

Incident Response

POLICY V.1.4

Volume V, Information Technology
Chapter 1, Data Security
Issuing Office: OVPIT
Responsible Officer: VPIT
Responsible Office: OVPIT
Originally Issued: May 17, 2005
Approved: March 9, 2006

Table of Contents

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

Reason for Policy

A formal policy for the reporting of and response to IT Incidents is necessary to ensure the secure operation of IT Resources, to protect the data security and privacy of students, faculty, and staff, and respond appropriately to IT Incidents.

This policy sets forth a set of general requirements for the efficient response to IT Incidents in order to maintain the security and privacy of IT Resources, data and other assets, as well as satisfy requirements of state and federal law.

Definitions

Word

Definition

IT Incident:

Any event involving University IT Resources which:

- violates local, state or U.S. federal law, or
 - violates regulatory requirements which Purdue is obligated to honor, or
 - violates a Purdue University policy, or
 - is determined to be harmful to the security and privacy of University data, or IT Resources associated with, students, faculty, staff and/or the general public, or
 - constitutes harassment under applicable law or University policy, or
 - involves the unexpected disruption of University services.
-

- CIR:** The CIR, or Coordinator of Incident Response is the party responsible for managing University-wide IT Incident response. The IT Security and Privacy office, under OVPIT, currently fulfills the role of CIR.
- CIRT:** A CIRT, or Computer Incident Response Team, is a group of skilled individuals designated to respond to any IT Incident which requires coordination across multiple departments, or which cannot in the reasonable judgment of the CIR be adequately addressed by a single department, or when it is otherwise determined to be appropriate to employ such a team by the CIR. The CIR is responsible for defining the specific procedures for and operations of CIRTs.
- PSC:** Purdue Security Contact is the person or persons assigned to coordinate IT Incident response for an individual business unit, college/school, or department. The PSC is responsible for interacting with the CIR.
- IT Resource** All tangible and intangible computing and network assets provided by or for 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.
- IP Address:** Internet Protocol Address. A unique numerical address that identifies computers connected to the Internet or other IP networks.
- Reporter:** A person who notifies the CIR of an event he or she believes to be an IT Incident.

Statement of Policy

Classification

In order to facilitate the accurate and productive response to IT Incidents, all IT Incidents must be classified and assessed by the CIR for severity at their onset. As the IT Incident progresses its classification may be reevaluated and changed as necessary to ensure proper handling.

In some cases, IT Incidents may fall under multiple classifications. When this happens, the classification with the highest severity should generally dictate the course of IT Incident response.

The CIR is responsible for providing and maintaining appropriate IT Incident classification guidelines and resolution procedures.

Reporting

Receiving Reports

Reported events become IT Incidents only after they have been received and evaluated by the CIR. All event reports should be sent first to the CIR for assessment and assignment. The CIR upon receiving a report is responsible for assessing its veracity, determining whether or not the event constitutes an IT Incident and classifying the IT Incident, and initiating handling procedures.

The CIR reserves the right, per the Delegation of Administrative Authority and Responsibility For Information Assurance, Security and Awareness (policy V.1.1) and subject to applicable law and other applicable University policies, to use the following resources for IT Incident detection and/or response:

1. System and application logs
2. Passive network traffic monitoring (e.g., IDS, and other network packet analyzers)
3. Active scanning of systems suspected of violating university policy, or systems exhibiting symptoms of compromise
4. Other resources as determined appropriate by the CIR and as allowed by Purdue policy and applicable law.

To facilitate accurate reporting, handling, and record keeping, the CIR is responsible for providing a protocol by which the CIR, PSC, and Reporters of potential IT Incidents can communicate. The CIR should also maintain a record of communication and data collection for all events reported to the CIR. In addition, the CIR is responsible for providing a formal operations guide. This guide shall outline the specific processes and methods for handling IT Incidents.

Reporting Incidents

When any event is observed which appears to satisfy the definition of an IT Incident, it must be reported to the CIR. If it is unclear as to whether or not an event constitutes an IT Incident, such an event should be sent to the CIR for evaluation. Events that may constitute an IT Incident may be reported to the CIR via email at abuse@purdue.edu. The person who reports the event, including complaints relayed on behalf of customers, should document and report any available relevant information about the event, including, but not limited to dates, times, persons/resources involved, and IP addresses.

The CIR is responsible for publishing all IT Incident reporting guidelines and additional contact information. Absent these guidelines, all events that may constitute IT Incidents should be reported directly to the CIR via abuse@purdue.edu.

Situations which are suspected to be crimes should be reported immediately to the appropriate law enforcement agencies by the person who possesses first-hand knowledge of the facts or circumstances related to a suspected crime. Those events which are suspected to be both a crime and an IT Incident should be reported first to the appropriate law enforcement agencies, and then a notification that a police report has been filed should be sent to the CIR. However, it should be noted that in such situations the CIR would not generally act on the report unless asked to do so by said law enforcement agencies.

Incident Response

POLICY V.1.4

Volume V, Information Technology
Chapter 1, Data Security
Issuing Office: OVPIIT
Responsible Officer: VPIT
Responsible Officer: OVPIIT
Originally Issued: May 17, 2005
Approved: March 9, 2006

Purdue students, faculty, and staff should report crimes to the Purdue University Police Department. Those persons external to the University should report crimes to their local law enforcement agency.

Response

After receiving a report, assessing its veracity, determining whether or not the event constitutes an IT Incident, and classifying the IT Incident, the CIR will determine if the IT Incident warrants a formal response. IT Incidents that do not warrant formal response will be remanded to the appropriate PSC for handling. All reported events or IT Incident must be documented throughout the response process.

If an event report does warrant formal IT Incident response procedures by the CIR, it is the responsibility of the CIR to coordinate the appropriate resources for such response. If deemed appropriate by the CIR, a CIRT will be formed and led by the handler assigned to the IT Incident.

The CIR is responsible for documenting appropriate procedures for responding to event reports and IT Incidents, and coordinating CIRTs.

Business Continuity

In the course of responding to an IT Incident it may be necessary, subject to applicable laws and University policies, to require the suspension of involved or targeted services/systems in order to:

- Protect students, faculty, staff, IT Resources, other systems, data, and University assets from threats posed by the involved services/systems
- Protect the service/system in question
- To preserve evidence and facilitate the IT Incident response process

The decision to suspend operations will be made by the CIR, as designated by the Vice President for IT per Information Technology policy V.1.1, Delegation of Administrative Authority and Responsibility for Information Assurance, Security, and Awareness.

In the case of mission critical applications, the CIR will make a good-faith effort to consult with the appropriate PSC, and if available, service/application owner before such suspensions are carried out. If, in the judgment of the CIR an excessive amount of time (giving due weight to the relative severity of the IT Incident) has passed without response from the appropriate PSC or service/application owner, suspension may occur without consultation. In other cases, the appropriate PSC will be notified of suspension of service.

Any equipment not owned by the University which is using University IT Resources, and is found to be the target, source, or party to an IT Incident may be subject to immediate suspension of services without notice until the issue has been resolved, or the subject system is no longer a threat.

In all cases, it is the CIR who shall determine if and when a service suspension may be lifted.

Incident Response

POLICY V.1.4

Volume V, Information Technology
Chapter 1, Data Security
Issuing Office: OVPIT
Responsible Officer: VPIT
Responsible Office: OVPIT
Originally Issued: May 17, 2005
Approved: March 9, 2006

In order to facilitate proper and timely handling of IT Incident responses, it is necessary that network-connected devices can be identified and located as soon as possible. To this end, PSCs are required to maintain an inventory of network-connectable devices under their control, per guidelines to be established by the CIR. Absent these guidelines, PSCs are required to maintain a list of all such devices which includes, at a minimum, the primary location of the device, and the physical addresses for all network interfaces used by the device (i.e., MAC address).

Scope

This policy covers students, faculty, staff, 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 preceding 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 and may be referred to appropriate external authorities.

Regional Campuses

Regional campuses are required to institute their own IT Incident response plan and procedures in accordance with this policy. This includes providing a single electronic mail address to report regional campus-specific events that may constitute IT Incidents¹, as well as the appropriate procedures for handling these events.

Who Should Know This Policy

President
Provost
Executive Vice President & Treasurer
Chancellors
Vice Presidents
Deans
Directors / Department Heads / Chairs
Principal Investigators

Business Office Staff
Faculty
Administrative and
Professional Staff
Clerical and Service Staff
All Employees
Undergraduate Students
Graduate Students

¹ This abuse email address should be listed as the AbuseEmail and OrgAbuseEmail fields of the ARIN records for all IP blocks owned by each campus.

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/

Delegation of Administrative Authority and Responsibility For Information Assurance, Security and Awareness

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

Contacts

For questions about this policy, contact IT Security and Privacy, abuse@purdue.edu

Procedures

As mentioned in this policy, the CIR is responsible for publishing all procedures for reporting, classifying, responding to, and communication of IT Incidents.

Compliance

Failure to honor the requirements set forth in this policy may result in disciplinary or administrative action, and temporary or permanent loss of IT Resource privileges or services.