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

Policy Statement

Indiana University organizational units (campuses, departments, offices, affiliated agencies, etc.) operating technology resources are responsible for ensuring that those systems are managed securely. This is required for all such systems, but is especially critical for those systems that support vital business functions and/or host sensitive personal or institutional information.

The University Information Technology 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, and to provide consulting services, for all Indiana University computer systems, telecommunications, or other information technology resources.

Managers and technicians within functional units are required to report any breaches or possible breaches of the security of Indiana University networks, systems, or data to the University Information Technology Policy Office Incident Response Coordinator, per published procedures. The University Information Technology Policy and Security Offices will assess the situation, and minimally provide advice as to appropriate response and reporting. While circumstances will vary, response will be guided by published general procedures and will be the task of the reporting unit.

The University Information Technology Policy and Security Offices have the authority (derived from Trustee Resolution of May 2001) to 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 IT Policy Officer or Security Officer that the unit responding does not have the means to react appropriately and/or in a timely manner to a specific incident.

Reason For Policy

Computing and networking and other information technologies have become critical in support of most if not all Indiana University operations. This dependence has resulted in a very large, very diverse, and very complex technology environment, which in turn has resulted in a greater opportunity for intrusion attempts. At the same time, much more data is being stored, accessed, and manipulated electronically, and as the risk to systems increases, the risk of unauthorized disclosure or modification of personal, proprietary, or institutional data is also

increased. It is very important that everyone associated with providing and using these technology services is diligent in their administration and responsive to security threats. It is also important that information related to intrusions, attempted intrusions, or other such incidents are shared so the event can be recognized and perhaps avoided elsewhere.

The use of automated scanners and break-in scripts makes it easy for someone to quickly scan entire networks for vulnerable systems. Systems that are not properly secured are likely to be discovered, and they will then be subject to intrusion. Data on vulnerable/exploited systems WILL be compromised, altered, or destroyed. Such systems may be used to compromise or initiate denial of service attacks against other University systems or systems at external sites.

Procedure

The following are generalized goal-oriented requirements; some may have multiple methods or solutions. Attending to these is important for all systems, but is ABSOLUTELY CRITICAL for those systems that support vital business functions and/or host sensitive personal or institutional information.

(Numbers do not indicate sequence or priority; they merely provide a method to reference specific items.)

For a computer system to be managed securely, *functional unit* management must:

1. Fully understand the sensitivity of the function or operation being supported by the system and the data being stored and/or manipulated on the system.
2. Hire technicians with the expertise necessary to appropriately maintain the hardware, operating systems, systems software, programs and other associated components of the systems to which they are assigned.
3. Ensure that technicians understand their responsibilities and the consequences of poorly managed systems (compromise of local or other systems, damage to data or systems, disclosure of sensitive data, potential legal liability for the department and Indiana University, possible loss of Federal and other funding for the department and Indiana University, etc.).
4. Provide necessary initial and refresher training to technicians as hardware or software components are revised or added.
5. Ensure that assignments and job plans account for time required for systematic and periodic audit and maintenance of systems.

For a computer system to be managed securely, functional unit technicians must:

1. Fully understand the sensitivity of the function or operation being supported by the system and the data being stored and/or manipulated on the system.
2. Not choose operating systems that are known as being difficult to maintain and secure.
3. Use technical tools to take an image of any freshly installed operating systems in order to speed recovery in the case of a system compromise.
4. Remove or disable unneeded services and software, especially those that are network-accessible.
5. Log activities on the system:
    a. Successful user logins, including the location from which the logins originated,
    b. Unsuccessful login attempts, including the location from which the attempts originated,
    c. Unsuccessful file access attempts, and
    d. Successful file accesses for files and databases containing sensitive information.
6. Disable or secure remote access from system-to-system (e.g., rlogin).
7. Proactively seek out and apply vendor-supplied fixes necessary to repair security vulnerabilities, within a timeframe commensurate with the level of risk (i.e., within 24 hours for high-risk, with 48 hours for medium-risk, and within 72 hours for low-risk).

8. Encrypt stored sensitive data where possible to minimize disclosure if the system is compromised.
9. Encrypt sensitive data being transmitted to-and-from the system where possible to ensure the data is protected in transit.
10. Deploy encrypted communications methods (e.g., Secure Shell) for user access to the system and for access via privileged accounts (e.g., "root") from other than the console.
11. Technically limit access to local network addresses where possible (e.g., TCPWrappers) given the function or process being supported.
12. Scan computers for security vulnerabilities using available technical tools:
    a. regularly, at least every 30 days to ensure new vulnerabilities are identified promptly,
    b. immediately after installation/configuration of a new system is completed,
    c. immediately after introduction of a new operating system or an upgrade to a current operating system, and
    d. immediately after installation or upgrade of networking or other system software.
13. Install and maintain anti-virus software on operating systems for which Indiana University has licensed such software, and maintain current virus pattern files.
14. Subscribe to vendor and other advisory services applicable to the operating environment being maintained.
15. Periodically visit the web site of the UISO to view current bulletins or to obtain recent security guides and other related material.
16. Provide access to only those persons who are otherwise eligible to use Indiana University technology resources, and require all users be identified and authenticated before access is allowed.
17. Limit access to needed services to only authorized persons.
18. Use different passwords for privileged accounts ("root", for example) on various systems being maintained by the same technician(s).
19. Where technically practicable, use two-factor authentication for privileged access (i.e. “root”, or system administrator access) to servers, applications, and network infrastructure. (For guidance, see KB article – At IU, what options are available for implementing two-factor authentication for privileged access to servers, applications, and network infrastructure.)
20. Perform day-to-day work as a non-privileged user and only use privileged accounts for tasks that require additional capabilities.
21. Ensure that all accounts require a password, and if technically possible, that there are automatic routines (dictionaries, pattern enforcers, etc.) that force the user to choose a good password initially and each time the password expires.
22. Implement a system such that all re-usable passwords are not sent over the network in clear-text, where technically possible.
23. Securely remove data from media once that data and/or device is no longer required, in order to prevent unauthorized disclosure of the data.

Intrusion attempts, security breaches, or other technical security incidents perpetrated against University-owned computing or other information technology resources either attached to an Indiana University-operated telecommunications network or freestanding in a University office must be reported to the Incident Response team. Functional unit managers and/or technicians must:

1. Report any successful security breaches in order to obtain assistance, advice, or (minimally) for file in the central incident database.
2. Report any systematic unsuccessful attempts (e.g., login attempts, .probes. or .scans.).
3. Where feasible given the circumstances, reports should be sent as soon as the situation is detected; minimally the report should be sent as soon as possible thereafter.

Upon receiving a report of a security incident, the UIPO Incident Response Coordinator will:

1. Ensure that appropriate information is collected and logged per applicable procedures.
2. Immediately assess actual or potential disclosure or inappropriate access to institutional or personal information.
3. Report the situation to the University Information Policy Officer and/or the University Information Security Officer.
4. Consult with and/or assign the incident to an UISO security engineer for further investigation as necessary.
5. Provide preliminary advice or comment to the functional unit technician as required.
6. Initiate steps to warn other Indiana University technicians if it appears that the situation has the potential to affect other University systems as well.
7. Perform or assist in any subsequent investigation and/or perform computer forensics as required.

Upon receiving a report of a security incident, the University Information Policy Officer and/or University Information Security Officer will:

1. If circumstances dictate, report to the Vice President for Information Technology and Chief Information Officer (VP/CIO).
2. If circumstances dictate, contact the senior manager of the department or agency involved.
3. If circumstances dictate, report and/or consult with Internal Audit, University Counsel, University Police, or other appropriate agencies.
4. Ensure that appropriate records are filed.
5. Confirm actual or probable disclosure or inappropriate access to institutional or personal information.
6. Invoke formal incident response procedures commensurate with the situation.

The functional unit managing a system that has been compromised is ultimately responsible for making the determination if the system will be only restored and operations resumed, or if pursuit of the perpetrator is feasible and appropriate based on possible continued affect on operations. Such investigation may be requested by law enforcement, and University Counsel must be consulted to see if any such request is legally binding before a contrary decision is made to only recover the system and restore the service.

The functional unit managing a system that has been compromised is responsible for all monetary, staff, and other costs related to investigations, cleanup, and recovery activities resulting from the compromise, response, or recovery.

In order to protect University data and systems, as well as to protect threatened systems external to the University, the University Information Policy Officer or 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 the use of 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 affect on University functions caused by the restriction approaches or exceeds risk associated with the threat, as negotiated between the affected constituents and the Information Policy Officer or Information Security Officer.

In order to protect University data and systems, as well as to protect threatened systems external to the University, the University Information Policy Officer or 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 points to the system as having 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 where 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 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 Information Policy Officer or Information Security Officer.

Reports of security incidents should be sent to it-incident@iu.edu.

Technology policies can be found at the Web site of the University Information Policy Office

Security resources and other security-related materials can be found at the Web site of the University Information Security Office.

The UISO operates during normal business hours. For situations after hours, contact your local campus computing support centers or help desks and ask them to page the UISO, which monitors pages 24x7. A response from UISO should be expected with 15-30 minutes. If other methods fail to reach the UIPO or UISO within 30 minutes, contact the Bloomington Data Center Operators at 812-855-9910 and ask them to page the UISO.

Definitions

Indiana University Information Technology Resources or systems includes all University-owned computers, peripherals, and related equipment and software; voice communications infrastructure, peripherals, and related equipment and software; data communications infrastructure, peripherals, and related equipment and software; and all other associated tools, instruments, and facilities. Included in this definition are classroom technologies; computing and electronic communication devices and services, including modems; electronic mail; phones; voice mail; facsimile machines, multimedia and hyper media equipment and related supporting devices or technologies. The components may be individually controlled (e.g., assigned to an employee) or shared single-user or multi-user, and they may be stand-alone or networked.

Security breach:
any successful unauthorized access to an Indiana University computer or system or network.

University-owned computing resources
computer and computer-related equipment acquired and maintained all or in part by funds through Indiana University.

Systematic unsuccessful attempts
continual probes, scans, or login attempts, where the perpetrators obvious intent is to discover a vulnerability and inappropriately access that device.

University Information Policy Office (UIPO):
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):
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.

Incident Response Coordinator/team:
a UIPO function that receives, triages, resolves, assigns, and tracks incidents of technology abuse or security breaches for all Indiana University campuses. This staff coordinates with many various University offices as well

as with external internet service providers, complainants, and law enforcement. Reports sent to it-incident@iu.edu automatically generate an incident entry in the UIPO database, and are handled by the IRC staff.

Response commensurate with the risk to operations and data:
service manager and technician reaction to a reported security vulnerability should directly correspond to the potential for damage to the local system (or adjacent systems) or inappropriate disclosure or modification of data:

1. Very High Risk . response should be immediate:
    a. Damage to the system or data is occurring, or
    b. Attempts to exploit the vulnerability on that system are occurring, or
    c. The vulnerability is currently being actively exploited against other similar technologies within the University; damage to systems and data is being experienced in those other incidents.
2. High Risk . response should be within 24 hours:
    a. The vulnerability is known to exist on the system;
    b. the exposure is currently being actively exploited against other similar technologies external to the University;
    c. damage to systems and data is being experienced in those other incidents.
3. Medium Risk . response should be within 48 hours:
    a. The system is susceptible to the vulnerability given that the system is configured incorrectly;
    b. the exposure is currently being actively exploited against other similar technologies external to the University;
    c. there is some potential for damage to systems and data.
4. Low Risk . response should be within 72 hours:
    a. The system is susceptible to the vulnerability given that the system is configured incorrectly;
    b. the exposure is currently being actively exploited against other similar technologies external to the University;
    c. damage to systems and data is possible but is not considered likely

History

- 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

IT-12.1 Mobile Device Security Standard