**Contingency Planning (CP) 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 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*](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 objective of this standard is to ensure that plans for emergency response, backup operations, and post-disaster recovery for organizational information systems are established, maintained, and effectively implemented to ensure the availability of information technology resources and continuity of operations.

## Standard

The following tables detail baseline security controls for contingency planning 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:** | **Contingency Plan** | | |
| **Required for:** | **High** | **Moderate** |  |
| **IU Implementation** | * Establish contingency plans for information technology resources identifying critical business functions, priorities, roles and responsibilities, emergency operations, and disaster recovery procedures. * Review and approve contingency plans annually. | | |
| **Notes** | See also [Domain 11, Business Continuity Management](https://informationsecurity.iu.edu/program/safeguards/managing-business-continuity.html), from the Information Security and Privacy Program.  See also [Prepare your department for a crisis](https://protect.iu.edu/emergency-continuity/continuity-plan.html). | | |
| **NIST Cross Reference** | CP-2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **System Backup** | | |
| **Required for:** | **High** | **Moderate** |  |
| **IU Implementation** | Back up system information and documentation. Backups must be:   * Stored at a secure, separate location * Encrypted per university and compliance requirements * Regularly tested | | |
| **Notes** | Use of centrally provisioned, common IT infrastructure and services provided by UITS often fulfills this requirement. Check with the service owner for details.  See also [Back up data](https://informationsecurity.iu.edu/resources-professionals/backing-up-data.html). | | |
| **NIST Cross Reference** | CP-9 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **System Recovery and Reconstitution** | | |
| **Required for:** | **High** | **Moderate** |  |
| **IU Implementation** | * Systems must be recoverable to a known state after an incident. * Review and test disaster recovery plans annually. | | |
| **Notes** | See also [Departmental disaster recovery planning](https://informationsecurity.iu.edu/resources-professionals/disaster-recovery-planning.html).  Effective disaster recovery includes resetting all system parameters, reinstalling patches, and reconfiguring/reinstalling applications and system software. | | |
| **NIST Cross Reference** | CP-10 | | |

## 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

October 11, 2022 updates

February 12, 2022 draft for review

## Related Information

* [Business Continuity Planning](https://protect.iu.edu/emergency-planning/continuity-planning/index.html)