Privacy of Electronic Information and Information Technology Resources

IT-07

About This Policy

Effective Dates:
01-31-2008

Last Updated:
08-17-2011

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 authorized users of Indiana University information technology resources, irrespective of whether those resources or data are stored on or accessed from on-campus or off-campus locations. Unauthorized users are not protected by this policy.

Policy Statement

Stored electronic files and voice and data network communications may not be accessed by someone other than:

- the person to whom the account in which the information has been stored is assigned; or
- the person from whom the communication originated, or to whom the communication was sent; or
- the person to whom the device containing the stored electronic files has been assigned;

except in certain limited circumstances in which access is appropriate to serve or protect other core values and operations within the university as outlined in this policy. In accessing or granting access to electronic information and information technology resources, university personnel will comply with all applicable laws and university policies.

Reason For Policy

Indiana University cherishes the diversity of values and perspectives inherent in an academic institution and is therefore respectful of intellectual freedom and freedom of expression. The university does not condone censorship, nor does it endorse the routine inspection of electronic files or monitoring of network activities related to individual use. At times, however, legitimate reasons exist for persons other than the account holder to access computers, electronic files, or data related to use of the University network, including but not limited to: ensuring the continued confidentiality, integrity, and availability of university systems and operations; securing user and system data; ensuring lawful and authorized use of university systems; providing appropriately de-identified data for institutionally approved research projects; and responding to valid legal requests or demands for access to university systems and records. This policy seeks to balance individual freedom and privacy with the need for access by persons other than the account holder when necessary to serve or protect other core values and operations within the university or to meet a legal requirement.

Procedure

This policy covers:

- Data and other files, including electronic mail and voice mail, stored on, encrypted on, or in transit to or from individual computer or voice mail accounts on:
- University-owned systems/devices, or systems/devices managed by the university on behalf of affiliated organizations (e.g. Indiana University Foundation or Indiana University Alumni Association);
- University-owned computers assigned to a specific individual or group for use in support of job functions;
- University data and other university files on personally owned devices;
- Telecommunications (voice and data) traffic from, to, or between any devices described above or connected to the Indiana University technology infrastructure.

1. **Access by technicians and administrators that requires authorization**

A technician or administrator may access or permit access to specific information technology resources and electronic information as defined in this policy, in any of the following circumstances, if the technician or administrator:

1. a. **Permission Granted by Owner** - receives a written authorization from the individual to whom the account or device or communication has been assigned or attributed; or
   b. **Violations of Law or Policy** - receives a written authorization from the appropriate campus Chancellor, Provost, Human Resources Director, or Dean of Students (or equivalent) for situations where there is reasonable belief that the individual to whom the account or device is assigned or owned has engaged, is engaging, or imminently intends to engage, in illegal activities or violations of university policy using the account or device in question; or
   c. **Critical Operational Necessity** - receives a written authorization from the senior executive officer of a department for situations in which retrieving the material is critical to the operation of the department and when the account holder is deceased, terminated, incapacitated, unavailable, or unwilling to provide access; or
   d. **Deceased or Incapacitated Individual** - receives a written authorization from the senior executive officer of a department or school who has consulted with the campus Human Resources Director, Vice Provost or Vice Chancellor of Faculty & Academic Affairs (or campus equivalent), or Dean of Students to provide access to a lawful representative (e.g., spouse, parent, executor, holder of power of attorney) of a deceased or incapacitated employee, faculty member, or student; or
   e. **Internal Audit Need** - receives a directive from the Director of Internal Audit for information relating to specific audits or investigations; or
   f. **Response to Lawful Demand** - receives authorization from the Office of General Counsel confirming that access is required under the terms of a valid subpoena, warrant, other legal order, or contract, or an applicable law, regulation, or university policy; or
   g. **Substantial University Risk** – receives an authorization (written, or verbal with written confirmation) from the appropriate campus Chancellor, Provost, Vice President, or equivalent approving access after concluding that access is needed to address an emergency or to avoid or minimize exposure of the university to substantial risk of harm or liability;
   h. **Institutionally Approved Research** – receives written authorization approving access from the Institutional Review Board, any other applicable research administrative office(s), and/or the Office of General Counsel after concluding that such access is needed in support of an institutionally approved research project and the access complies with applicable laws and University policies, including rules governing the protection of human research subjects.

2. **Notification**

   A technician or administrator accessing information covered by this policy shall make reasonable efforts to report such access to the affected individual prior to that access, except:

- when prior notification is not appropriate or practical due to the urgency of the circumstances;
- when such notice may result in destruction, removal, or alteration of data; or
- when other circumstances make prior notice inappropriate or impractical.

Where prior notification is not appropriate or practical, reasonable efforts will be made to notify the affected individual as soon as possible following access unless other circumstances make follow-up notification inappropriate.

3. **Preservation of electronic information and of information technology resources**

   The copying and secure storage of the contents of an individual's email, other computer accounts, office computer, or transient network traffic to prevent destruction and loss of information may occur

   a. upon receiving credible notification of a university or law enforcement investigation for alleged illegal activity or violations of university policy on the part of a member of the university community; or
   b. upon receiving advice by the Office of General Counsel that such copying and storage is otherwise needed in order to comply with legal obligations to preserve electronic information or secure information technology resources; or
   c. upon receiving authorization from the campus Chancellor, Provost, Vice President or equivalent indicating that such preservation reasonably appears necessary to protect university operations; or
   d. when there is a reasonable belief illegal activity or violations of university policy have occurred, are occurring, or are imminently about to occur.

   Access to such copies and stored materials shall be in accordance with this policy. Preserved materials that are no longer needed must be destroyed in a secure manner.

4. **Access by technicians and administrators that does not require further authorization**

   Technicians or administrators do not require further authorization, within the scope of their legitimate university responsibilities, in any of the following circumstances:

   a. **Emergency Problem Resolution** - Technicians may access, and permit access to, information technology resources and electronic information in emergency situations, when the technician has a reasonable belief that a program or process active in the account or on the device is causing or will cause significant system or network degradation, or could cause loss/damage to a system or other users' data. This includes forensic and/or other analysis in response to a security incident, sensitive data exposure, or system/device compromise.
   b. **Collaborative Information or Resources** - Technicians may access, and permit access to, for legitimate purposes, information technology resources and electronic information that by their nature are not private, such as shared computers and shared document folders.
   c. **System-generated,** Content-neutral Information – Technicians may access and use system-generated logs and other content-neutral data describing the use of technology for the purposes of analyzing system and storage utilization, problem troubleshooting, and security administration, and in support of audits. Technicians may **not** disclose or permit access to specific information technology resources assigned to, or electronic information associated with, an individual except as authorized under Section 1 above.
   d. **Incident Response** - The incident response function within the University Information Policy Office (UIPO) is responsible for investigating reports of abuse or misuse of university information technology resources. Incident response staff may use system-generated, content-neutral information for the purposes of investigating technology misuse incidents, and in support of audits. Incident response staff may **not** disclose or permit access to specific information technology resources assigned to, or electronic information associated with, an individual except as authorized under Section 1 above.
   e. **Network Communications** - Security engineers of the University Information Security Office (UISO) may observe, capture, and analyze network communications. "Network communications" may contain content

data and in some cases this content may be viewed to complete analysis. If any data must be stored to complete the assigned tasks, it will be stored securely and deleted as soon as possible. Security engineers may **not** disclose content or log data to other persons except as authorized under Section 1 above.

f. **Implied Consent** – Technicians may access, and permit access to, information technology resources and electronic information in situations where a user has requested assistance diagnosing and/or solving a technical problem or where the technician is performing required maintenance or troubleshooting. In these cases, technicians should strive to limit the scope of the access to that which is necessary to address the problem.

5. **Other Provisions**

a. **Advice and Interpretation** - The Chief Information Policy Officer in the Office of the Vice President for Information Technology represents the University CIO for privacy issues related to the IU Bloomington and IUPUI campuses, and is also available to provide advice and policy interpretation to campus CIOs, department management, and any member of the Indiana University community. Technicians receiving requests for access to computer accounts, files, or network traffic by persons other than the account holder, who are not sure how to handle that request within the provisions of this policy, will consult with the Chief Information Policy Officer or the appropriate campus Chief Information Officer (CIO) prior to granting the access.

b. **Legal Requests** - All legal requests or demands for access to information technology resources or electronic information, including all requests under the Indiana Access to Public Records Act and all subpoenas, warrants, court orders, and other legal documents directing that access be afforded to law enforcement agencies or others, must be delivered immediately to the Office of General Counsel. Should such documents be served on individual system technicians or other persons, the documents must be sent immediately to the Office of General Counsel for review. Counsel will review the request or order, and advise the relevant personnel on the necessary response. In the event that a law enforcement agency seeks to execute a search warrant or other order immediately and will not wait for review by the Office of General Counsel, individual system technicians or other persons receiving such orders should not obstruct the execution of the warrant or order, but should document the actions by law enforcement, notify the Office of General Counsel as soon as possible, and take reasonable steps whenever possible to preserve a copy of any data being removed, for appropriate university use.

c. **Expectation of Privacy** - Although the university seeks to create an atmosphere of privacy with respect to information and information technology resources, users should be aware that because IU is a public institution, and members of the University community are engaged in institutional and academic research projects that may require access to certain de-identified user data, and because the university must be able to ensure the integrity and continuity of its operations, use of the university's information resources cannot be completely private. For example, in addition to the types of permissible access described above, when users engage in incidental personal use of their university email accounts, the contents of their email may be subject to disclosure in response to requests under Indiana's "open records" law. Therefore, users of Indiana University information technology resources are hereby notified that they should have no expectation of privacy in connection with the use of those resources beyond the provisions of this policy. Users should also be aware that although the university takes reasonable measures to ensure the privacy of university information technology resources, the university does not guarantee privacy.

d. **Initiating Access** - Persons seeking access to specific information technology resources and/or electronic information assigned to or associated with an individual, that are maintained by University Information Technology Services (UITS), must send those requests to it-incident@iu.edu. Acting for the University CIO, the University Information Policy Office (UIPO) is responsible for ensuring adherence to proper policy and procedures and will coordinate any subsequent approved access.
Persons seeking access to specific information technology resources and/or electronic information assigned to or associated with an individual, that are **not** maintained by University Information Technology Services (UITS), should direct those requests to the technology director of the unit maintaining those resources (on the Bloomington or IUPUI campuses), or the appropriate campus CIO (on the regional campuses). Campus CIOs and unit technology directors are encouraged to consult with the UIPO as needed.

"Persons seeking access" includes system or database administrators or other technicians who need such access to perform their university responsibilities, or who receive requests from others to access those resources or information.

Definitions

Authorized users are people acting within the scope of a legitimate affiliation with the university, using their assigned and approved credentials (ex. network IDs, passwords, or other access codes) and privileges, to gain approved access to university information technology resources. A person acting outside of a legitimate affiliation with the university or outside the scope of their approved access to university information technology resources is considered an unauthorized user. Content-neutral information is information relating to the operation of systems, including information relating to interactions between individuals and those systems. Such information includes but is not limited to operating system logs (i.e., record of actions or events related to the operation of a system or device), user login records (i.e., logs of usernames used to connect to university systems, noting source and date/time), dial-up logs (i.e., connections to university modems, noting source, date/time, and caller id), network activity logs (i.e., connections attempted or completed to university systems, with source and date/time), non-content network traffic (i.e., source/destination IP address, port, and protocol), email logs (i.e., logs indicating email sent or received by individuals using university email systems, noting sender, recipient, and date/time), account/system configuration information, and audit logs (i.e., records of actions taken on university systems, noting date/time). Critical operational necessity is an urgent need that is indispensable or vital to the operation of a unit. Indiana University information technology resources 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; all other associated tools, instruments, and facilities; and the services that make use of any of these technology resources. The components may be individually controlled (i.e., assigned to an employee) or shared single-user or multi-user; they may be stand-alone or networked components; and they may be stationary or mobile. This also includes university data and files whether stored on university-owned or personally owned equipment. University Chief Information Officer The primary responsibility of the University CIO is the development and use of information technology in support of the university's vision for excellence in research, teaching, outreach, and lifelong learning. The University Information Policy Office represents the University CIO with respect to policy issues related to the IU Bloomington and IUPUI campuses.

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 offices 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 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.

History

- Reviewed December 2011.
- Revised August 17, 2011: changed titles in *Sanctions* section to more accurately reflect current usage.
- Revised July 23, 2010: updated Institutionally Approved Research language.
- Revised March 4, 2010: enhancing language in *Sanctions* section
- Updated procedures section for "Persons affiliated with external entities collaborating with Indiana University" to match academic no-pay process — September 23, 2008

- (1) Updated Alumni email eligibility to reflect new Alumni Association service — March 2, 2007
- Revised March 12, 2006
- Approved May 23, 2006
- Posted as an interim policy November 15, 2000

Related Information

IT-07 Frequently Asked Questions