6.33 Media Transport Policy

Effective: July 1, 2025

Purpose: This policy establishes requirements for the secure transport of physical and electronic media containing sensitive or confidential information to protect against unauthorized access, loss, or disclosure.

Scope: This policy applies to the University campus wide.

Responsible Office: Information Technology

Policy Statement: This policy applies to all Emporia State University employees, contractors, and third parties who handle or transport media containing sensitive data, including but not limited to:

- USB drives, CDs/DVDs, external hard drives
- Printed documents
- Backup tapes
- Laptops and mobile devices

Authorization

Only authorized personnel may transport sensitive media.
Authorization must be documented and approved by the appropriate department head or data owner.

Physical Transport

Media must be stored in locked containers or tamper-evident packaging.
Transport must be conducted directly and without unnecessary stops.
If using a courier or third-party service, the vendor must be contractually obligated to comply with data protection standards.

Electronic Transport

Electronic transmission of sensitive data must use encrypted channels (e.g., VPN, SFTP, encrypted email).
Portable devices must have full-disk encryption and strong authentication enabled.

Logging and Tracking

All media transports must be logged, including:
- Description of media
- Date and time of transport
- Origin and destination
- Name of person responsible
Logs must be retained for at least one year.

Incident Reporting

Any loss, theft, or unauthorized access to media must be reported immediately to the Information Security Officer (ISO). An incident response will be initiated in accordance with the university's Incident Response Policy.

Enforcement

Violations of this policy may result in disciplinary action, up to and including termination, and potential legal consequences.

Review and Updates

This policy will be reviewed annually by the ISO and updated as necessary to reflect changes in technology, regulations, or university operations.

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.

Sensitive Media: Any media containing confidential, restricted, or regulated data as defined in the Information Classification Policy.

Transport: The physical or electronic movement of media from one location to another, whether on or off campus

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 General University procedures.

[Hyperlink to Information Technology procedures]

Related Policy Information:

History: Adopted: