**Configuration Management (CM) 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:**

*4/7/23 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 that:

* Baseline configurations and inventories of organizational IT resources are established and maintained throughout the respective system development life cycles; and
* Security configuration settings for information technology resources employed in organizational information systems are established and enforced.

## Standard

The following tables detail baseline security controls for configuration management 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:** | **Baseline Configurations** |
| **Required for:** | **High**   | **Moderate**  |  |
| **IU Implementation**   | Develop, document, and maintain a standard system build, known as a baseline configuration.Review and update the baseline configuration at least annually and when: * Updates/patches affecting the baseline are released (for example, critical operating system or application updates/patches or updated versions), and
* System components are installed or upgraded.
 |
| **Notes**   | * The baseline configuration serves as the basis for future system builds.
* Baseline configurations must be maintained so organizational changes and configurations are captured.
* Baseline configurations for development and test environments must be maintained and managed separately from production baseline configurations.
* 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.
* To identify an update, as a general rule, look for an increase in the number to the left of the decimal place, such as 12.6 to 13.1.
 |
| **NIST Cross Reference**   | CM-2 |

|  |  |
| --- | --- |
| **Control:** | **Impact Analysis** |
| **Required for:** | **High**   | **Moderate**  |  |
| **IU Implementation**   | Prior to change implementation, analyze proposed changes to information technology resources to determine potential impacts. |
| **Notes**   | Changes to IT resources must be implemented in a test environment before implementation in the production environment. This allows units to look for security and operational impacts due to flaws, weaknesses, incompatibility, or intentional malice.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**   | CM-4 |

|  |  |
| --- | --- |
| **Control:** | **Least Functionality** |
| **Required for:** | **High**   | **Moderate**  |  |
| **IU Implementation**   | Configure systems for only the specific intended function. |
| **Notes**   | Only install necessary software and services.* Only install the necessary services.
* Configure only the necessary ports and protocols.
* Ensure that unnecessary ports and protocols are disabled.
* For example, do not run a web server on a machine that is not intended to be a web server or where a web server is not required to operate the system.

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**   | CM-7 |

|  |  |
| --- | --- |
| **Control:** | **System Inventory** |
| **Required for:** | **High**   | **Moderate**  |  |
| **IU Implementation**   | Maintain an inventory of systems.  |
| **Notes**   | Inventories should accurately reflect the systems, including all identifiable IT asset components, such as hardware, software, and firmware.For example, inventories may include system name, system owners, software version numbers, hardware specifications, software license information, security categorization, and network components.Inventories may also include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location.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**   | CM-8 |

## 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