Effective: *08/08/2022*
Last Revised: *08/07/2023*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
IT Security Services
security@nebraska.edu

1. Purpose

4.2.3 Duplication
Non-public information must not be copied from secure locations to locations not managed with the same access controls and media protections.

4.3 Physical Media Protection and Control

4.3.1 Physical and Digital Media Storage
Physical (e.g. paper, microfilm hardcopies) and digital (videos, recordings, electronic documents) copies of medium and high-risk data should be stored in secure locations. Access to medium and high-risk data should be limited to only personnel that requires access for legitimate business purposes.

4.3.2 Removable Media Usage
Sensitive information should be stored on removable media only when required in the performance of assigned duties or when providing information required by other state or federal agencies. When sensitive information with data classification of Level 4 (High) or Level 5 (Research) is stored on removable media, it must be encrypted in a format that is consistent with NIST SP 800-175B Revision 1 FIPS 180, 198, and 202.

Additionally, unauthorized usage of portable storage devices or public cloud storage services is prohibited. In efforts to reduce risk of inappropriate usage, identifiable owners (e.g., individuals, organizations, or projects) should be assigned to the device or logged via a device request process, as appropriate.

4.3.3 Media Encryption
All Information Systems that access, process, transmit, or store Medium or High Risk Data as defined in **Executive Memorandum 42** must have disk(s) encryption enabled on the OS disk and any connected disks which contain data which is classified at the equivalent risk. Hard Disk Drives (HDDs), Solid State Drives (SSDs), and other internal (PCI bus storage) or external (USB, etc) connected storage media are within scope of this standard. The following table displays examples and is not limited to approved OS encryption technologies in alignment with NIST SP 800-175B Revision 1, FIPS 180, 198, and 202.

Device Encryption Examples	
Windows	BitLocker (Minimum AES-128)
Apple / Mac	FileVault (Minimum AES-128)
Linux	Linux Unified Key Setup (LUKS) (Minimum AES-128)

4.4 Clear Desk

4.4.1 Unattended Devices
Whenever unattended or not in use, all Information Systems must be left logged off or protected with a screen and keyboard locking mechanism controlled by a password or similar user authentication mechanism.

4.4.2 Clear Screen
When viewing sensitive information on a screen, users should be aware of their surroundings and should ensure that third parties are not permitted to view the sensitive information.

4.4.3 Clear Desk
Sensitive information, e.g., on paper or on electronic storage media, when not in use, must be secured within a segregated, controlled room limited to only authorized personnel, or using lockable furniture. Access to medium and high-risk data should be limited to only personnel that requires access for legitimate business purposes.

4.4.4 Printing and Faxing
Paper containing sensitive or classified information must be removed from printers and faxes immediately. Faxes and printers used to print sensitive information should not be in public areas. Any time a document containing sensitive information is being printed the user must make sure they know the proper printer is chosen and go directly to the printer to retrieve the document.

4.5 Electronic Media Protection and Control

4.5.1 Electronic Media Storage

Standard electronic information repositories must be established within the internal network and authorized privately hosted networks, and formally assigned ownership. Standard electronic information repositories must enforce strong access control and encryption at rest based on their classification, in alignment NIST SP 800-175B Revision 1, FIPS 180, 198, and 202**.**

4.5.2 Internet Access of Sensitive Information

Electronic information with classifications of medium and high risk must not be publicly accessible via the internet without appropriate access controls, or by individuals who are not authorized University personnel, contractors, or third parties.

4.6 Media Sanitization

4.6.1 IT Storage Disposal and Re-use

Prior to media disposal, the media device must be shredded or destroyed to ensure the device is unable to be read or utilized in accordance with the **Digital Media Sanitization Procedure**. Prior to media reuse, a data sanitization must occur.

4.6.2 Physical Record Disposal

All physical records containing medium risk and high-risk information must be disposed of using secure shredding methods and lock bins.

4.7 Media Transport

4.7.1 Controlled Media Areas and Transport Restrictions

Controlled areas are defined by the organization that denotes sufficient physical or procedural safeguards in place to protect system and information.

To maintain media accountability during transport outside of controlled areas, transportation activities of media containing high risk data must be restricted to authorized personnel and available safeguards should be leveraged (e.g. locked containers and cryptography). Tracking and logging of media transport activities should be retained to prevent and detect any loss, tampering, or destruction of media.

5. Procedures

Procedures specific to this Standard are to be documented and maintained by the individual service owners throughout the University system.