**Physical and Environmental Protection (PE) 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*

## 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:

* Physical access to information systems, equipment, and their respective operating environments is limited to authorized individuals;
* The physical plant and support infrastructure for information systems are protected;
* Supporting utilities (e.g., electrical service) for information systems are provided;
* Information systems are protected against environmental hazards; and
* Appropriate environmental controls are provided in facilities containing information systems.

## Standard

The following tables detail baseline security controls for physical and environmental protection 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.

Controls PE-6, PE-8, and PE-16 apply only to university, campus, or unit-level data centers categorized as “High”.

|  |  |
| --- | --- |
| **Control:** | **Physical Access Authorizations** |
| **Required for:** | **High**   |  |  |
| **IU Implementation**   | * Develop, approve, and maintain a list of individuals who are authorized to access the physical area where IT resources are housed.
* Review the list of authorized individuals at least quarterly and remove individuals from the list who are no longer authorized for access.
 |
| **Notes**   | * This control applies to all employees, students, and contractors.
* 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**   | PE-2 |

|  |  |
| --- | --- |
| **Control:** | **Physical Access Controls** |
| **Required for:** | **High**   |  |  |
| **IU Implementation** | * Implement physical access control for the physical areas housing IT resources.
* Maintain physical access logs for the facility.
* Ensure visitors are monitored and/or escorted in the facility.
 |
| **Notes** | * This control applies to all employees, students, and contractors.
* Examples of appropriate physical controls can include locked doors, reception desk staff, keycard readers, and/or door keys or access cards for authorized personnel only.
* Controls for visitors may include visitor badges, visitor escorts, and/or requiring visitors to sign in at the front desk.
* See also PS-5, Access Control for Output Devices in this standard.
* 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

**SCOPE:** Does not apply to public areas. |
| **NIST Cross Reference** | PE-3 |

|  |  |
| --- | --- |
| **Control:** | **Access Control for Output Devices** |
| **Required for:** | **High**   |  |  |
| **IU Implementation**   | Control physical access to information output devices such as printers and fax machines to prevent unauthorized access to Critical or Restricted data. |
| **Notes**   | See Physical Access Controls in this standard for examples of access controls.**SCOPE:** Applies to devices such as computers, monitors, printers, copiers, fax machines, and audio devices. |
| **NIST Cross Reference**   | PE-5 |

|  |  |
| --- | --- |
| **Control:** | **Monitoring Physical Access** |
| **Required for:** | **High**   |  |  |
| **IU Implementation**   | Monitor physical access to areas storing information systems. |
| **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**   | PE-6 |

|  |  |
| --- | --- |
| **Control:**   | **Visitor Access Records** |
| **Required for:** | **High**   |  |  |
| **IU Implementation**   | Document visitor access to data centers. Retain access logs for a minimum of 45 days. |
| **Notes**   | Logs can be electronic or as simple as a sign-in sheet. Logs are only needed for the parts of a facility that require authorized access (i.e., they are not necessary for public areas).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**   | PE-8 |

|  |  |
| --- | --- |
| **Control:** | **Emergency Power** |
| **Required for:** | **High**   |  |  |
| **IU Implementation** | Use a backup or uninterruptible power supply to continue operations in the event of the loss of primary power, and/or to facilitate an orderly shutdown of the resource. |
| **Notes** | Some systems may require longer backup power solutions than others. Consider the effects of an outage on systems in terms of their criticality or impact on public safety, and take these effects into consideration when determining the length of time for which backup power is needed.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** | PE-11 |

|  |  |
| --- | --- |
| **Control:**   | **Delivery and Removal** |
| **Required for:** | **High**   |  |  |
| **IU Implementation**   | Develop a process to authorize, control, and record the entry and exit of information technology resource components into and out of the facility.Maintain records of current components. |
| **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**   | PE-16 |

## Definitions

**Data Center** - A data center or computer facility is a physical site, location, or area where concentrations of information technology resources such as computers (other than personal computers/workstations), computer systems, and associated components, such as telecommunications and storage systems, are housed to provide necessary environmental, physical, or other safeguards. Data centers may be institutional-level, campus-level, or unit-level.

**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