**Incident Response (IR) 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

Per [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) the University Information Security Office (UISO) Incident Response Team is responsible for overseeing and guiding the information and IT security incident management process to promote a coordinated, consistent, efficient, and effective response.

Although the UISO Incident Response Team has institutional-level responsibility for assisting units and coordinating the response to information and IT security incidents, units must also have their own procedures to facilitate initial response at the departmental level.

Most units will find that the [departmental incident response plan template](https://informationsecurity.iu.edu/doc/managing-incidents---ir_procedure_template_2021.pdf) (found at [informationsecurity.iu.edu](https://informationsecurity.iu.edu/report-incident/managing-incidents.html)) will be sufficient to meet this need. In the event a more robust plan is desired, contact it-incident@iu.edu for guidance.

The key objectives of this standard are to ensure:

* An operational information and IT security incident handling capability for organizational information systems, including adequate preparation, detection, analysis, containment, recovery, and user response activities; and
* The tracking, documentation, and reporting of incidents to appropriate organizational officials and/or authorities.

## Standard

The following tables detail baseline security controls for information and IT security incident response 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:** | **Incident Response Awareness** |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation**   | All users must be aware of their responsibility to properly handle and report incidents. Users agree to this responsibility through their assent to the [Acceptable Use Agreement](https://informationsecurity.iu.edu/policies/acceptable-use.html) as part of their initial account creation process and every two years thereafter.Additionally, units must annually review security incident response responsibilities with their users consistent with their assigned roles and responsibilities.  |
| **Notes** | Awareness for end users can be as simple as an annual reminder of their responsibility to report incidents.Administrators may require additional training on how to handle incidents including detection and appropriate response measures. |
| **NIST Cross Reference**   | IR-2 |

|  |  |
| --- | --- |
| **Control:** | **Incident Handling** |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Units must:1. Have procedures to facilitate initial response at the unit level;
2. Identify a unit-level coordinator and unit member responsible for reporting; and
3. Have initial action plans and procedures for escalation to the UISO Incident Response Team.

The UISO Incident Response Team:1. Implements an incident handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.
 |
| **Notes** | See:* [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)
* [How to Report an IT Incident](https://informationsecurity.iu.edu/report-incident/index.html)
* [Report a suspected information or IT security issue at IU](https://kb.iu.edu/d/ahex)
 |
| **NIST Cross Reference** | IR-4 |

|  |  |
| --- | --- |
| **Control:** | **Incident Monitoring** |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Information and IT security incidents must be monitored and documented. Records must be maintained about each incident, including any information necessary to support effective incident response.  |
| **Notes** | In addition to incident monitoring performed by UISO at the university level, units must maintain a log of unit-level incidents. |
| **NIST Cross Reference** | IR-5 |

|  |  |
| --- | --- |
| **Control:** | **Incident Reporting** |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | All users are required to “report unauthorized access to, inadequate protection of, and inappropriate use, disclosure, and/or disposal of information, immediately” per [Policy ISPP-26](https://policies.iu.edu/policies/ispp-26-information-system-incident-reporting/index.html). |
| **Notes** | See [Report an IT incident](https://informationsecurity.iu.edu/report-incident/index.html). |
| **NIST Cross Reference** | IR-6 |

|  |  |
| --- | --- |
| **Control:** | **Incident Response Assistance** |
| **Required for:** | **High**   | **Moderate**  | **Low**   |
| **IU Implementation**   | Indiana University offers support materials containing advice and assistance related to the handling and reporting of incidents for users of IU IT resources.At the institutional level, this is primarily through [Policy ISPP-26](https://policies.iu.edu/policies/ispp-26-information-system-incident-reporting/index.html), the UISO Incident Response Team, the Support Center (which directs users to Incident Response as appropriate), and the Knowledge Base.Unit IT Staff, application administrators, and service owners must also be able to advise and assist users appropriately.Units must be prepared to assist, as needed, especially in the areas of preparation, detection, and recovery. |
| **Notes**   | See:* [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))
* [How to Report an IT Incident](https://informationsecurity.iu.edu/report-incident/index.html)
* [Report a suspected information or IT security issue at IU](https://kb.iu.edu/d/ahex)
 |
| **NIST Cross Reference**   | IR-7 |

|  |  |
| --- | --- |
| **Control:** | **Incident Response Plan** |
| **Required for:** | **High**   | **Moderate**  | **Low**   |
| **IU Implementation** | The University Information Security Office Incident Response Team is responsible for creating and maintaining a university-level incident plan that outlines overarching goals and processes to facilitate response to information and IT security incidents.Units must also have procedures to facilitate initial response at the departmental level. Units must maintain a department incident response plan that identifies a unit-level coordinator, procedures for unit-level reporting, initial actions, and escalation procedures to the UISO Incident Response Team. |
| **Notes** | Most units will find that the [departmental incident response plan template](https://informationsecurity.iu.edu/doc/managing-incidents---ir_procedure_template_2021.pdf) (found at [informationsecurity.iu.edu](https://informationsecurity.iu.edu/report-incident/managing-incidents.html)) will be sufficient to meet this need. In the event a more robust plan is desired, contact it-incident@iu.edu for guidance. |
| **NIST Cross Reference** | IR-8 |

## Definitions

**Security Incident** -The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or the attempted or successful interference with system operations in an information system. Security incident also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, misrouting of mail, or compromise of physical security, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification, or destruction.

**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

* [Policy ISPP-26 (Information & Information System Incident Reporting, Management, and Breach Notification](https://policies.iu.edu/policies/ispp-26-information-system-incident-reporting/index.html))
* [Report an Incident](https://informationsecurity.iu.edu/report-incident/index.html)
* [Unit Incident Response Plan Template](https://informationsecurity.iu.edu/doc/managing-incidents---ir_procedure_template_2021.pdf)
* [NIST 800-53 r5.1 Incident Response Control Family](https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1&family=IR)
* [Policy DM-01 (Management of Institutional Data](https://policies.iu.edu/policies/dm-01-management-institutional-data/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 & Abuse of Information Technology Resources](https://policies.iu.edu/policies/it-02-misuse-abuse-it-resources/index.html))
* [Policy IT-07 (Privacy of Electronic Information & Information Technology Resources](https://policies.iu.edu/policies/it-07-privacy-it-resources/index.html))
* [Policy IT-11 (Excessive Use of Information Technology Resources](https://policies.iu.edu/policies/it-11-excessive-use-it-resources/index.html))