**Access Control (AC) 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 revised*

**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 access to IT resources is limited:

* To authorized users,
* To processes acting on behalf of authorized users or devices (including other information systems), and
* To the types of transactions and functions authorized users are permitted to execute.

## Standard

The following tables detail baseline security controls for access control 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:** | **Account Management** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | * Use centrally provisioned university accounts whenever feasible. * Document account types, roles, and responsibilities, including accounts that share passwords (for example, group accounts). * Implement a defined account management process. * Review accounts quarterly (at a minimum) to assess the need for continued account access. | | |
| **Notes** | A system can meet the requirements of this safeguard by leveraging centrally provisioned IU accounts or IU Active Directory for authentication.  Related policies:   * [Policy IT-03 (Eligibility to Use IT Resources)](https://policies.iu.edu/policies/it-03-eligibility-use-it-resources/index.html) * [Policy IT-18 (Computer and Network Accounts Administration)](https://policies.iu.edu/policies/it-18-accounts-administration/index.html) * [Policy IT-28 (Cyber Risk Mitigation Responsibilities)](https://policies.iu.edu/policies/it-28-cyber-risk-mitigation/index.html) | | |
| **NIST Cross Reference** | AC-2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Access Enforcement** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Ensure systems enforce authorizations to systems, applications, and data in accordance with security categorization and university policy. | | |
| **Notes** | Examples of technical access control mechanisms include passwords, roles, encryption, etc.  A system may meet some or all of the requirements of this safeguard by leveraging centrally provisioned authentication and group management. | | |
| **NIST Cross Reference** | AC-3 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Least Privilege** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | * Allow only the access necessary to accomplish assigned tasks. * Perform day-to-day operations using a non-privileged account. Only use privileged accounts for tasks that require additional capabilities. * Regularly review privilege levels (quarterly minimum). | | |
| **Notes** | A system can meet this safeguard by leveraging centrally provisioned IU systems, IU Login, or IU Active Directory for authentication. | | |
| **NIST Cross Reference** | AC-6 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Unsuccessful Login Attempts** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Where feasible, lock out access after 25 unsuccessful login attempts for a minimum of 10 minutes. | | |
| **Notes** | A system can meet this safeguard by leveraging centrally provisioned IU systems, IU Login, or IU Active Directory for authentication. | | |
| **NIST Cross Reference** | AC-7 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Device Lock** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Whenever feasible, employ a session lock/screen lock on any device or application after 15 minutes of user inactivity. | | |
| **Notes** | The time period should be consistent across all devices managed by individual teams. | | |
| **NIST Cross Reference** | AC-11 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Wireless Access** | | |
| **Required for:** | **High** | **Moderate** |  |
| **IU Implementation** | When accessing IU resources from wireless networks external to IU, ensure that the Wi-Fi connection is encrypted. | | |
| **Notes** | * IU VPN can be used as an alternative for secure connections to IU resources. * External networks must be using at least WPA2 to qualify. * WPA is obsolete and must not be used. | | |
| **NIST Cross Reference** | AC-18 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Access Control for Mobile Devices** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | All mobile devices used by faculty, staff, affiliates, or student-employees to access, store, or manipulate institutional data must follow IT-12.1 (Mobile Device Security Standard). | | |
| **Notes** | Refer to [IT-12.1 (Mobile Device Security Standard)](https://informationsecurity.iu.edu/policies/standards/it121.html) for details. | | |
| **NIST Cross Reference** | AC-19 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Use of External Systems** | | |
| **Required for:** | **High** | **Moderate** |  |
| **IU Implementation** | * Use IU-provided assets to access IU systems and data when feasible. * Ensure that IU procurement, data steward, and security review processes are followed prior to storing or processing IU data on external systems. | | |
| **Notes** | Related policies:   * [Policy HR-06-80 (Remote Work for Staff and Temporary Employees)](https://policies.iu.edu/policies/hr-06-80-remote-work-employees/index.html) * [Policy ACA-83 (Remote Work for Academic Appointees)](https://policies.iu.edu/policies/aca-83-remote-work-for-academic-appointees/index.html) * [Policy DM-02 (Disclosing Institutional Information to Third Parties)](https://policies.iu.edu/policies/dm-02-disclosing-institutional-information/index.html)   Does not apply to students using their personal computers/devices in their role as students. | | |
| **NIST Cross Reference** | AC-20 | | |

## 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