UNIVERSITY OF TOLEDO
DATA PRIVACY INCIDENT RESPONSE PROTOCOL

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

The University of Toledo provides 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 **data privacy security events** must be properly reported and investigated to determine whether data breaches have occurred. In the event of a **data privacy 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 obligations of contracts and/or federal, state, or local law.

Purpose of the Protocol

To require that data privacy events be 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 a data privacy 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 Data Privacy Incident Response Management Process.
Data privacy 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.
Data privacy incident	A data privacy 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.
Data privacy breach	Any compromise event involving data protected by privacy or security laws, contractual agreements, or regulations that requires notification.
Data Privacy Incident (Security Responders)	Individuals designated by unit management to respond to data privacy 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 Data Privacy 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 IT Security webpage.

UNIVERSITY OF TOLEDO
DATA PRIVACY INCIDENT RESPONSE PROTOCOL

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

Term	Definition
Potential Breach Notification Committee (PBC)	Committee at the University of Toledo Center who determine if a breach of protected health information (PHI) or Personally Identifiable student information (PII) have 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 a data privacy incident and, in conjunction with the Chief Information/Technology 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 during university employment or to perform duties authorized by the university.

Protocol Details

I. This policy establishes the university's commitment to respond to data privacy events, which include information security incidents and data privacy 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 a data privacy event, incident, or breach.

III. The University Privacy Officer or their appointed designees will manage this Data Privacy Incident Response Protocol and its derivative works, such as the Data Privacy Incident Response Management Process.

IV. Statements created to support elements of the data privacy 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 protocol is allowed.

V. All faculty, staff, students, volunteers, agents, contractors, and all other individuals handling institutional data on the university's behalf must report data privacy 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 data privacy events to determine whether privacy incidents have occurred. Effective and efficient data privacy standards are required to promote public trust; respond to data privacy events; comply with legal, regulatory, and contractual requirements; and establish procedures for reporting and notification.

VII. Enforcement

Failure to comply with this protocol 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.

UNIVERSITY OF TOLEDO
DATA PRIVACY INCIDENT RESPONSE PROTOCOL

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

Students are also subject to the Code of Student Conduct.

PROCEDURE

Issued: 3/24/2021 Revised:

I. The University Privacy Officer or their appointed designees will develop data privacy incident response management standards, requirements, guidelines, and practices as needed to support proper reporting and notification of data privacy incidents.

II. Each university organization (such as colleges and vice president units) with institutional data must:

   A. Develop a data privacy incident response plan that complies with the requirements set forth in the Data Privacy 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 **Data Privacy Incident Security Responders (Security Responders)** to respond to data privacy security events that occur within the organization; and

   C. Establish how and when to include the **Privacy Team**, per the Incident Response Job Aid and Data Privacy Incident Response Management Process.

III. All individuals to whom this protocol applies must report data privacy events immediately upon discovery to their local IT Help Desk or Security Responders. **Email phishing** attempts can be reported by clicking the "Phishing / Spam" button from the Add-ins menu in the email client's menu bar or by forwarding the email to emailabuse@utoledo.edu.

IV. As set forth in the Data Privacy 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) or Personally Identifiable Information (PII) data, to determine if a data privacy incident has resulted in data loss that requires notification to impacted individuals or organizations.

V. The following data privacy incident response categories provide the foundation for the implementation of this protocol. Detailed guidance on each of these categories is contained in the Data Privacy Incident Response Process:

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

UNIVERSITY OF TOLEDO
DATA PRIVACY INCIDENT RESPONSE PROTOCOL

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

Responsibilities

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

UNIVERSITY OF TOLEDO
DATA PRIVACY INCIDENT RESPONSE PROTOCOL

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

Resources

Governance Documents

Student Code of Conduct, https://www.utoledo.edu/policies/main_campus/student_life/pdfs/3364_30_04_Student_code_of_conduct.pdf

Information Security Incident Response Management Process, https://www.utoledo.edu/offices/internalaudit/institutional-compliance/docs/DataPrivacyIncidentResponseManagementProcess.pdf

IT Security policies, https://www.utoledo.edu/policies/administration/info_tech/

Responsible Use of University Computing and Network Resources policy, https://www.utoledo.edu/policies/administration/info_tech/pdfs/3364-65-01-responsible-technology-use-policy.pdf

University Policies, https://www.utoledo.edu/policies/

Additional Guidance

Cybersecurity Phishing, https://www.utoledo.edu/it/security/Awareness/Phishing.html

Example Information Security Events which May or May Not be a Data Breach, https://www.utoledo.edu/offices/internalaudit/institutional-compliance/docs/security_events_to_potential_breach_examples.pdf

FAQs

- HIPAA Privacy Rule, https://www.utoledo.edu/offices/compliance/Privacy_FAQs.html
- FERPA, https://www.utoledo.edu/offices/registrar/ferpa_faculty_staff.html
- General Data Protection Regulation, https://www.utoledo.edu/it/gdpr/GDPRfaq.html
- FACTA Red Flags, https://www.utoledo.edu/offices/internalaudit/institutional-compliance/FACTA_Red_Flags_FAQs.html
- IT Security, https://www.utoledo.edu/it/security/

University Compliance Officers, https://www.utoledo.edu/offices/internalaudit/institutional-compliance/iccomplianceofficers.html

Incident Response Plan Job Aid, https://www.utoledo.edu/offices/internalaudit/institutional-compliance/docs/IncidentResponsePlanJobAid.pdf

Merchant Managers and Security Liaisons, treasurer@utoledo.edu

UNIVERSITY OF TOLEDO
DATA PRIVACY INCIDENT RESPONSE PROTOCOL

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

Contacts

Subject	Office	Telephone	E-mail/URL
Policy questions	Privacy Office, IT Security Office	419-383-4270	privacyoffice@utoledo.edu, itsecurityoffice@utoledo.edu
Export Control	Export Control Office	419-530-6226	exportcompliance@utoledo.edu
Reporting a data privacy event	IT Help Desk (Main Campus)	419-530-2400	ithelpdesk@utoledo.edu
	IT Help Desk (Health Science Campus)	419-383-2400	ithelpdesk@utoledo.edu
	Office of the Chief Information/ Technology Officer, Division of Technology and Advanced Solutions	419-530-1737	dtas@uoledo.edu
Additional reporting requirements for protected health information or personally identifiable information	University Privacy Officer		privacyoffice@utoledo.edu
Additional reporting requirements for payment card information (PCI)	The Office of the Treasurer		treasurer@utoledo.edu
Report a crime	University Police	419-530-2600	utpolice@utoledo.edu

History

Issued: 3/24/2021 Issued as "Data Privacy Incident Response Protocol"

Revised: