**System and Communications Protection (SC) 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:**

*4/20/2023 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 objectives of this standard are to ensure that:

* Organizational communications (i.e., information transmitted or received by organizational information systems) are monitored, controlled, and protected at the external boundaries and at key internal boundaries of the information systems; and
* Architectural designs, software development techniques, and systems engineering principles are employed to promote effective information security within organizational information systems.

## Standard

The following tables detail baseline security controls for system and communications 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.

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Denial of Service Protection** | | |
| **Required for:** | **High** | **Moderate** |  |
| **IU Implementation** | Implement safeguards to mitigate the risk of Denial of Service (DoS) attacks. | | |
| **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** | SC-5 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Boundary Protection** | | |
| **Required for:** | **High** | **Moderate** |  |
| **IU Implementation** | Control network communications at internal and external boundaries. Implement as many of the following as practicable:  1. Ensure operating system firewalls for Windows, Mac, and endpoint devices are enabled.  2. Enable host firewalls on servers and configure them to deny by default. Open only those ports necessary for the service to operate.  3. Locate servers behind the Data Center firewall and configure firewall rules to deny by default. Open only those ports necessary for the service to operate.  4. Use private IP addresses unless external access is necessary and the server has appropriate controls in place.  5. Disable unneeded network ports and protocols on servers.  6. Disable or secure system-to-system access on servers.  7. Bastion hosts and/or VPN must be used for remote admin access to servers.  8. Regularly review and update server boundary protections. | | |
| **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** | SC-7 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Transmission Confidentiality and Integrity** | | |
| **Required for:** | **High** | **Moderate** |  |
| **IU Implementation** | * Encrypt data in transit. * Use a [web server certificate](https://kb.iu.edu/d/beec) to enable web server authentication and SSL/TLS encryption on web servers. * Use the [Cisco Secure Email Encryption Service (CSEES)](https://kb.iu.edu/d/bbtq) to encrypt any emails with sensitive information that leave the IU network. | | |
| **Notes** | * Examples of encrypted network communications include sftp, https, ssh, and VPN. * Examples of unencrypted network protocols include telnet, ftp, rcp, unencrypted smb, and vnc. * Encrypt data prior to transmission if use of an unencrypted connection is unavoidable. * 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** | SC-8 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Cryptographic Key Establishment and Management** | | |
| **Required for:** | **High** | **Moderate** | **Low** |
| **IU Implementation** | Manage encryption keys to keep them secure:  1. Ensure that private keys have read-only permissions to key owners or processes that need to access them.  2. Use vendor-recommended best practices to protect keys when implementing encryption in the cloud.  3. Do not write down keys on paper. Use a password manager or a hardware key.  4. Do not hard-code keys into software.  5. Limit keys to a single, specific purpose.  6. Use publicly known encryption algorithms, e.g., RSA (2048-bit minimum) or ECDSA, etc. | | |
| **Notes** | Do not use a self-made encryption algorithm.  See also [Passphrase vaulting](https://kb.iu.edu/d/atyy) and [About data encryption](https://kb.iu.edu/d/bgpo).  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** | SC-12 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Control:** | **Protection of Information at Rest** | | |
| **Required for:** | **High** |  |  |
| **IU Implementation** | Encrypt Critical and Restricted data at rest.   1. Enable native encryption on endpoints, workstations, and mobile devices. 2. Use full-disk encryption (FDE) or file-level encryption (FLE)(e.g., encrypted file system) on physical and virtual servers. 3. Use vendor-recommended encryption mechanisms when a server is implemented in the cloud. 4. Encrypt removable media (e.g., external hard drives, flash drives, magnetic tapes, CD/DVDs). 5. Use self-encrypting drives (SEDs) where possible. | | |
| **Notes** | * To enable full-disk encryption on Windows, turn on BitLocker, and on Mac, turn on FileVault. On Linux, full-disk encryption options include LUKS, EncFS, ZFS, etc. * See [IT-12.1 (Mobile Device Security Standard)](https://informationsecurity.iu.edu/policies/it121.html). * Centralize key escrow of keys where practicable for easy access to data. * 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** | SC-28 | | |

## 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