

Privacy for Electronic Information

POLICY V.1.3

Volume V, Information Technology

Chapter 1, Data Security

Issuing Office: OVPIT

Responsible Officer: VPIT

Responsible Office: OVPIT

Originally Issued: May 25, 2005

Revised:

Table of Contents

Reason for Policy.....	1
Statement of Policy.....	2
Procedures.....	4
Who Should Know This Policy.....	5
Related Documents.....	5
Contacts.....	5
Definitions.....	6
Compliance.....	7

Reason for Policy

The right to privacy is a deeply held conviction, especially within intellectual and academic communities. Privacy is critical to the intellectual freedom that forms the foundation of higher education. While the right to individual privacy is highly valued in the University community, it must, however, be balanced with legal obligations and the larger needs of the community.

Although Purdue University seeks to create, maintain, and protect the privacy of electronic information on its IT Resources, users should be aware that the use of Purdue's IT Resources is not completely private. Accordingly, users of Purdue's IT Resources are hereby specifically notified that they have no expectation of privacy in connection with their use of such IT Resources. Except as provided in this policy, Purdue University does not routinely monitor the content of communications or transmissions using IT Resources. The normal operation and maintenance of the University's IT Resources require the back up and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities. There are also special circumstances such as illness; death; violation of University policies, regulations procedures or rules; or illegal activity which may warrant intrusive or restrictive action within an individual's computer account and/or devices.

The purpose of this policy is to outline the special circumstances under which the University may access content or electronically stored wire and electronic communications and information on its IT Resources in order to protect its legitimate business and academic Interests. Those legitimate business and academic Interests include Purdue's need to ensure that it can, without limitation, operate and maintain its IT Resources as well as protect the integrity, security, or functionality of University IT Resources; protect the University's other property, rights, and resources; ensure compliance with University policies, procedures, or regulations; preserve the integrity and reputation of the University; safeguard the property, rights, and data of third parties; and comply with applicable law.

Statement of Policy

Scope

This policy covers students, faculty, staff, and any and all individuals or entities using any Purdue IT Resources and all uses of such IT Resources. Any individual or entity using Purdue IT Resources consents to all of the provisions of the following policy and agrees to comply with all of the terms and conditions set forth herein, all other applicable University policies, regulations, procedures and rules, and with applicable local, state, and federal law and regulations.

Violations of this policy or any other University policy or regulation may result in the revocation or limitation of IT Resource privileges as well as other disciplinary actions or may be referred to appropriate external authorities.

This policy covers the following types of information at all Purdue campuses:

1. Data, e-mail, and voice mail stored in IT Resources, including without limitation, computer accounts on University-owned systems or other University-owned Devices.
2. Data, e-mail, and voice mail stored in computer accounts or other Devices managed by the University on behalf of an associated organization; for example, the Purdue Research Park.
3. Voice and data telecommunications traffic to, from, or between IT Resources, including without limitation any of the Devices listed above.

Policy statement

In general, the types of information enumerated above are considered private and cannot be accessed by someone other than the person to whom the IT Resource account has been assigned, the person from whom the information originated, or the person to whom the Device has been assigned. Furthermore, as noted above, Purdue University does not routinely monitor the content of communications or transmissions using IT Resources. The University does, however, specifically reserve the right, with or without notice, to intercept, access, monitor, inspect, copy, store, use, or disclose the contents of communications or transmissions employing IT Resources when it reasonably believes these actions are appropriate in order to protect its Interests.

More specifically, and without limiting the foregoing general rights, the University reserves the right to monitor and inspect computer accounts and Devices as warranted by the need to protect the information and services held on University IT Resources and any legal obligations that arise, and the University may, without notice, use: (a) security tools designed to locate security flaws in equipment connected to IT Resources; (b) network monitoring hardware and software that capture the contents of packets traversing the network; (c) network hardware and software designed to protect IT Resources and users

Privacy for Electronic Information

POLICY V.1.3

Volume V, Information Technology
Chapter 1, Data Security
Issuing Office: OVPIT
Responsible Officer: VPIT
Responsible Office: OVPIT
Originally Issued: May 25, 2005
Revised:

of IT Resources, including without limitation Anti-Phishing Services, Anti-Virus Services, Intrusion Detection Systems, Spam Filtering Services, and Anti-Spyware Services; or (d) system log information, including without limitation source and destination for a connection, session start and end times, login name, timestamps, and commands issued. In addition, and again without limiting the above-enumerated general right to act when it reasonably believes these actions are appropriate in order to protect its Interests, the University may, acting through University-authorized technicians and administrators and pursuant to the procedures specified herein, access or permit access to the contents of communications or electronically stored wire and electronic communications and information employing IT Resources if it:

- Has a reasonable belief that a process active in the account or device is causing or may cause significant damage to University IT Resources or could cause loss/damage to user, University, or third-party data.
- Receives a written request from federal, state, or local law enforcement agencies and complies with applicable University policies.
- Has a reasonable belief that an individual has or is violating University policies, regulations, procedures, or rules using the accounts or Devices in question.
- Determines that a staff member, faculty member, or student is deceased, has been terminated, or is otherwise unavailable for the purposes of retrieving information that is critical to the operational effectiveness of the department.
- Receives a written request from the Office of the Dean of Students on behalf of the parents, guardian, or personal representative of the estate of a deceased student.
- Receives a written request from the Purdue Director of Audits when Internal Audit is investigating fiscal misconduct linked to the user whose account or Device is in question.
- Is authorized by an appropriate order of a court of competent jurisdiction and complies with applicable University policies relating to the handling of such orders.

Again, without limiting the foregoing general rights, the University may, in its sole discretion, disclose the results of any general or individual monitoring or accessing permitted hereunder, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies or use those results in appropriate University disciplinary proceedings. Where applicable and warranted, the account or equipment user will be notified of the accessing or monitoring and the corrective actions taken.

The contents of the user's e-mail, computer accounts, Devices, and network traffic may be recorded and stored to prevent destruction should the information be requested pursuant to valid legal process.

All users of University IT Resources, as a condition to the use of University IT Resources, specifically consent to the general rights of Purdue University specified herein.

Procedures

Except for monitoring of activity and accounts of individual users of University IT Resources when the user has voluntarily made them accessible to the public, or where the University has reserved the right to do so without notice or by policy, any access to the contents of communications or electronically stored wire and electronic communications and information employing IT Resources permitted under this policy must, in addition to any requirements specified herein, be authorized as follows:

1. A dean, in the case of an academic unit, a vice president in the case of an administrative unit, and/or a chancellor in the case of a regional campus shall have made a written finding prior to such access that the access is reasonably required in order to protect the University's Interests and shall have forwarded such written finding to the Office of the Vice President for Information Technology.
2. The official designee of the Office of the Vice President for Information Technology shall have made a written finding prior to such access that: (a) the access is reasonably required in order to protect the University's Interests, and (b) authorizes the requested access and specifies the scope and conditions of any permitted access. These written findings shall be maintained by the Office of the Vice President for Information Technology.
3. Notwithstanding the foregoing, the Vice President for Information Technology or his or her designee may authorize access in the event that he or she reasonably determines that: (a) there exists an emergency that materially threatens the University's Interests, (b) that emergency access is reasonably required in order to protect the University's Interests, and (c) he or she specifies the scope and conditions of any permitted access. The OVPIT shall, as soon as reasonably possible after such emergency, make a written finding verifying the existence and satisfaction of the foregoing conditions.

Any access permitted hereunder shall be the minimum access required in order to protect the University's Interests.

In all cases, technicians and administrators who receive requests from law enforcement or other outside agencies seeking access to computer accounts, files, or network traffic of an IT Resource user shall forward such requests to the appropriate and responsible Purdue department (which may include without limitation the Purdue Police Department, Public Information Officer, Office of the Dean of Students, or the Employee Relations/Human Resource Policy department as appropriate) in accordance with applicable Purdue policy. In all cases, technicians and administrators will obtain written documentation of any requests made before accessing or permitting access to an individual's electronic information resources.

Who Should Know This Policy

President	Business Office Staff
Provost	Faculty
Executive Vice President & Treasurer	Administrative and
Chancellors	Professional Staff
Vice Presidents	Clerical and Service Staff
Deans	All Employees
Directors / Department Heads /	Undergraduate Students
Chairs	Graduate Students
Principal Investigators	

Related Documents

Laws that influence and affect this policy include but are not limited to:

COPPA	http://www.ftc.gov/coppa/
DMCA	http://www.copyright.gov/legislation/dmca.pdf
ECPA	http://www.access.gpo.gov/uscode/title18/parti_chapter119_.html
FERPA	http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
GLBA	http://www.ftc.gov/privacy/glbact/
HIPAA	http://www.hhs.gov/ocr/hipaa/
USA Patriot Act	http://www.lifeandliberty.gov/

Notice of Privacy Practices for Purdue's Health Plans as required by HIPAA

http://www.purdue.edu/oop/policies/pages/records/vi_2_1_healthplan.html

Purdue delegation of authority for information awareness and security

http://www.purdue.edu/oop/policies/pages/information_technology/v_1_1.html

Contacts

For questions about this policy, contact IT Security and Privacy, itap-securityhelp@purdue.edu

Definitions

Word	Definitions
Anti-Phishing Services	Services designed to protect users from techniques used to gain personal information for purposes of identity theft, using fraudulent e-mail messages and Web pages that appear to be the property of legitimate businesses. These authentic-looking messages and Web pages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers, and Social Security numbers.
Anti-Spyware Services	Services designed to protect users from software that covertly installs itself, gathers information without the user's knowledge, and transmits this information to a third party, usually over the Internet.
Anti-Virus Services	Services designed to protect a server or other computer from known or potential computer viruses.
Device(s):	Any mechanism used to store, retrieve, manipulate, or transfer data such as a disk drive, compact disk, personal digital assistant, or cellular phone.
Interests	The legitimate business and academic rights and responsibilities of the University. These include, but are not limited to, protecting the University's IT Resources, other property, rights, and resources; ensuring compliance with University policies, procedures, or regulations; preserving the integrity and reputation of the University; safeguarding the property, rights, and data of third parties; and complying with applicable law.
Intrusion Detection	Software and/or hardware designed to detect inappropriate or anomalous activity on a computer or a data network.
IT Resource	All tangible and intangible computing and network assets provided by the University to further its mission of discovery, learning, and engagement. Examples of such assets include, but are not limited to, hardware, software, Purdue Airlink, network bandwidth, mobile devices, electronic information resources, printers, and paper.
Spam Filtering Services	Services based on software and or hardware designed to detect unsolicited and unwanted e-mail and to prevent those messages from getting to a user's inbox.

Compliance

- If a technician, administrator, or other individual accesses electronic information without proper authorization as outlined in this policy, the individual is subject to disciplinary action up to and including termination.
 - If an individual suspects that his or her electronic information has been compromised he or she should report the incident to abuse@purdue.edu.
 - Nothing in this policy changes or supersedes Executive Memorandum No. C34 regarding Data Security and Access Policy, Executive Memorandum No. C-2 regarding Disclosure of University Records, or Executive Memorandum No. B-44 regarding the Family Educational Rights and Privacy Act.
-