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.

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.

Key Custodian. Individuals that mange activities associated with the lifecycle of encryption keys.

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

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

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

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

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

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

III. STANDARDS

A. Encryption of data at rest

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

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

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

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

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

B. Encryption of data in motion

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

2. Any implementation of secure network connection (e.g., point to point connectivity via IPSec/VPN Tunnels) with third parties must leverage identified secure cryptographic algorithms.

3. Confidential and/or private data must not be shared using Instant Messaging applications, regular e-mail, or any other insecure method. Please reference PS-124-ST-2 for approved methods for data sharing.

4. All web-based applications must utilize secure protocols, TLS 1.1 and above, for any data transmission regardless of classification.

    i. Display of confidential or private data must be based on user's authorization and/or need-to-know principle.

    ii. Where applicable confidential or private data must be masked.

5. Database and application servers must utilize encrypted transmission protocols for data transmission between them.

6. Confidential or private data transmission between applications must use appropriate encryption protocols (e.g., SOAP with HTTPS).

7. Any transmission of confidential or private data over wireless networks must utilize encryption techniques such as LEAP, WPA2, IPSec VPN, TLS, etc.

C. Encryption methodologies

1. Any keys generated to support encryption effort must, at minimum, meet standards set forth by FIPS 140-3.

2. The following symmetric algorithms shall be used, at minimum, for encryption

    i. AES (256 bits)

    ii. Twofish (256 bits)

    iii. Serpent (256 bits)

3. The following algorithms shall be used, at minimum, for public key asymmetric encryption

    i. RSA (2048 bits)

    ii. ECC (384 bits)

4. SHA-256 or better hashing algorithm must be utilized where a need exists to use a hashing algorithm.

5. All SSL/TLS certificates must be acquired through LSU provided Certificate Authority services.

D. Encryption Key management

1. LSU Eunice must implement an enterprise key management solution.

2. Each unit must identify Key Managers and Key Custodians and where applicable, these duties must be segregated.

    i. It is recommended that a primary and secondary Key Custodians be identified and there must not be a reporting relationship between the primary and secondary personnel.

3. All encryption keys are classified as confidential data, and must be encrypted while being stored in a secure location.

4. All keys must be unique and single purpose use only, i.e., keys used for encrypting keys cannot be used as data encrypting keys.

5. All key management activities must be logged and documented to ensure an appropriate audit trail is maintained.

6. LSU Eunice and individual units must develop processes and procedures for key lifecycle management (generation, storage and retrieval, transport, receipt, loading, and erasure and destruction).

7. Keys must be generated using a method that is not easily reproduced.

8. Encryption keys must be separate for test, development, and production environments.

9. Keys must be stored in the minimum number of locations required to satisfy business continuity and disaster recovery requirements.

10. Any password, passphrases, and keys associated with encrypted data must be sent separately from the encrypted information itself and must be transmitted using secure methods only (TLS, IPSec, SFTP, etc.).

11. Where asymmetric encryption is utilized, the operational period of asymmetric keys issued by a Certificate Authority must not exceed one year.

12. Where symmetric encryption is utilized:

    i. Master keys are to be changed, at a minimum, annually.

    ii. Key Exchange Keys shall be changed, at a minimum, twice a year.

    iii. Data Encryption Keys shall be changed, at a minimum, once per session or every 24 hours.

13. In an event where it is suspected that there was unauthorized access to or exposure of encryption keys, keys must be revoked and replaced immediately.

14. Changes to employment of key custodians shall result in key revocation and replacement.

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

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

IV. REVISION HISTORY

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