THE OHIO STATE UNIVERSITY

Information Security Incident Response Management

University Policy

Applies to: Faculty, staff, students, volunteers, agents, contractors, and all other individuals handling institutional data on the university's behalf.

Responsible Office **Office of the Chief Information Officer**

POLICY

Issued: 01/10/2007
Revised: 4/15/2019

The Ohio State University is dedicated to providing secure networks and systems to protect all institutional data. This requires a conscious and deliberate understanding of the ever-changing threats to breach those networks and systems, especially where such breaches result in a loss of university data. Therefore, all **information security events** must be properly reported and investigated to determine whether data breaches have occurred. In the event of an **information security breach**, notification to certain individuals, agencies, or organizations is required by law, regulation, contractual agreement, industry regulation, and/or university policy. This policy provides guidance on the applicable reporting, investigation, and notification requirements.

Reporting under this policy does not release individuals from other reporting requirements that may be triggered due to contractual obligations and/or federal, state, or local law.

Purpose of the Policy

To require that information security events are reported and investigated to determine whether data breaches have occurred that trigger specific notification requirements.

Definitions

Term	Definition
Data Incident Response Team (DIRT)	One or more teams of university representatives who determine if an information security breach has occurred and facilitate university actions. These actions include determining whether notification requirements have been triggered and which individuals, agencies, or organizations must be notified to comply with applicable laws, contractual agreements, industry regulations, or university policy. DIRT-Leadership is the DIRT leadership team who determine appropriate action. Members of DIRT and DIRT-Leadership are defined in the Information Security Incident Response Management Process.
Information security event	Any observable occurrence in the operations of a network or information technology service, system or data indicating that a security policy may have been violated or a security safeguard may have failed. See Example Information Security Events which May or May Not be a Data Breach.
Information security incident	An information security event where it is alleged or suspected that unauthorized access, use, modification, or disclosure of printed, electronic, audio or visual non-public institutional data to an **unauthorized individual or entity** may have occurred.
Information security breach	Any compromise event involving data protected by privacy or security laws, contractual agreements, or regulations that requires notification.
Information Security Incident (Security Responders)	Individuals designated by unit management to respond to information security events and who have received training by their associated Security Team. These individuals will coordinate the unit's response pursuant to their incident response plan based on the Information Security Incident Response Management Process.
Email phishing	Email scams where the attacker attempts to trick an individual into giving them their credentials or access to their system. More information can be found on the Cybersecurity webpage.

Applies to: Faculty, staff, students, volunteers, agents, contractors, and all other individuals handling institutional data on the university’s behalf.

Term	Definition
Potential Breach Notification Committee (PBC)	Committee at the Wexner Medical Center who determine if a breach of protected health information (PHI) has occurred and facilitate actions. These actions include whether notification requirements have been triggered and which individuals, agencies, or organizations must be notified to comply with applicable laws, contractual agreements, industry regulations, or university policy.
Security Team	One or more teams of individuals who investigate and substantiate an information security incident and, in conjunction with the Chief Information Security Officer, determine whether a Data Incident Response Team or Potential Breach Notification **Committee** should be convened. Also known as the University Incident Review Team.
Unauthorized individual or entity	An individual or entity that accesses non-public institutional data where such access is not required or authorized in the course of university employment or to perform duties authorized by the university.

Policy Details

I. This policy establishes the university’s committment to respond to information security events, which include **information security incidents** and information security breaches.

II. The university strives, through this policy, to provide its faculty, staff, students, volunteers, agents, contractors, and all other individuals handling institutional data on the university’s behalf with clear direction for proper reporting, response, and notification in the event of an information security event, incident, or breach.

III. The Chief Information Security Officer or their appointed designees will manage this Information Security Incident Response Management policy and its derivative works, such as the Information Security Incident Response Management Process.

IV. Statements created to support particular elements of the information security incident response and notification practice at the university will be organized into existing policies, standards, requirements, guidelines, and practices. Creation of new policies, standards, requirements, guidelines, and practices to support the intent of this policy is allowed.

V. All faculty, staff, students, volunteers, agents, contractors, and all other individuals handling institutional data on the university’s behalf must report information security events.

VI. Rationale
Protection of university data is critically important, but inevitably institutional data will be lost, stolen, or exposed. It is important to establish a universal process for investigating security events to determine whether security incidents have occurred. Effective and efficient information security standards are required to promote public trust; respond to information security events; comply with legal, regulatory, and contractual requirements; and establish procedures for reporting and notification.

VII. Enforcement
Failure to comply with this policy may result in suspension of access to information assets or information systems or both and may also result in disciplinary action, up to and including termination or criminal prosecution. Students are also subject to the Code of Student Conduct.

PROCEDURE

Issued: 01/10/2007
Revised: 4/15/2019

I. The Chief Information Security Officer or their appointed designees will develop information security incident response management standards, requirements, guidelines, and practices as needed to support proper reporting and notification of information security incidents.

II. Each university organization (such as colleges and vice presidential units) with institutional data as defined in the Institutional Data policy must:

A. Develop an information security incident response plan that complies with the requirements set forth in the Information Security Incident Response Management Process as well as federal and state security-related regulations and contractual agreements that apply to the institutional data each organization possesses;

B. Designate a team of **Information Security Incident Security Responders (Security Responders)** to respond to information security events that occur within the organization; and

C. Establish how and when to include the **Security Team**, per the Incident Response Job Aid and Information System Incident Response Management Process.

III. All individuals to whom this policy applies must report information security events immediately upon discovery to their local IT Help Desk or Security Responders. **Email phishing** attempts can be reported by clicking the "Report Phish" button in the email client's menu bar or by forwarding the email to report-phish@osu.edu.

IV. As set forth in the Information Security Incident Response Management Process, the university will establish a **Data Incident Response Team (DIRT)**, or **Potential Breach Notification Committee (PBC)** in the case of Protected Health Information (PHI) data, to determine if an information security incident has resulted in data loss that requires notification to impacted individuals or organizations.

V. The following information security incident response categories provide the foundation for the implementation of this policy. Detailed guidance on each of these categories is contained in the Information Security Incident Response Process:

A. Detection and Notification
B. Classification
C. Containment and Recovery
D. Investigation
E. Reporting
F. Post-incident Activity

Responsibilities

Position or Office	Responsibilities
All individuals who suspect or believe a security event has occurred	Report alleged or suspected security events immediately according to the procedure in this policy. Additional details of acceptable reporting procedures are defined in the Information Security Incident Response Management FAQs.
University organizations with institutional data	1. Develop an information security incident response plan. 2. Designate Security Responders to respond to information security events. 3. Establish how and when to include the Security Team.
Unit Management	Designate individuals to be Security Responders.
Chief Information Security Officer	1. Manage this Information Security Incident Response Management policy and its derivative works to support proper reporting and notification of information security incidents. 2. Work in conjunction with the Security Team to determine whether a Data Incident Response Team or Potential Breach Notification Committee should be convened.
Security Responders	1. Complete training provided by the Security Team. 2. Respond to information security events that occur within their university organization. 3. Coordinate the response pursuant to their incident response plan.
Security Team	1. Investigate and substantiate an information security incident. 2. Work in conjunction with the Chief Information Security Officer to determine whether a Data Incident Response Team or Potential Breach Notification Committee should be convened.
Data Incident Response Team (DIRT)	1. Convene to determine whether an information security breach has occurred and if notification is required. 2. DIRT Leadership will determine appropriate action.
Potential Breach Committee (PBC)	Convene to determine if a breach of protected health information (PHI) has occurred and if notification is required.

Resources

Governance Documents
Code of Student Conduct, https://studentlife.osu.edu/csc
Information Security Control Requirements, go.osu.edu/infosec-iscr
Information Security Incident Response Management Process, cybersecurity.osu.edu/system/files/osu_information_security_incident_response_management_process.pdf
Institutional Data policy, go.osu.edu/idp
IT Security policy, ocio.osu.edu/sites/default/files/assets/Policies/ITSecurity.pdf
Responsible Use of University Computing and Network Resources policy, ocio.osu.edu/policy/policies/responsible-use/
University Policies, policies.osu.edu

Additional Guidance
Cybersecurity Phishing, cybersecurity.osu.edu/cybersecurity-you/avoid-threats/phishing
Example Information Security Events which May or May Not be a Data Breach, go.osu.edu/ISIRMP-examples
FAQs, go.osu.edu/ISIRMP-FAQ
HIPAA Compliance and Security Officers, compliance.osu.edu/HIPAAprivacyITsecurity.pdf
Incident Response Plan Job Aid, https://cybersecurity.osu.edu/system/files/osu.iscr.job.aid.it14.1.1.incident_response_plan_v1.1_0.pdf
Merchant Managers and Security Liaisons, u.osu.edu/treasurer/files/2014/10/Quick-Start-Guide-Merchant-Managers-and-Security-Liaisons-1-2afnvit.pdf

Contacts

Subject	Office	Telephone	E-mail/URL
Policy questions	Office of the Chief Information Officer, Enterprise Security Governance & Policy	614-292-1508	itpolicy@osu.edu
Export Control	Export Control Office	(614) 292-4284	exportcontrol@osu.edu
Reporting an information security event	Local Help Desk Or 8-Help Office of the Chief Information, Officer, Enterprise Security Operations OSU Wexner Medical Center, IT Help Desk	Local # or 614-688-8743 614-688-5650 614-293-3861	Local Help Desk security@osu.edu issecurity@osumc.edu
Additional reporting requirements for protected health information	HIPAA privacy and IT security officer (OSUWMC)		privacyoffice@osumc.edu compliance.osu.edu/HIPAAprivacyITsecurity.pdf
Additional reporting requirements for payment card information (PCI)	The Office of the Treasurer		u.osu.edu/treasurer/files/2014/10/Quick-Start-Guide-Merchant-Managers-and-Security-Liaisons-1-2afnvit.pdf
Report a crime	University Police	614-292-2121	police@osu.edu

Applies to: Faculty, staff, students, volunteers, agents, contractors, and all other individuals handling institutional data on the university’s behalf.

History

Issued:	01/10/2007	Issued as “Disclosure or Exposure of Personal Information”
Revised:	04/28/2010	
Revised:	04/15/2019	Renamed “Information Security Incident Response Management”