Information and Information System Incident Reporting, Management, and Breach Notification

ISPP-26

About This Policy

Effective Dates:
11-02-2012

Last Updated:
08-27-2012

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:

- information – whether in printed, verbal, or electronic form – created, collected, stored, manipulated, transmitted or otherwise used in the pursuit of Indiana University's mission, regardless of the ownership, location, or format of the information.
- information systems used in the pursuit of Indiana University's mission irrespective of where those systems are located.
- individuals encountering such information or information systems regardless of affiliation.

Policy Statement

Per the procedures below, all individuals are required to ***immediately*** report to the University Information Policy Office (UIPO) any:

- suspected or actual security breaches of information – whether in printed, verbal, or electronic form – or of information systems used in the pursuit of the university's mission.
- abnormal systematic unsuccessful attempts to compromise information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission.
- suspected or actual weaknesses in the safeguards protecting information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission.

The UIPO will:

- oversee and guide the incident management process to promote a coordinated, consistent, efficient, and effective response, and to ensure compliance with applicable breach notification laws and regulations, including any required notifications of individuals and/or regulatory or government officials.
- leverage and coordinate with the experience, expertise, and resources of other university offices including applicable compliance offices and officers as necessary and appropriate.

Although the UIPO will coordinate incident response, ownership of the incident remains with the unit experiencing the incident, which must allocate unit resources to resolve the incident in a timely manner.

Reason For Policy

Information – whether in printed, verbal, or electronic form – and information systems have become critical parts of the infrastructure supporting Indiana University operations and innovations. This increased dependence has occurred against a backdrop of increasing uses of information for business purposes, technological complexity, security and privacy threats, legal mandates, and ethical expectations leading to more significant operational, reputational, and financial consequences of service interruptions and unauthorized information exposures or modifications.

Yet, in spite of the most vigilant efforts to minimize them, incidents will occur that jeopardize the security and privacy of information and information systems. The institution's process of preparing for, preventing, detecting, responding to, and tracking these events has a significant impact on reducing their frequency and severity.

Legal and contractual mandates increasingly require expeditious reporting of certain breaches to regulatory or governmental authorities, ***in some cases as soon as 24 hours after discovery***, and/or to the individuals affected.

Therefore, a coordinated, consistent, efficient, and effective approach to identifying, investigating, and handling potential information and information system breaches is needed.

Procedure

Reporting

Immediately report to the University Information Policy Office (UIPO) at it-incident@iu.edu any:

- suspected or actual incidents of loss, inappropriate disclosure, or inappropriate exposure of information used in the pursuit of the university's mission – whether in printed, verbal, or electronic form – including but not limited to those incidents involving the following information, systems, or processes:
  - critical information such as individually identifiable health information, credit card numbers, Social Security numbers, driver’s license numbers, or bank account numbers.
  - lost or stolen mobile devices or media such as laptops, tablets, smart phones, USB drives, and flash drives.
  - viewing of information without a demonstrated need to know (e.g., snooping).
- abnormal systematic unsuccessful attempts to compromise information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission, such as:
  - abnormal unsuccessful login attempts, probes, or scans.
  - repeated attempts by unauthorized individuals to enter secured areas.
- suspected or actual weaknesses in the safeguards protecting information – whether in printed, verbal, or electronic form – or information systems used in the pursuit of the university's mission, such as:
  - weak authentication processes.
  - ability to access information you are not authorized to access.
  - weak physical safeguards such as locks and access controls.
  - lack of secure transport methods.

In cases where a unit has an information security, privacy, or compliance officer, incidents should be reported to both UIPO and the unit officer.

The UIPO operates during normal business hours. When identifying suspected or actual incidents after hours, contact your local campus computing support centers or help desks and ask them to page the University Information Security Office (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.

Incident Response

Upon receiving a report, the UIPO Incident Response team will:

1. Ensure appropriate information and evidence is collected and logged.
2. Immediately assess initial actual or potential loss, corruption, inappropriate disclosure, inappropriate exposure, or breach of information.

3. Immediately advise and assist in containing and limiting the loss, corruption, inappropriate disclosure, inappropriate exposure, or breach.
4. Invoke incident response procedures commensurate with the situation.
5. As appropriate, assemble an Incident Team to advise and assist in ongoing investigation and decision making. The nature of the incident and the type(s) of information involved will determine the make-up of the Incident Team, and it typically will include representatives from the unit experiencing the incident, Legal Counsel, Media Relations, the Committee of Data Stewards, and/or the Compliance Officer for the information sector(s) involved (e.g., the HIPAA Privacy and/or HIPAA Security Officer).
6. As appropriate, ensure the University Information Policy Officer and/or the University Information Security Officer is informed of the initial situation and kept updated throughout the investigation.
7. As appropriate, ensure that executive administration is informed of the initial situation and kept updated throughout the investigation.
8. As appropriate, contact law enforcement for assistance.
9. As appropriate, consult with and/or assign a UISO security engineer to perform forensics or other specialized technical investigation.
10. As appropriate, provide technical advice to the unit technician, and ensure legal, compliance, Data Steward, media, and executive administration advice is made available to unit administration in a timely manner.
11. Initiate steps to warn other Indiana University units or technicians if the situation has the potential to affect other university information or information systems.
12. Confirm actual or probable events from investigatory information and facilitate decision-making by the Incident Team.
13. In coordination with the Incident Team members and following internal procedures, determine if notification to individuals and/or regulatory or governmental authorities is required and/or desired, and invoke breach notification procedures commensurate with the situation.
14. Ensure appropriate university approvals are obtained prior to any notifications to individuals or regulatory and government officials.
15. Document decisions and any notifications made to individuals or regulatory and government officials.
16. Schedule a debriefing meeting with the unit and Incident Team after the response, to ensure appropriate corrective action in the affected unit is taken, to identify any actions that could be taken to reduce the likelihood of a future similar incident, and to continuously improve the response processes.
17. In cases where it is found that a reported incident involves information or physical privacy concerns, UIPO will communicate with the relevant privacy official who will then invoke policy ISPP-27 Privacy Complaints as appropriate, in addition to incident response procedures.

Financing the Incident
The unit(s) experiencing the incident is/are responsible for all monetary, staff, and other costs related to investigations, cleanup, and recovery activities resulting from the compromise, response, and recovery. The unit(s) may consult with the Office of Insurance, Loss Control, and Claims as to methods for funding the incident.

Definitions

Breach the acquisition, access, use, or disclosure of information in a manner not permitted under existing law or university policy that compromises the security or privacy of the information (i.e. poses a significant risk of financial, reputational, or other harm to the individual and/or university). Health Information any information created, maintained or received, via any communication or record retention format, by any entity such as a provider, insurance plan, employer, or university that identifies an individual and any services regarding their health care or health payments relating to their past, present, or future health status. Information system a discrete set of information resources, procedures and/or techniques, organized or designed, for the classification, collection, accessing, use, processing, manipulation, maintenance, storage, retention, retrieval, display, sharing, disclosure, dissemination, transmission, or disposal of information. An information system can be as simple as

a paper-based filing system or as complicated as a tiered electronic system. Security Incident the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. Security incident also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, misrouting of mail, or compromise of physical security, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

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

- Approved November 2, 2012
- Revised March 14, 2012, June 28, 2012, and August 27, 2012.
- Edited January 12, 2012 – normalized against the Program documents.
- Drafted October 28, 2011 – breach notification requirement extracted from IT-12 and updated.

Related Information

Privacy Complaints Policy ISPP-27
Information Security and Privacy Program Domain 10 – Incident Management
Report an Incident
Reporting Security Incidents
Information Security Incident Management
Reporting Suspected Sensitive Data Exposures
Acceptable Use Agreement

Related Forms

Incident Response Procedure Template