**Maintenance (MA) Standard**

Figure - 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:**

*4/7/23 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*

## 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:

* Periodic and timely maintenance of organizational information technology resources is performed; and
* Effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance are provided.

## Standard

The following tables detail baseline security controls for maintenance 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:**   | **System Maintenance Procedures** |
| **Required for:** | **High**   | **Moderate**  | **Low**   |
| **IU Implementation**   | * Maintenance procedures for hardware and software must be developed and documented for information technology resources to ensure maintenance is performed regularly by designated individuals.
* Maintenance procedures must include the “Controlled and Timely Maintenance” control and the “Maintenance Personnel” control referenced in the IT-12 Maintenance Standard.
* Units must review and update system maintenance procedures annually, concurrent with disaster recovery plans.
 |
| **Notes**   | See also control SI-2, Flaw Remediation, in the IT-12 System and Information Integrity Standard.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**   | MA-1 |

|  |  |
| --- | --- |
| **Control:**   | **Controlled and Timely Maintenance** |
| **Required for:** | **High**   | **Moderate**  | **Low**   |
| **IU Implementation**   | * Units must perform regular system maintenance of information technology resources and maintain maintenance logs.
* Perform maintenance on a timescale commensurate with risk.
* When appropriate, units should present proposed maintenance to the UITS internal change management group, noting changes to security posture.
* If maintenance involves removal of hardware from university facilities, securely wipe equipment to remove university data prior to removal.
 |
| **Notes**   | 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 (some links may require authentication):* [UITS Change Management site](https://change.uits.iu.edu/)
* [About the Limited Change Period](https://kb.iu.edu/d/audt)
* [UITS Change Management process](https://kb.iu.edu/d/bfaq)
* [Securely wipe disk drives](https://kb.iu.edu/d/auhn)
* Control MP-6 of the IT-12 [Media Protection Standard](https://informationsecurity.iu.edu/policies/standards/it-12-mp.docx)
 |
| **NIST Cross Reference**   | MA-2 and MA-6 |

|  |  |
| --- | --- |
| **Control:**   | **Maintenance Personnel** |
| **Required for:** | **High**   | **Moderate**  | **Low**   |
| **IU Implementation**   | * Document the individuals authorized to perform hardware or software maintenance.
* Assign and document the university personnel designated to supervise required maintenance activities performed by individuals not previously identified as authorized maintenance personnel, such as third-party vendors or consultants.
 |
| **Notes**   | For third parties, documenting third-party contact information satisfies this requirement. |
| **NIST Cross Reference**   | MA-5 |

## Definitions

**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  |

## History

April 7, 2023 revised after stakeholder feedback

February 12, 2022 draft for review