**Audit and Accountability (AU) 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 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:

* Information system audit records are created, protected, and retained to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and
* The actions of individual information system users can be uniquely traced to those users.

Most information technology has the capability to generate logs such as authentication logs, access logs, system logs, application logs, or service logs. Although different terms may be used for the logs generated by different parts of the technology stack, the concept remains the same. These logs are files that record observable occurrences, events, transactions, or activities that occur on an IT resource and are used for a variety of purposes including troubleshooting, system optimization, detecting unauthorized access or usage, incident investigations, or to meet compliance requirements.

## Standard

The following tables detail baseline security controls for audit and accountability 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:** | **Event Logging** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | 1. Identify the types of events that the IT resource can log, and then determine which are needed to secure and support operations and to meet compliance requirements. 2. Document what logs are being kept and review annually or after major system updates.   Systems must have logs to support business operations, security, and incident response. Logs must at a minimum:   * Log successful and unsuccessful logins. * Log database access to Restricted and Critical data. * Log time and date of events. * Log network addresses when applicable. * Be able to trace actions to individual users. | | |
| **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** | AU-2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Content of Audit Records** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | At a minimum, all logs must contain the following elements:   * WHEN: Time stamp of activity with UTC offset * WHAT: Description of action taken (for example, logged in, accessed file, moved file, executed program, modified configuration, etc.) and identifier of resource being interacted with * WHO: Account or session being used to access the resource * WHERE: Location of the user accessing the resource (e.g., IP address) | | |
| **Notes** | The above information is provided by metadata such as time stamps, source and destination addresses, user or process identifiers, success or failure indicators, and filenames involved.  Unless otherwise required by contract, regulation, etc., logs must NOT contain the following kinds of information:   * Unencrypted Critical or Restricted data * Access tokens * Cleartext authentication credentials * Database connection strings * Encryption keys * Information illegal to collect in the relevant jurisdiction | | |
| **NIST Cross Reference** | AU-3 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Response to Audit Logging Process Failures** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Monitor the log process and notify the appropriate personnel to take appropriate action in the event of failure. | | |
| **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** | AU-5 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Audit Log Record Review, Analysis, and Reporting** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | * Review and analyze logs for deviations from baseline and indications of inappropriate, unlawful, unauthorized, suspicious, or unusual activity, and report to appropriate personnel. * Log review and analysis must be automated and performed daily. | | |
| **Notes** | Use automated log analysis and alerting for resources involving Critical and Restricted institutional data, and test the log automation every 90 days. [(IDS Checklist row 41](https://datamanagement.iu.edu/tools/ids-checklist.html))  Related: [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) | | |
| **NIST Cross Reference** | AU-6 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Time Stamps** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Ensure that all log entries are time stamped, and that time stamps are synchronized with the university’s time servers or a trusted authoritative time source. | | |
| **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** | AU-8 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Audit Log Record Retention** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Retain logs for a minimum of 30 days (60 days recommended if practicable) or longer if necessary and in accordance with the [Indiana University Records Retention Schedule](https://one.iu.edu/launch-task/iu/records-retention-schedule?terms=records%20retention) to meet applicable regulatory requirements (e.g., PCI-DSS, HIPAA, etc.) and to support troubleshooting, audits, and incident response.  Be sure to allocate sufficient log storage space to retain the log data for the required timeframe. | | |
| **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** | AU-4, AU-11 | | |

## 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