6.10 - ENCRYPTION

Effective: October 15, 2025

Purpose: Emporia State University maintains information for business and academic use which at times might need to be transmitted. When transmitting sensitive or confidential information encryption techniques should be used to control access to the information, protect the integrity of transactions, and protect ESU's information assets.

Scope: This policy applies to all persons granted access to ESU's information systems when transmitting protected information to off-campus entities.

Responsible Office: Information Technology

Policy Statement: ESU users transmitting information classified as sensitive or confidential as defined in the policy on Information Classification will use encryption when transmitting to off-campus entities.

Encryption Types and Methods:
ESU shall utilize industry-standard encryption types, including symmetric (e.g., AES), asymmetric (e.g., RSA), and hash functions (e.g., SHA-256), as appropriate for the data and transmission method. Approved methods include VPN, SSL/TLS, PKI, and encryption software.

Key Management:
All encryption keys must be generated, stored, distributed, rotated, and revoked in accordance with ESU's key management procedures. Keys must be protected against unauthorized access, and key management activities must be logged and reviewed by the ISO.

Information Technology (IT) will be responsible for identifying appropriate encryption methodologies for transmission of information classified as sensitive or confidential. Encryption methodologies include, but are not limited to:

- Virtual Private Network (VPN);
- Secure Socket Layer (SSL);
- Public Key Infrastructure (PKI) (e.g., digital id's for secure email); and
- Encryption Software.

Units may be responsible for the licensing cost of third-party solutions as necessary. Users transmitting information classified as sensitive or confidential pursuant to the policy on Information Classification are responsible for contacting the Information Security Officer (ISO) regarding the type of encryption that should be used.

The ISO will be responsible to raise awareness about when encryption should be used to help educate the University community. Encryption resources will be available on the Information Technology website. The ISO is responsible for monitoring and reporting compliance with this policy. The ISO is responsible for reviewing this policy annually.

University users transmitting information classified as sensitive or confidential as defined in the policy on Information Classification will use encryption when transmitting to off-campus entities.

The President or designee must approve any exceptions to this policy.

Definitions: All words and phrases shall be interpreted utilizing their plain meanings unless otherwise defined in another University or Board of Regents policy or by statute or regulation.

Procedures: All procedures linked and related to the policies above shall have the full force and effect of policy if said procedures have first been properly approved by the University's administrator in charge of Information Technology.

[Hyperlink to Information Technology procedures]

Related Policy Information: [Include here any supporting information for this policy]

History: Adopted: 10/13/2009 [FSB 09006 passed by Faculty Senate on 10/06/2009, approved by President, and included in UPM as Policy 3J.12]
Revised: 10/02/2013 [Policy updated]
Revised: 04/26/2019 [FSB 18023 passed by Faculty Senate on 04/16/2019 and approved by President]
Revised: 08/15/2024 [Policy format revised as part of UPM Revision]
Revised: 10/20/2025 [Policy updated to include more details about encryption method]