**System and Information Integrity (SI) 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 draft*

**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 the confidentiality, integrity, and availability of institutional systems and information by:

* Ensuring that software code is validated and safe for use;
* Monitoring software and systems for malicious behavior and attacks;
* Protecting systems from abuse by invalid input; and
* Ensuring that data is removed and destroyed within proper time frames.

## Standard

The following tables detail baseline security controls for system and information integrity 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:** | **Flaw Remediation** |
| **Required for:** | **High**   | **Moderate**  |  |
| **IU Implementation**   | * Acquire all software code, updates, and patches from verified vendors.
* Test all code, updates, and patches before installation.
* Install security-relevant software and firmware updates within one month of the release of the update or sooner. Patches and updates for active exploits must be applied within five business days.
* Remove or disable code no longer being used immediately after updates or patching.
 |
| **Notes**   | * Where available, code and patch hashes should be checked before being applied.
* 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**   | SI-2 |

|  |  |
| --- | --- |
| **Control:** | **Malicious Code Protection** |
| **Required for:** | **High**   | **Moderate**  |  |
| **IU Implementation**   | * Install or enable antivirus/antimalware protection for all systems where it is available.
* Periodically scan information systems and assets for malicious code.
 |
| **Notes**   | * Malicious code includes, for example, viruses, worms, Trojan horses, and spyware.
* Malicious code protection mechanisms include, for example, antivirus signature definitions and reputation-based technologies.
* Heuristic-based antivirus/antimalware that consistently monitors behavior would also comply with this requirement in lieu of scheduled scans.
* 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**   | SI-3 |

|  |  |
| --- | --- |
| **Control:** | **System Monitoring** |
| **Required for:** | **High**   | **Moderate**  |  |
| **IU Implementation**   | Monitor IT resources to detect attacks and indicators of potential attacks. |
| **Notes**   | * See also the IT-12 Audit and Accountability (AU) Standard.
* Potential monitoring tools include log analysis, vulnerability scanning, etc.
* 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**   | SI-4 |

|  |  |
| --- | --- |
| **Control:** | **Security Alerts, Advisories, and Directives** |
| **Required for:** | **High**   | **Moderate**  | **Low**   |
| **IU Implementation**   | Subscribe to relevant internal and external information sources and prioritize action plans based on risk.  |
| **Notes**   | * [UISO Security Bulletins](https://informationsecurity.iu.edu/security-bulletins/index.html)
* See [Information Sources recommended for IT Pros at IU](https://kb.iu.edu/d/bczr).
 |
| **NIST Cross Reference**   | SI-5 |

|  |  |
| --- | --- |
| **Control:** | **Information Input Validation** |
| **Required for:** | **High**   | **Moderate**  | **Low**   |
| **IU Implementation**   | Applications must validate data input. Developers must write and/or implement code that that verifies the validity of data submitted to applications. Verification should consider:* Data type
* Data length or size
* Prohibited input, e.g., SQL syntax or commands

For example, numeric value fields must only contain numerals and must be trimmed to an appropriate length. |
| **Notes**   | For further guidance, see the [Open Web Application Security Project](https://owasp.org/) (OWASP) [testing guide](https://github.com/OWASP/wstg/tree/master/document/4-Web_Application_Security_Testing) and [Input Validation Cheat Sheet](https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html).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**   | SI-10 |

|  |  |
| --- | --- |
| **Control:** | **Error Handling** |
| **Required for:** | **High**   | **Moderate**  | **Low**   |
| **IU Implementation**   | Application error messages must provide only the information necessary to enable corrective actions without revealing information that is Critical or Restricted, or that could be exploited. |
| **Notes**   | For further guidance, see: * [Open Web Application Security Project](https://owasp.org/) (OWASP) [testing guide](https://github.com/OWASP/wstg/tree/master/document/4-Web_Application_Security_Testing) and [error handling principles](https://github.com/OWASP/wstg/blob/master/document/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/README.md)
* [Handling application and scripting errors for IU websites](https://kb.iu.edu/d/auey)
* [Form validation and error handling](https://kb.iu.edu/d/axfs)

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**   | SI-11 |

|  |  |
| --- | --- |
| **Control:** | **Information Management and Retention** |
| **Required for:** | **High**   | **Moderate**  | **Low**   |
| **IU Implementation**   | Data must be retained and destroyed in accordance with associated legal requirements, regulations, and IU policy. |
| **Notes**   | For further guidance, see:* [Policy UA-18 (University Records Retention and Disposition)](https://policies.iu.edu/policies/ua-18-university-records-retention-disposition/index.html)
* “Records Retention Schedule” applet at [one.iu.edu](https://one.iu.edu/)
* [About secure data removal](https://kb.iu.edu/d/bgug)
* [Critical Data Guide](https://datamanagement.iu.edu/docs/critical-data-guide.pdf)

If further guidance is needed, consult the University Information Policy Office, the relevant Data Steward, and/or the Office of the Vice President and General Counsel. |
| **NIST Cross Reference**   | SI-12 |

## 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