This policy is under review. To view the current version, please visit here.

Security of Information Technology Resources

IT-12

About This Policy

Effective Dates:
11-28-2007

Last Updated:
10-23-2017

Responsible University Administrator:
Office of the Vice President for Information Technology & Chief Information Officer

Policy Contact:
University Information Policy Office, uipo@iu.edu

Scope

This policy 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.

Policy Statement

Information technology resources should be securely managed and used in a manner commensurate with their risk and criticality to protect the confidentiality, integrity, and availability of university information.

University organizational units, IT professionals, and users are responsible for ensuring their respective IT resources meet the applicable procedures and standards attached to this policy.

The University Information Policy and Security Offices have the authority (derived from Trustee Resolution of May 2001) to:

- Develop and implement policies necessary to minimize the possibility of unauthorized access to Indiana University's information technology infrastructure. This entails establishing security resources, policies, guidelines, and standards, as well as providing consulting services, for all Indiana University information technology resources.
- Assume leadership, responsibility, and control of responses to unauthorized access to Indiana University's information technology infrastructure, unauthorized disclosure of electronic information, and computer security breaches regardless of the Indiana University office involved.

These offices are to draw upon the experience, expertise, and resources of other university offices (including the Office of Internal Audit) where necessary and appropriate. This authority will be exercised if it becomes clear to the University Information Policy Officer or University Information Security Officer that the unit responding does not have the means to react appropriately and/or in a timely manner to a specific incident.

To protect university data and systems, as well as to protect threatened systems external to the university, the University Information Policy Officer or University Information Security Officer may place limits or restrictions on technology services provided on or from any university-owned or -managed system and network.

- Limitations may be implemented through policies, standards, and/or technical methods, and could include (but may not be limited to) usage eligibility rules, password requirements, or restricting or blocking certain protocols or use of certain applications known to cause security problems.

- Restrictions may be deployed permanently based on continuing threat or risk after appropriate consultation with affected constituents, or they may be deployed temporarily, without prior coordination, in response to an immediate and serious threat.
- Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or where the effect on university functions caused by the restriction approaches or exceeds risk associated with the threat, as negotiated between the affected constituents and the University Information Policy Officer or University Information Security Officer.

To protect university data and systems, as well as to protect threatened systems external to the university, the University Information Policy Officer or University Information Security Officer may unilaterally choose to virtually isolate a specific university system from university, campus, or external networks, given:

1. Advance consultation with the appropriate campus Chief Information Officer, where practical and where circumstances warrant.
2. Information in hand reasonably suggests that the system has been compromised.
3. There is ongoing activity associated with the system that is causing or will cause damage to other university systems or data or to assets of other internal or external agencies, or there is a medium to high risk of such damage occurring.
4. All reasonable attempts have been made to contact the responsible technicians or department management, or such contact has been made and the technician or department managers are unable to or choose not to resolve the problem in a reasonable time.
5. Isolation is removed when the risk is mitigated to an acceptable level, or where loss of access or function caused by the isolation approaches or exceeds risk associated with the threat, as negotiated between the responsible functional manager and the University Information Policy Officer or University Information Security Officer.

Reason For Policy

Information technologies have become critical in support of most if not all Indiana University operations. This dependence has resulted in a very large, diverse, and complex technology 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 are likely to be discovered and can then be subject to intrusion. Data on vulnerable/exploited systems is at risk of compromise, alteration, or destruction. Such systems may also be used to compromise or initiate denial of service (DOS) attacks against other university systems or systems at external sites.

This policy will promote compliance with legal, regulatory, and contractual requirements to safeguard data while protecting university IT resources from compromise.

Procedure

Functional unit management, IT professionals, and users (as applicable) are required to apply appropriate safeguards to their respective IT resources as indicated in the standards listed below using the following high-level process:

1. Identify the security categorization of the IT resource (high, moderate, or low) following the Security Categorization Procedure.
2. Apply the appropriate safeguards from the information security standards below as applicable to the IT resource based on its security category. The security category defines the minimum requirements for that level.

3. Document technology-appropriate required safeguards in place and note gaps in required safeguards. For existing IT resources, units have up to one year from the last review/update date of this policy to close gaps in newly required applicable safeguards.
4. Request an exception if applicable and relevant safeguards cannot practicably be applied to a particular IT resource.

Standards

- Access Control (AC) Standard
- Awareness and Training (AT) Standard
- Audit and Accountability (AU) Standard
- Configuration Management (CM) Standard
- Contingency Planning (CP) Standard
- Identification and Authentication (IA) Standard
- Incident Response (IR) Standard
- Maintenance (MA) Standard
- Media Protection (MP) Standard
- Mobile Device Security Standard
- Physical and Environmental Protection (PE) Standard
- Planning (PL) Standard
- Personnel Security (PS) Standard
- Risk Assessment (RA) Standard
- System and Services Acquisition (SA) Standard
- System and Communications Protection (SC) Standard
- System and Information Integrity (SI) Standard

Note: Specific compliance areas (e.g., HIPAA, PCI-DSS, etc.) may require additional controls beyond those specified in these standards. Contact the appropriate compliance office or officer for details.

Definitions

Indiana University information technology resources include all facilities and technologies used by the university to accept, store, transmit, process, manipulate, manage, display, or output data or information. This includes all hardware, software, and firmware components of the technology stack whether owned and managed by the university or provisioned from third parties on behalf of the university (e.g., licensed, leased, etc.). These components may be individually controlled (e.g., assigned to an employee), shared single-user or multi-user, centrally managed, standalone, or networked. This includes but is not limited to:

- Computers, servers, workstations, web servers, peripherals, and related equipment and software;
- Voice communications infrastructure, peripherals, and related equipment and software;
- Data communications and network infrastructure, peripherals, and related equipment and software;
- Classroom technologies and computer labs;
- Applications, systems, programs, and databases; and
- Electronic communication devices and services, including electronic mail, phones, voice mail, fax services, and related equipment and software.

University-owned computing resources are computer and computer-related equipment acquired and maintained in full or in part by funds provided by Indiana University.

University Information Policy Office (UIPO) is a unit within the Office of the Vice President for Information Technology and Chief Information Officer. The components of the UIPO mission germane to this policy are:

- To develop technology deployment and usage policies; and
- To provide a technology incident response function.

University Information Security Office (UISO) is a unit within the Office of the Vice President for Information Technology and Chief Information Officer. The mission of the UISO is to provide proactive security analysis, development, education, and guidance related to Indiana University's information asset and information technology environment.

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) for more detail.

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
Policy Interpretation	UIPO	uipo@iu.edu
Security Assessments	UISO	sassess@iu.edu
Incident Reporting	Incident Response	It-incident@iu.edu

History

- May 2020 – Revised to align with NIST 800-53 standard.
- October 23, 2017 – Added provision for two-factor privileged authentication.
- Jul 30, 2012 — Revised contact information.
- Oct 17, 2011 — Added links on reporting incidents to Related Policies, Laws, and Documents section.
- Nov 28, 2007 — Posted as interim policy. Currently in review.
- July 18, 2002 — Posted as draft.

Related Information

NIST 800-53 – Security and Privacy Controls for Information Systems and Organizations