**Security Categorization Procedure for**

Figure 1- Indiana University Seal—only approved university-wide policies may use the seal

**Information Technology Resources**

# IT-12

**About This Procedure**

**Effective Date:**

*In review*

**Date of Last Review/Update:**

*3/23/23 draft*

**Responsible University Office:**

*University Information Policy Office*

**Responsible University Administrator:**

***Office of the Vice President for Information Technology and Chief Information Officer***

**Contact:**

***University Information Security Office***

*uiso@iu.edu*

## Scope

This procedure 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 objective of this procedure is to describe a methodology for assigning a security category to university IT resources for the purpose of determining minimum security safeguards to be applied to the resource. The security category is based on the potential impact on individuals, the unit, or the university should an adverse event occur that jeopardizes information or IT resources “needed by the organization to accomplish its mission, protect its assets, fulfill its legal obligations, maintain its day-to-day functions, and protect individuals.” (Loosely based on FIPS 199, with simplifications to facilitate adoption and use.)

The technical manager of the IT resource and the resource owner shall work together to determine the security category of an IT resource.

## Procedure

1. Define the IT resource to be categorized. Determine the scope of the IT resource (for example, service, server, system, application, etc.) and identify, as applicable, the included hardware and software components, data, information flow, system interconnections, networking, and system boundaries.
2. Identify the data types that the resource transmits, processes, and/or stores and the **highest** institutional data classification involved using the “Data Classification” table. (For more on IU data classifications and definitions, see the [IU Data Management](https://datamanagement.iu.edu/index.html) website and the [Data Sharing and Handling](https://datamanagement.iu.edu/tools/dsh.html) tool.)

|  |
| --- |
| **Table 1. Data Classification**  |
|   | **Definition**  | **Example Data Types**  |
| **Critical**  | Inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access to this type of information by an individual or many individuals  | Patient records, payment card data, Social Security numbers, driver’s license numbers, passwords  |
| **Restricted**  | Because of legal, ethical, or other constraints, may not be accessed without specific authorization, or only selective access may be granted  | Student records, last 4 digits of SSN, date of birth, employee home address, facility floor plans  |
| **University-Internal**  | May be accessed by eligible employees and designated appointees of the university in the conduct of university business; access restrictions should be applied accordingly  | University ID numbers, student directory information, offer letters, tenure recommendations, basic floor plans  |
| **Public**  | Few restrictions; generally releasable to a member of the public upon request; upon receipt of a request, seek advice from the appropriate Data Steward; if the request is made pursuant to the Indiana open records statute, seek advice from the Office of the VP and General Counsel, as well as the appropriate Data Steward  | Usernames, student names and majors, employee names and compensation, campus maps  |

1. Use the “Usage Classification” table to identify the usage impact by evaluating the potential impact on use/operations.

|  |
| --- |
| **Table 2. Usage Classification**  |
|   | **Definition**  | **Example Systems or Services**  |
| **Essential** | The service is essential to the university. The service:* Is critical to the operations of the university;
* Serves the university community as a whole or a large population of users; AND/OR
* Is essential to the health or safety of community members and unavailability of the system would likely imperil them.
 | GlobalNOC, Active Directory, DHCP, DNS, internet and internal networks  |
| **Operational**  | The service is a part of the operations of the university. The service:* Is a general function of the university;
* Supports general functions of the university; AND/OR
* Serves many users or groups of users.
 | Canvas, email, MS OneDrive, Kuali, IUanyWare, Zoom |
| **Non-essential**  | The service is non-essential. The service:* Is a minor function of the university;
* Is unimportant to supporting the objectives of the university; AND/OR
* There would be little or no impact if the service were unavailable.
 | Departmental website, IU Classifieds |

1. Use the “Security Categorization” table to determine where the data classification from Table 1 intersects with the usage classification from Table 2, and assign the specified value as the security category of the IT resource.

|  |
| --- |
| **Table 3. Security Categorization** |
|   | **Usage Classification**  |
| Non-essential  | Operational  | Essential |
| **Data Classification**  | Public  | Low  | Moderate  | N/A |
| University-Internal  | Moderate | Moderate  | High  |
| Restricted  | N/A | High | High  |
| Critical  | N/A | High  | High  |

EXAMPLES

Example 1:

A unit maintains institutional information classified as “**Public**” on its web server and determines a data compromise or loss of the server could result in an “**Operational**” usage impact.

The resulting security categorization is: **Moderate** (where data classification intersects with usage classification in Table 3).

|  |
| --- |
| **Security Categorization**  |
|   | **Usage Classification** |
| Non-essential  | Operational  | Essential |
| **Data Classification**  | Public  | Low  | Moderate  | N/A |
| University-Internal  | Moderate | Moderate  | High  |
| Restricted  | N/A | High | High  |
| Critical  | N/A | High  | High  |

Example 2:

A unit managing routine administrative informationwith a data classification of “**University-Internal**” on its server in the Intelligent Infrastructure determines that the potential impact of loss on business operations is “**Non-essentia**l”.

The resulting security categorization is: **Moderate** (where data classification intersects with usage classification in Table 3).

|  |
| --- |
| **Security Categorization**  |
|   | **Usage Classification** |
| Non-essential  | Operational  | Essential |
| **Data Classification**  | Public  | Low  | Moderate  | N/A |
| University-Internal  | Moderate | Moderate  | High  |
| Restricted  | N/A | High | High  |
| Critical  | N/A | High  | High  |

Example 3:

A unit manages student information with a data classification of “**Restricted**” on its server with a usage classification of “**Operational**”.

The resulting security categorization is: **High** (where data classification intersects with usage classification in Table 3).

|  |
| --- |
| **Security Categorization**  |
|   | **Usage Classification** |
| Non-essential  | Operational  | Essential |
| **Data Classification**  | Public  | Low  | Moderate  | N/A |
| University-Internal  | Moderate | Moderate  | High  |
| Restricted  | N/A | High | High  |
| Critical  | N/A | High  | High  |

Example 4:

A unit manages health data with a data classification of “**Critical**” on its on-premises clinical imaging server with a usage classification of “**Operational**”.

The resulting security categorization is: **High** (where data classification intersects with usage classification in Table 3).

|  |
| --- |
| **Security Categorization**  |
|   | **Usage Classification** |
| Non-essential  | Operational  | Essential |
| **Data Classification**  | Public  | Low  | Moderate  | N/A |
| University-Internal  | Moderate | Moderate  | High  |
| Restricted  | N/A | High | High  |
| Critical  | N/A | High  | High  |

Example 5:

Networking maintains a routing table necessary for the day-to-day function of Indiana University with a usage classification of “**Essential**” and a data classification of “**University-Internal**”.

The resulting security categorization is: **High** (where data classification intersects with usage classification in Table 3).

|  |
| --- |
| **Security Categorization**  |
|   | **Usage Classification** |
| Non-essential  | Operational  | Essential |
| **Data Classification**  | Public  | Low  | Moderate  | N/A |
| University-Internal  | Moderate | Moderate  | High  |
| Restricted  | N/A | High | High  |
| Critical  | N/A | High  | High  |

## Reason for the Procedure

Information technologies are critical to most if not all Indiana University operations. This dependence has resulted in a large, diverse, and complex technological environment, which in turn has resulted in a greater threat surface and opportunity for intrusion attempts.

As more data is being stored, accessed, and manipulated electronically, the risk to systems increases, as does the risk of unauthorized disclosure or modification of personal, proprietary, or institutional data.

The use of automated scanners and break-in scripts facilitates the scanning of entire networks for vulnerable systems. Systems that are not properly secured will be discovered and can be subject to intrusion and exploitation. Data on vulnerable systems is at risk of compromise, alteration, or destruction. Compromised systems will also be used to compromise or attack other systems.

This procedure supports [Policy IT-12](https://policies.iu.edu/policies/it-12-security-it-resources/index.html) to promote compliance with legal, regulatory, and contractual requirements to safeguard data while protecting university IT resources from compromise.

## Definitions

**Procedure** - Procedures (like standards) support policy by further describing specific implementation details (i.e., the "how"). A procedure can be thought of as an extension of a policy that articulates a process to be used in carrying out/complying with the policy. A procedure may describe a series of steps, or how to use standards and guidelines to achieve the goals of a policy. Procedures, along with standards, promote a consistent approach to following policy. Procedures make policies more practically meaningful and effective. Procedures overlap with standards, although procedures tend to be more focused on process while standards tend to be more focused on requirements or specifications. Because procedures directly support policies, compliance with procedures is nonoptional and failure to follow procedures 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 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** | **Email** |
| General questions | University Information Security Office | uiso@iu.edu |

## History

February 12, 2022 draft for review

March 23, 2022 revised and simplified

April 6, 2022 additional examples added

**Related Information**

* [Policy DM-01 (Management of Institutional Data)](https://policies.iu.edu/policies/dm-01-management-institutional-data/index.html)
* [Data Management Website](https://datamanagement.iu.edu/types-of-data/classifications.php)
* [Data Sharing and Handling Tool](https://datamanagement.iu.edu/tools/data-storage-and-handling.php)