**Media Protection (MP) Standard**

Figure 1- Indiana University Seal—only approved university-wide policies may use the seal

# IT-12

**About This Standard**

**Effective Date:**

*In review*

**Date of Last Review/Update:**

*4/7/2023 revision*

**Responsible University Office:**

*University Information Policy Office*

**Responsible University Administrator:**

***Office of the Vice President for Information Technology and Chief Information Officer***

**Policy Contact:**

***University Information Security Office -*** [*uiso@iu.edu*](mailto:uiso@iu.edu)

## Scope

This standard supports [Policy IT-12 (Security of Information Technology Resources)](https://policies.iu.edu/policies/it-12-security-it-resources/index.html) and applies to all Indiana University information technology resources, regardless of whether those resources are managed by the university or provisioned from third parties on behalf of the university, and to all users of those resources regardless of affiliation.

## Objectives

The key objectives of this standard are to ensure:

* Information systems media, both paper and digital, are protected appropriately;
* Access to data on information systems media is limited to authorized users; and
* Information systems media are sanitized or destroyed before disposal or release for reuse.

## Standard

The following tables detail baseline security controls for media protection that are to be applied to a particular information technology resource based on its [security categorization](https://informationsecurity.iu.edu/policies/standards/it12-security-categorization-procedure.docx). Select controls as applicable. For example, all controls may not apply to every system component or technology, or to situations governed by specific regulations.

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Restricted Access to Media** | | |
| **Required for:** | **High** | **Moderate** |  |
| **IU Implementation** | Restrict access to media storing digital information to individuals with a need to access that media. | | |
| **Notes** | * Restricting access to digital media might be accomplished with the use of access control lists, pass codes, and firewalls. Restricting access to physical media might be accomplished with locked file cabinets. * Use of centrally provisioned, common IT infrastructure and services provided by UITS often fulfills many of these requirements. Check with the service owner for details. * See also [Policy DM-01 (Management of Institutional Data](https://policies.iu.edu/policies/dm-01-management-institutional-data/index.html)). | | |
| **NIST Cross Reference** | MP-2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Media Storage** | | |
| **Required for:** | **High** |  |  |
| **IU Implementation** | Securely store digital media. | | |
| **Notes** | * Secure storage of media might be accomplished by keeping media in a locked data center, file cabinet, desk drawer, or safe. * See System and Communications Protection Standard, control SC-28 for encryption of data on media. * Use of centrally provisioned, common IT infrastructure and services provided by UITS often fulfills many of these requirements. Check with the service owner for details. | | |
| **NIST Cross Reference** | MP-4 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Media Sanitization** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Sanitize all media prior to disposal, sale, or reassignment. | | |
| **Notes** | * **Important**: Media sanitization applies to all digital and nondigital system media subject to disposal or reuse, regardless of whether the media is considered removable. * Examples include digital media in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. * Consider not only hard drives, removable drives, and backup tapes, but also media found in scanners, copiers, printers, tablets, and phones. * Sanitization of digital might be accomplished through DoD wipes of magnetic media, cryptographic deletion of solid-state media, or physical shredding of any media (including paper or digital storage devices). * Verify and document sanitization prior to disposal. * If sanitization cannot be accomplished at the unit level, the unit will contract with IU Surplus or an approved vendor to ensure compliance. * Use of centrally provisioned, common IT infrastructure and services provided by UITS often fulfills many of these requirements. Check with the service owner for details.   See also:   * [Policy FIN-PURCH-11 (Disposal and Redistribution of University Property)](https://policies.iu.edu/policies/fin-purch-11-disposal-and-redistribution-university-property/index.html) * [About secure data removal](https://kb.iu.edu/d/bgug) * [NIST Guidelines for Media Sanitization](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf) | | |
| **NIST Cross Reference** | MP-6 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Media Use** | | |
| **Required for:** | **High** |  |  |
| **IU Implementation** | * Critical or Restricted data must never be stored on individual user workstations or mobile devices (i.e., laptops, smart phones, tablets, personal digital assistants, thumb drives, removable media, etc.). * Exceptions require prior written approval and appropriate technical safeguards (see Policy IT-12, Standard IT-12.1, and this document). Formal approval must come from the senior executive officer of the unit and confirm a critical business need. If prior formal written approval has been obtained, any Critical data stored on such individual devices and media must be encrypted. | | |
| **Notes** | See also paragraph 9e of [DM-01-S (Standard for the Management of Institutional Data](https://policies.iu.edu/policies/dm-01-management-institutional-data/dm-01-s-updated.docx)).  Use of centrally provisioned, common IT infrastructure and services provided by UITS often fulfills many of these requirements. Check with the service owner for details. | | |
| **NIST Cross Reference** | MP-7 | | |

## Definitions

**Media** -Media refers to devices onto which digital information is recorded or stored. Digital media includes but is not limited to flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs.

**Standard** - Standards (like procedures) support policy by further describing specific implementation details (i.e., the "how"). A standard can be thought of as an extension of policy that articulates the rules, mechanisms, technical or procedural requirements, or specifications to be used in carrying out/complying with policy. Standards, along with procedures, promote a consistent approach to following policy. Standards make policies more practically meaningful and effective. Standards are definitional and clarifying in nature, specifying the minimums necessary to meet policy objectives. Because standards directly support policies, compliance with standards is nonoptional and failure to follow standards may result in sanctions imposed by the appropriate university office.

## Sanctions

Indiana University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities. Depending on the individual and circumstances involved, this could include the Office of Human Resources, Vice Provost or Vice Chancellor of Faculties (or campus equivalent), Dean of Students (or campus equivalent), Office of the Vice President and General Counsel, and/or appropriate law enforcement agencies. See [Policy IT-02 (Misuse and Abuse of Information Technology Resources)](http://policies.iu.edu/policies/categories/information-it/it/IT-02.shtml) for more details.

Failure to comply with Indiana University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

## Additional Contacts

|  |  |  |  |
| --- | --- | --- | --- |
| ***Subject*** | **Contact** | **Phone** | **Email** |
| Questions about the standard | University Information Security Office | 812-855-UISO (8476) | [uiso@iu.edu](mailto:uiso@iu.edu) |

## History

April 7, 2023 revised after stakeholder feedback

February 12, 2022 draft for review