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

ITS-09: Media Protection Standard

Standard Contents

1. Purpose

The purpose of the Media Protection Standard is to define the organization’s requirements for the implementation and on-going management of media protection standards and corresponding media protection controls. Media refers to organizational data and systems that store, transmit or process that data. The standard outlines the methods and requirements that ensure media protection during the storage, transportation, and sanitization of Information Systems.

2. Scope

This Standard shall apply to all The University of Nebraska (“The University”) technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of The University and to which this policy applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this Standard.

3. Standard Statement

It is the intention of this Standard to establish media protection capabilities through The University to implement best practices pertaining to the protection of media. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer (“CISO”) as defined in **ITS Policy Exception Standard**. The following subsections outline the Media Protection Standard.

4. Media Protection Requirements

4.1 Information Asset Ownership

4.1.1 Information Asset Ownership
Ownership of information assets must be formally established. Research and institutional data stewards of information assets must be assigned clearly defined responsibilities to ensure the protection of confidentiality, integrity, and availability of the asset appropriate to business context. Data stewards are responsible for the initial classification of data and affiliated information systems.

4.1.2 Sensitive Data Marking
All physical and electronic media must be properly marked to alert individuals to the presence of sensitive data stored on the media. Media must be classified in alignment with **Executive Memorandum 42.** Where collections of media intermix items with various classifications, the collection must be marked with the highest-level of sensitivity included within the collection.

Should any specific department, division, or project specific media classifications be required, these anomalies must be consistent with **Executive Memorandum 42.**

4.2 Due Care in Handling Sensitive Information

4.2.1 Individual Due Care
Personnel must take all reasonable and appropriate measures to prevent medium and high-risk information from being lost, stolen, intercepted, or shared by/with unauthorized individuals. Medium and high-risk information may be shared only with:

- Other University employees with authorization to access the information
- Third party vendors approved through University procurement in alignment with services provided, with appropriate contractual provisions in place
- Legally authorized individuals, such as in response to a subpoena or to other entities as required by law

4.2.2 Information Disclosure
All disclosure of medium and high-risk information to external parties must be performed via approved disclosure procedures and with the approval of the information asset owner or data steward.

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.

6. Compliance

Compliance Measurement
The University of Nebraska IT Security Services team will verify compliance to this Standard through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Standard owner.

Exceptions
Any exception to the Standard must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the Standard exception is required
- Any risks created by the Standard exception
- Risk mitigation plan and duration of the exception
- Evidence of approval following established Exception Standard

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	08/07/2023
Approved by:	Bret Blackman	IT CIO	08/07/2023

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published
1.1	07/31/2023	Updated Scope and Definitions in Sections 4.3.3 and 4.4.1