**System and Services Acquisition (SA) 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*](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 objective of this standard is to ensure IT systems and services are acquired in a manner that balances their importance to IU’s mission with IU’s dedication to data security. It outlines:

* Who is responsible for managing this policy;
* Documentation requirements;
* Requirements for engaging external entities; and
* Requirements associated with systems and components which are no longer supported.

## Standard

The following tables detail baseline security controls for system and services acquisitionthat 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 Documentation** | | |
| **Required for:** | **High** |  |  |
| **IU Implementation** | The following system documentation is required:   1. System security plan: For systems and servers, document the security categorization and IT-12 implemented safeguards in a system security plan (SSP). Include data-flow diagrams for systems that process institutional data classified as Critical. 2. Documentation for administrators: Obtain from the vendor, or develop and maintain, administrator documentation for information technology resources that addresses:    1. Effective use and maintenance of security and privacy functions and mechanisms; and    2. Known vulnerabilities regarding configuration. 3. Documentation for users: Obtain from the vendor, or develop and maintain, user documentation for information technology resources that addresses:    1. Effective use of any user-accessible security and privacy functions and mechanisms; and    2. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals.   Failure to obtain: Units should report failed attempts to obtain documentation per [Policy ISPP-26 (Information and Information System Incident Reporting, Management, and Breach Notification)](https://policies.iu.edu/policies/ispp-26-information-system-incident-reporting/index.html).  Documentation should be made available to individuals with a legitimate need. | | |
| **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. | | |
| **NIST Cross Reference** | SA-5 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **External System Services** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Prior to engaging external entities for information technology resources including systems, services, or software:   1. Consult with IT Community Partnerships (ITCP) via the [Software and Services Selection Process (SSSP)](https://kb.iu.edu/d/aoyl). 2. Require that providers of external systems or services comply with applicable university security and privacy requirements and employ legally required controls. 3. Work with the Office of Procurement Services to implement IU’s standard data security terms and any additional conditions required by the Data Stewards to protect IU institutional data and IT resources. | | |
| **Notes** | See also:   * [Policy DM-02 (Disclosing Institutional Information to Third Parties)](https://policies.iu.edu/policies/dm-02-disclosing-institutional-information/index.html) * [Protect data shared with cloud services and other third parties](https://informationsecurity.iu.edu/protect-data/sharing-data.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** | SA-9 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Unsupported System Components** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Replace system components (including applications and operating systems) when support for the components is no longer available.  Alternatives can include:   * Arranging for in-house support for developing customized patches for critical software components; or * Contractually obtaining ongoing support for the unsupported components; or * Implementing compensating controls that address the risk of operating unsupported components. | | |
| **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.  Applications for grants should consider the long-term cost of replacing system components for which support may cease prior to the completion of the project/study. | | |
| **NIST Cross Reference** | SA-22 | | |

## 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](mailto:uiso@iu.edu) |

## History

April 7, 2023 revised after stakeholder feedback

February 12, 2022 draft for review