**Personnel Security (PS) 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 objectives of this standard are to ensure that:

* Individuals occupying positions of responsibility within the university (including third-party service providers) are trustworthy and meet established security criteria for those positions;
* Organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and
* Formal sanctions are employed for personnel failing to comply with organizational security policies and procedures.

## Standard

The following tables detail baseline security controls for personnel security 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:** | **Personnel Screening** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Follow appropriate screening procedures for employees and part time employees (as set forth by the appropriate offices) prior to granting them access to information or information technology resources.  All units must follow personnel security practices as listed in:   * Policy HR-02-10 (Background Checks) * [Policy PS-01 (Programs Involving Children](https://policies.iu.edu/policies/ps-01-programs-involving-children/index.html)) (if applicable) | | |
| **Notes** | **For affiliate users:** “Sponsors should weigh the risks of an affiliated user causing harm through inappropriate use of IU information technology resources against the benefits of the user having access. Sponsors are responsible for taking steps to reduce the likelihood of inappropriate use (including appropriate user training). Additionally, prior to requesting the account, the sponsor and the person being sponsored should have a written agreement defining the terms of the affiliation relationship. Any written agreement must comply with university policy [FIN-TRE-VI-100, Signature Authority and Delegation](https://policies.iu.edu/policies/fin-tre-100-signature-authority-delegation/index.html). Sponsors should consult with their department or unit on how best to document the user's affiliation with and responsibilities to both IU and the sponsor's department or unit.” ([Policy IT-03 (Eligibility to Use IT Resources](https://policies.iu.edu/policies/it-03-eligibility-use-it-resources/index.html))) | | |
| **NIST Cross Reference** | PS-3 Personnel Screening | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Personnel Termination** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | * When an employee is terminated, their credentials and authenticators must be revoked within a timeframe appropriate to the risks involved. * If an employee is terminated for cause, an accelerated timeline for revoking access must be considered to reduce risk. * Terminated employee access/authorizations to information technology resources must be removed. * Units must retrieve all security-related organizational information or system-related property from terminated employees and inform the appropriate personnel of these changes. | | |
| **Notes** | When an employee is terminated, the employee’s designated [IT Professional](https://itpeople.iu.edu/) or [Fiscal Officer](https://research.iu.edu/fiscal-officer-lookup/index.html) must follow any unit exit procedures, which could include such steps as:   1. [Reviewing Active Directory group memberships](http://tools.cci.iu.edu) and making necessary changes. 2. Reviewing access to institutional systems and making changes as appropriate. 3. Updating device registrations assigned to the individual (see [MAS Tools](https://mas.iu.edu/mas), [Windows Device Management](https://ls.iu.edu/WDM/Overview), [Apple Device Management](https://ls.iu.edu/MAC/Overview)). 4. Wiping old devices assigned to the individual (see [Data Removal](https://informationsecurity.iu.edu/personal-preparedness/data-removal.html), [Erasing Solid State Drives](https://informationsecurity.iu.edu/personal-preparedness/hardware-software/solid-state-drive.html), [Securely wipe disk drives](https://kb.iu.edu/d/auhn), [Remove institutional data from your mobile device](https://kb.iu.edu/d/azev) if no longer using it). 5. Reassigning [group accounts](https://one.iu.edu/task/iu/group-accounts) and [affiliate sponsorships](https://one.iu.edu/collection/iu/access-management). 6. Updating recurring meetings scheduled by the individual. 7. Reviewing folders, files, and resources such as online forms and workflows owned by the user in institutional storage locations and transitioning to new ownership as needed. 8. Collecting university-owned hardware. 9. Asking the departing employee to back up all personal data they want to retain from sources such as departmental storage drives, cloud storage, Canvas, and [email](https://kb.iu.edu/d/barg) prior to account expiration. | | |
| **NIST Cross Reference** | PS-4 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Personnel Transfer** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | When an employee is transferred, the employee’s former unit must review that employee’s access to information systems and remove, add, or modify access as appropriate. | | |
| **Notes** | It is recommended that the employee’s former unit coordinate with the new unit during this process. | | |
| **NIST Cross Reference** | PS-5 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Access Agreements** | | |
| **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 agreements to meet legal and regulatory requirements that may apply to specific information technology resources. | | |
| **Notes** | The Acceptable Use Agreement requirement is met automatically for centrally provisioned accounts.  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) * Control PL-4 in the [Planning Standard](https://informationsecurity.iu.edu/policies/standards/it-12-pl.docx) | | |
| **NIST Cross Reference** | PS-6 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Personnel Sanctions** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Users who violate university information technology policies associated with the use of IT resources at Indiana University may be subject to formal sanctions. | | |
| **Notes** | Users of IT resources at Indiana University are subject to sanctions as listed in the “Sanctions” section of the respective policies and as described in [Policy IT-02 (Misuse and Abuse of Information Technology](https://policies.iu.edu/policies/it-02-misuse-abuse-it-resources/index.html)) when they have violated existing laws or university procedures, including but not limited to:   * [University Information Technology Policies](https://policies.iu.edu/information-it/index.html); * [Code of Student Rights, Responsibilities, and Conduct](https://studentcode.iu.edu/); * [Academic, Faculty, and Student policies](https://policies.iu.edu/academic/index.html); * [University Human Resources Policies](https://policies.iu.edu/human-resources/index.html); and * [University Financial Policies](https://policies.iu.edu/financial/index.html).   Users of IT resources who have otherwise violated generally accepted [ethical norms and principles](https://principles.iu.edu/) may also be subject to such sanctions. | | |
| **NIST Cross Reference** | PS-8 Personnel Sanctions | | |

## 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

## Related Information

* [Policy HR-02-10 (Background Checks](https://policies.iu.edu/policies/hr-02-10-background-checks/index.html))
* [Policy PS-01 (Programs Involving Children](https://policies.iu.edu/policies/ps-01-programs-involving-children/index.html))
* [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))
* [Policy IT-01 (Appropriate Use of Information Technology Resources](https://policies.iu.edu/policies/it-01-appropriate-use-it-resources/index.html))
* [Policy IT-02 (Misuse and Abuse of Information Technology Resources](http://policies.iu.edu/policies/categories/information-it/it/IT-02.shtml))
* [Policy IT-03 (Eligibility to Use IT Resources](https://policies.iu.edu/policies/it-03-eligibility-use-it-resources/index.html))
* [Acceptable Use Agreement](https://informationsecurity.iu.edu/policies/acceptable-use.html) (requires IU computing account to access and sign agreement)