e-mail, or any other insecure method. Please reference PS-124-
82 ST-2 for approved methods for data sharing.
- 83 4. All web-based applications must utilize secure protocols, TLS 1.1 and above, for any
84 data transmission regardless of classification.
- 85 i. Display of confidential or private data must be based on user's authorization
86 and/or need-to-know principle.
- 87 ii. Where applicable confidential or private data must be masked.
- 88 5. Database and application servers must utilize encrypted transmission protocols for
89 data transmission between them.
- 90 6. Confidential or private data transmission between applications must use appropriate
91 encryption protocols (e.g., SOAP with HTTPS).
- 92 7. Any transmission of confidential or private data over wireless networks must utilize
93 encryption techniques such as LEAP, WPA2, IPSec VPN, TLS, etc.
- 94 C. Encryption methodologies
- 95 1. Any keys generated to support encryption effort must, at minimum, meet standards
96 set forth by FIPS 140-3.
- 97 2. The following symmetric algorithms shall be used, at minimum, for encryption
- 98 i. AES (256 bits)
- 99 ii. Twofish (256 bits)
- 100 iii. Serpent (256 bits)
- 101 3. The following algorithms shall be used, at minimum, for public key asymmetric
102 encryption
- 103 i. RSA (2048 bits)
- 104 ii. ECC (384 bits)
- 105 4. SHA-256 or better hashing algorithm must be utilized where a need exists to use a
106 hashing algorithm.
- 107 5. All SSL/TLS certificates must be acquired through LSU provided Certificate Authority
108 services.

109 D. Encryption Key management

- 110 1. LSU Eunice must implement an enterprise key management solution.
- 111 2. Each unit must identify Key Managers and Key Custodians and where applicable,
112 these duties must be segregated.
- 113 i. It is recommended that a primary and secondary Key Custodians be identified
114 and there must not be a reporting relationship between the primary and
115 secondary personnel.
- 116 3. All encryption keys are classified as confidential data, and must be encrypted while
117 being stored in a secure location.
- 118 4. All keys must be unique and single purpose use only, i.e., keys used for encrypting
119 keys cannot be used as data encrypting keys.
- 120 5. All key management activities must be logged and documented to ensure an
121 appropriate audit trail is maintained.
- 122 6. LSU Eunice and individual units must develop processes and procedures for key
123 lifecycle management (generation, storage and retrieval, transport, receipt, loading,
124 and erasure and destruction).
- 125 7. Keys must be generated using a method that is not easily reproduced.
- 126 8. Encryption keys must be separate for test, development, and production
127 environments.
- 128 9. Keys must be stored in the minimum number of locations required to satisfy business
129 continuity and disaster recovery requirements.
- 130 10. Any password, passphrases, and keys associated with encrypted data must be sent
131 separately from the encrypted information itself and must be transmitted using
132 secure methods only (TLS, IPSec, SFTP, etc.).
- 133 11. Where asymmetric encryption is utilized, the operational period of asymmetric keys
134 issued by a Certificate Authority must not exceed one year.
- 135 12. Where symmetric encryption is utilized:
- 136 i. Master keys are to be changed, at a minimum, annually.
- 137 ii. Key Exchange Keys shall be changed, at a minimum, twice a year.
- 138 iii. Data Encryption Keys shall be changed, at a minimum, once per session or
139 every 24 hours.
- 140 13. In an event where it is suspected that there was unauthorized access to or exposure
141 of encryption keys, keys must be revoked and replaced immediately.
- 142 14. Changes to employment of key custodians shall result in key revocation and
143 replacement.

144 15. If retired, expired, and/or replaced keys are retained, they must not be utilized for any
145 encryption purposes.

146 16. LSU Eunice must develop processes and procedures for key destruction.

147 **IV. REVISION HISTORY**

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

148