**Awareness and Training (AT) 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 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 objective of this standard is to mitigate risk by ensuring that:

* Ongoing security awareness training is provided to those who manage institutional data, including an awareness of the security risks and how to comply with applicable laws, regulations, policies, standards, and procedures.
* Employees understand their responsibilities in protecting the university’s information and are adequately trained to carry out their assigned information security-related duties and responsibilities; and
* A system and/or process is in place to track training requirements.

The university’s information security awareness program aims to deliver information about risks and security practices so that IU employees understand how to protect the confidentiality, integrity, and availability of systems and data. The purpose of the training is to inform employees about known threats, procedures for reporting a security incident, the types of data IU collects, how that data is classified, and what their data handling responsibilities are as employees of the university.

IU community members are responsible for:

* Completing assigned information security awareness course(s);
* Following safe computing practices as outlined in the [Acceptable Use Agreement](https://one.iu.edu/task/iu/acceptable-use-agreement);
* Reviewing [university information security policies](https://policies.iu.edu/?keywords=&dept=information-and-it&sort=); and
* Completing additional security and data compliance training related to their job.

## Standard

The following tables detail baseline security controls for awareness and training 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:**   | **Security Awareness Training** |
| **Required for:** | **High**   |  |  |
| **IU Implementation**   | Provide security awareness training to employees who manage institutional data and access IU’s enterprise systems to ensure they understand their responsibilities to safeguard the data they manage, how to safeguard that data, what data poses risk to the university, and how to report an incident if unauthorized access does occur.Those responsible for the training must review the content annually to ensure it is adequately maintained and addresses the following:* Executive management’s commitment to information security
* General responsibilities for securing and protecting the university’s information
* Basic information security procedures (e.g., information security incident reporting); see [ISPP-26](https://policies.iu.edu/policies/ispp-26-information-system-incident-reporting/index.html).
* Basic information for baseline controls (e.g., password security, malware, multifactor authentication); see [IT-12](https://policies.iu.edu/policies/it-12-security-it-resources/index.html).
* Secure use of mobile devices and security requirements for working remotely (e.g., IU-issued and IU-managed devices, VPN); see [IT-12.1](https://informationsecurity.iu.edu/policies/it121.html).
* Procedures for releasing data to third parties; see [DM-02](https://policies.iu.edu/policies/dm-02-disclosing-institutional-information/index.html).
* Contacts for additional information
 |
| **Notes**   | Required:* [Acceptable Use Agreement](https://informationsecurity.iu.edu/policies/acceptable-use.html) (all users)
* [Data Protection and Privacy Tutorial](https://expand.iu.edu/browse/e-training/courses/data-protection-and-privacy-tutorial)

For more, see <https://datamanagement.iu.edu/training/index.html>.Optional:* IU's [guide to online safety and security](https://informationsecurity.iu.edu/protect-data/index.html)
* [IT Training Security training opportunities](https://ittraining.iu.edu/explore-topics/security/index.html)
 |
| **NIST Cross Reference**   | AT-2 |

|  |  |
| --- | --- |
| **Control:**   | **Role-based Security Training** |
| **Required for:** | **High**   |  |  |
| **IU Implementation**   | Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards. Institutions determine the appropriate content of security training based on the assigned roles and responsibilities of individuals, the specific security requirements of organizations, and the information systems to which employees have authorized access.* Training must include policies, procedures, and tools based on the specific security roles assigned. Provide specific role-based security training for those managing data in enterprise systems (SIS, HRMS, EMR, etc.) and for specific data domains including FERPA, HIPAA, and HR data.
* Review training content annually to ensure content is maintained as tools and procedures are updated.
* Training must be reviewed and updated as applicable laws or regulations are amended.
 |
| **Notes**   | * Roles that would warrant this training include but are not limited to information developers, information architects and publishers, data stewards, data managers, IT professionals, IT managers, security analysts, security engineers, system and network administrators, fiscal officers, and purchasing acquisition contract managers.
* Security training information:
	+ [Required & Recommended Data Training](https://datamanagement.iu.edu/training/index.html)
	+ [FERPA Tutorial](https://ferpa.iu.edu/), including security information
	+ [HRMS Data Use Tutorial](https://expand.iu.edu/browse/e-training/courses/hrms-data-use)
	+ [HIPAA Training](https://compliance.iu.edu/compliance-areas/hipaa/training.html)
 |
| **NIST Cross Reference**   | AT-3 |

|  |  |
| --- | --- |
| **Control:**   | **Tracking Successful Completion of Training Requirements** |
| **Required for:** | **High**   |  |  |
| **IU Implementation**   | * User completion of training requirements must be tracked, including date of completion.
* Automate tracking and enforcement where possible.
* Notify users of training requirements and when required training is due for renewal.
* Data stewards and owners are responsible for identifying training requirements.
* Data managers are responsible for enforcing training requirements for enterprise systems.
 |
| **Notes**   | Tools for reviewing compliance training:* <https://usss.iu.edu/apps/compliancelookup/>
* <https://gm.acm.iu.edu/>
* Instructure analytics to verify completion of the Data Protection and Privacy Tutorial
* [My IU Compliance](https://indianauniversity.my.site.com/compliance/s/)
 |
| **NIST Cross Reference**   | AT-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