**Planning (PL) 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 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 that:

* Security plans that describe the security controls in place or planned for organizational information systems are developed, documented, and periodically updated; and
* Rules of behavior for individuals accessing the information systems are communicated.

## Standard

The following tables detail baseline security controls for planning 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 Security Plan** |
| **Required for:** | **High**   |  |  |
| **IU Implementation**   | * Document controls in a system security plan (SSP) to demonstrate compliance with [Policy IT-12](https://policies.iu.edu/policies/it-12-security-it-resources/index.html) safeguards.
* Ensure the plan is approved by both the technology professional managing the resource and the executive of the department that owns the resource.
* Annually review, maintain, and implement the plan.
* Protect the plan from unauthorized distribution or use.
 |
| **Notes**   | [Link to SSP template to be added]  |
| **NIST Cross Reference**   | PL-2 |

|  |  |
| --- | --- |
| **Control:** | **Rules of Behavior** |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | * All users must assent to the IU Acceptable Use Agreement during initial account creation and re-assent every two years thereafter for continued access.
* Users may be required to assent to additional rules of behavior in accordance with legal and regulatory requirements that apply to information technology resources.
 |
| **Notes** | See also:* [Acceptable Use Agreement](https://informationsecurity.iu.edu/policies/acceptable-use.html)
* [Verify Acceptable Use Agreement](https://one.iu.edu/launch-task/iu/verify-acceptable-use-agreement?terms=acceptable%20use%20agreement)
 |
| **NIST Cross Reference** | PL-4 |

## 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

## Related Information

* [Acceptable Use Agreement](https://informationsecurity.iu.edu/policies/acceptable-use.html)
* [Verify Acceptable Use Agreement](https://one.iu.edu/launch-task/iu/verify-acceptable-use-agreement?terms=acceptable%20use%20agreement)