# UToledo Data Privacy Incident Response Protocol

V1

## 1. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 6/23/2021 | Draft v1 | Document created from previous processes | David Cutri, CCO |

## 2. Approval History

| Date | Version | Approved by | Notes |
|---|---|---|---|
|  | v1 | UTMC Privacy and Security Committee |  |
|  | v1 | University Privacy and Information Security Committee |  |

# 3. Contents

## 4. Introduction

UToledo seeks to ensure the proper handling of information, and management of information systems. UToledo is subject to numerous laws and regulations which require notification of suspected or confirmed data incidents to external parties such as regulators, law enforcement, and impacted individuals. As such, the Data Privacy Incident Response Protocol specifies the need for a UToledo-wide data incident response process.

This process is overseen by the Privacy Officer and relies on partnership with all UToledo colleges and units to effectively manage the response to data incidents. It begins when an individual suspects an information security/data privacy incident and ends when the final approved response action(s) have been completed.

The process is to be activated whenever there is a suspected data privacy incident, which includes any potential unauthorized access or impact to UToledo-owned or managed information or systems. The process will determine if this action has resulted in an information breach, and any required reporting.

The definition of breach varies by regulation. For example, O.R.C. (O.R.C. 1349.19) defines a breach as:

> *“Breach of the security of the system” means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information… and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.”*

Therefore, this document will not provide a UToledo definition for “breach” but instead use the National Institute of Standards and Technology definition of security Incident (see the Definitions list)

The data incident response process will be reviewed and updated at least annually, to ensure ongoing regulatory compliance and effectiveness.

## 5. Process Purpose and Objectives

The goals of the UToledo Data Privacy Incident Response Protocol are:

- Minimize negative consequences of information security incidents.
- Improve the ability of UToledo to promptly restore operations.
- Enable prompt incident response decisions by appropriate stakeholders.
- Proactively reduce the exposure of UToledo to information security incidents by employing consistent incident management processes that incorporate lessons learned from past incidents.
- Satisfy Federal, State, and industry regulations that require improved protection of sensitive and private information, and timely disclosure of potential breaches to affected individuals.

## 6. Process Scope

This process applies to all faculty, staff, and students; academic and administrative units; affiliated entities; agents and contractors handling personal information or systems on behalf of UToledo.

## 7. Definitions

| Term | Description | Example |
|---|---|---|
| Adverse Event | Any observable occurrence with a negative consequence or impact to the confidentiality, integrity, or availability of a technology asset, system, or network. | • System crashes<br>• Network packet floods<br>• Unauthorized use of system privileges<br>• Unexplained alteration of data<br>• Missing or unaccounted-for computing equipment<br>• Other unexplained harmful or unwanted activity |
| Breach | A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose (source: NIST Computer Security Resource Center). | |
| CCO | Chief Compliance Officer | |
| CIO | Chief Information/Technology Officer | |
| CRO | Chief Risk Officer | |
| Compromise | Unauthorized access to, theft, control, or possession of, university data or systems. | • Unauthorized access to sensitive or protected data |
| Data Types | Data classifications:<br>• Public Data<br>• Internal Data<br>• Private Data<br>• Restricted Data | |
| DIRT | Data Incident Response Team<br>Comprised of the DIRT-Leadership team as well as Marketing and Communications, UTPD, Privacy Officer, Human Resources, and Legal Affairs. | |
| DIRT-Leadership | DIRT Leadership made up of the CIO, CCO, General Counsel, CRO, and data owner. | |
| EU | European Union | |
| 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. | • User connecting to a file share<br>• Server receiving a request for a web page<br>• Firewall blocking a connection attempt<br>• General malware/adware detection<br>• Intrusion Detection System alert<br>• Etc. |

| Term | Description | Example |
|---|---|---|
| FERPA | The Family Educational Rights and Privacy Act of 1974 (or the Buckley Amendment) is a United States Federal law that governs the access to educational information and records by public entities such as potential employers, publicly funded educational institutions, and foreign governments. | |
| GDPR | The General Data Protection Regulation (EU) 2016/679 is a regulation in EU law on data protection and privacy in the EU and the European Economic Area. | |
| GLBA | The Gramm–Leach–Bliley Act, also known as the Financial Services Modernization Act of 1999, enacted November 12, 1999 is an act of the 106th United States Congress (1999–2001). The Safeguards Rule requires financial institutions to develop a written information security plan that describes how the company is prepared for and plans to continue to protect clients' nonpublic personal information. | |
| HIPAA | The Health Insurance Portability and Accountability Act of 1996 (or the Kennedy–Kassebaum Act) is a United States Federal statute enacted by the 104th United States Congress and signed into law by President Bill Clinton on August 21, 1996. The HIPAA Privacy Rule is composed of national regulations for the use and disclosure of PHI in healthcare treatment, payment, and operations by covered entities. | |
| HSC | UToledo Health Science Campus | |
| Incident | A suspected or identified adverse event or group of adverse events, which if confirmed has or had significant potential to negatively impact the confidentiality, integrity, or availability of sensitive data or university technology assets. An incident may also be an identified violation or imminent threat of violation of a university policy. | • Loss of confidentiality of information<br>• Compromise of integrity of information<br>• Loss of system availability or denial of service<br>• Loss or theft of a technology asset<br>• Unauthorized damage to, or destruction of, a technology asset<br>• Unauthorized execution of, or damage to systems by, malicious code, such as viruses, trojan horses or hacking tools<br>• Compromise of authentication data or username and password credentials<br>• Use of university technology assets in violation of state or federal law |

| Term | Description | Example |
|---|---|---|
| IS | Incident Scoring | |
| IT | Information Technology | |
| MC | Main Campus | |
| NIST | National Institute of Standards and Technology | |
| O.R.C. | Ohio Revised Code | |
| Packet Floods | In a network, flooding is the forwarding by a router of a packet from any node to every other node attached to the router except the node from which the packet arrived. | Flooding is a way to distribute routing information updates quickly to every node in a large network. |
| PCI | The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes. | |
| PHI | Protected Health Information | |
| Privacy Officer | University Privacy Officer | |
| Security Responders | Also known as "Information Security Incident Responders". Individuals designated by unit management to respond to information security events and who have received training by IT Security. These individuals will coordinate the unit's response following their incident response plan based on the Data Privacy Incident Response Protocol. | Business Managers |
| Security Team | Also known as the IT Security Team. See section 8.1 for Security Teams. One or more teams of individuals who investigate and substantiate an information security/data privacy incident and, in conjunction with the Privacy Officer, determine whether a DIRT should be convened. | |
| Unauthorized Access | The viewing or possession of something without legal authority. Viewing private accounts, messages, files, or resources when one has not been given permission from the owner to do so. | |
| University Senior Leadership Response Team | In the event of a persistent incident, UToledo senior leadership will be engaged to oversee the response activities. This includes the President/Provost and any senior leaders they choose. | Wicked Panda has been one the most prolific and effective China-based persistent adversaries from the mid-2010s into the 2020s. CrowdStrike Intelligence assesses Wicked Panda consists of a superset of groups involving several contractors working in the interests of the Chinese state while still carrying out criminal, for-profit activities, likely with some form of tacit approval from Chinese Communist Party officials. |

| Term | Description | Example |
|---|---|---|
| UTMC | University of Toledo Medical Center | |
| UToledo | The University of Toledo | |
| UTPD | University of Toledo Police Department | |

## 8. Process Overview

All incidents will follow the same general management process:

1. A user will notify their security responders about a security event. Security responders are individuals designated by unit management to respond to information security events and trained by IT Security. These individuals will coordinate the unit's response following their incident response plan based on the Data Privacy Incident Response Protocol. Leadership within the unit are responsible for informing their employees of the names and contact information of the security responders.
2. When an incident is DETECTED, the IT Security team is NOTIFIED.
3. The incident is CLASSIFIED to determine potential size of impact (IS ratings are defined in the IS table in Section 8.2. Section 8.2 also contains a summary of typical remediation activities for a security event.)
4. Incidents are CONTAINED by IT Security and local units. Business processes and related systems are RECOVERED according to unit business continuity and disaster recovery plans.
5. IT Security will INVESTIGATE the incident, including root cause analysis.
6. IT Security will REPORT the incident to the appropriate authorities, partnering with data/business owners, as necessary.
7. IT Security will promptly refer data privacy incidents to the Privacy Officer.
8. POST-INCIDENT activities such as lessons learned activities will be conducted for IS3 and IS4 incidents by IT Security.
9. Following are actions in which the DIRT-Leadership team should be actively engaged:
    - Receiving the incident report from the Privacy Office
    - Determining whether to activate the DIRT Team
    - Developing a mandatory communication plan, if applicable
    - Determining compliance requirement
    - Informing department of actions needed to satisfy UToledo, State, and Federal requirements
10. Following are actions in which the DIRT team should be actively engaged:
    - Activating the DIRT team
    - Reviewing incident report, continuing investigation
    - Coordinating internal/external communications with DIRT-Leadership team
    - Developing communication, eradication, and recovery strategies
    - Relating and monitoring mitigation requirements
    - Confirming mitigation, and beginning monitoring
    - Closing the incident

## 8.1. Detection and Notification

The first indication of a potential incident can come from a variety of internal and external alerts, with varying levels of detail.

Policy requires **all individuals to notify the IT Help Desk or security responder of any events. In turn, the security responder must notify the IT Security team immediately if they suspect an incident has, or will, occur.**

UToledo has two IT Security teams who receive alerts:

| All Alerts | HSC Only |
|---|---|
| MC IT Security<br>ithelpdesk@utoledo.edu<br>419-530-2400 | HSC IT Security<br>ithelpdesk@utoledo.edu<br>419-383-2400 |

The IT Security team(s) will confirm receipt of all alerts and will conduct a preliminary triage for all alerts.

If the team(s) determines that the event reported is an incident, they will also assess the incident to determine the likely included data types:

- If the IT Security team identifies HIPAA, FERPA, PCI, GLBA, or GDPR data is potentially in scope, they will notify the UToledo Privacy Office within the Institutional Compliance organization.
- If the HSC IT Security team identifies non-HIPAA/FERPA/PCI/GLBA/GDPR data is potentially in scope, they will notify IT Security.
- The MC IT Security team will notify the HSC IT Security team of incidents on their respective campuses, to ensure independent verification of investigation activities.
- If the originating unit is the Privacy Office, it will conduct an initial assessment, then refer the matter to IT Security.
- If the originating unit is neither IT Security nor the Privacy Office, it will refer the matter to IT Security via the IT Help Desk.

When an incident is identified, the IT Security team(s) will notify the CIO, who will notify internal groups (including the President and senior leadership) according to the scoring rating of the incident, listed below.

## 8.2. Incident Classification

As stated in University of Toledo 3364-65-10 Technology Incident Response policy, section (E), the "… University's incident response capability shall include, but not be limited to, the following:" adverse events, minor incidents, and major incidents.

Adverse events and incidents are classified based on the following criteria:

- **Information Impact of the Incident**: impact based on the confidentiality, integrity, and availability of information on or attached to affected system(s).
- **Functional Impact of the Incident**: the current and/or future business functionality that affected system(s) provide, resulting in some type of negative impact to the users of those systems.
- **Recoverability from the Incident**: the effort necessary to recover from an incident carefully weighed against the value the recovery effort will create.
- **Compliance/Reputational Risk of the Incident:** the likelihood of fines or sanctions related to the event.

For each of these criteria, a rating is applied as follows:

| **IS Table** | | | | |
|---|---|---|---|---|
| | ***Typically*** **Minor Incidents** | ***Typically*** **Minor Incidents** | ***Typically*** **Major Incidents** | ***Typically*** **Adverse Events** |
| | **IS1 (Public Data)** | **IS2 (Internal Data)** | **IS3 (Private Data)** | **IS4 (Restricted Data)** |
| Information Impact | No unauthorized data access, usage, disclosure, loss, or alteration. | Unauthorized access, usage, disclosure, loss, or alteration of public/internal data. | Unauthorized access, usage, disclosure, loss, or alteration of private data. | Unauthorized access, usage, disclosure, loss, or alteration of restricted data. |
| Functional Impact | System does not have a critical University-wide impact; usage by 1-10 customers. | System does not have a critical University-wide impact; usage by 10-100 customers. | System is important to many groups or users at UToledo (unit-wide service or 100+ customers across units). | System is a critical UToledo-wide service or there are massive impacts to many unit services; critical business functions will cease. |
| Recoverability | Easy to recover/standalone system. | Relatively easy to recover such as standalone system with unique or non-unique credentials. | Difficult to recover such as standalone system with many dependencies; or many systems are believed to be impacted. | System cannot be recovered, and/or intense effort for recoverability will be needed (such as a massive lateral spread). |
| Compliance/Reputation | No risk of fines or sanctions; no requirements to notify external parties. | Low risk of fines or sanctions. Incident may result in notification to the public. | Fines or sanctions likely; incident may result in notification to the public. | Fines or sanctions assumed; incident to be made public. |

For any given incident, the criteria above will be assessed. The HIGHEST rating for a criterion will be the overall rating for the incident.

### Remediation

1. A basic data analysis is completed by the unit and security.
2. Regulatory agencies are notified of suspicion of breach, depending on data type.
3. IS1 incidents are remediated by the unit.
4. IS2 incidents are triaged by IT Security.
    a. Basic data analysis is completed by IT Security and the unit.
    b. If private/restricted data is found, DIRT processes are activated by IT Security (see below).
    c. If private/restricted data is not found, the unit remediates the incident.
5. IS3 incidents are triaged by IT Security.
    a. IT Security will perform a scope, vulnerability, root cause, and forensic analysis, in partnership with the unit.
    b. Concurrently, data analysis is completed by IT Security and the unit.
    c. If private/restricted data is found, DIRT processes are activated by IT Security (see below).
    d. If private/restricted data is not found, the unit remediates the incident.
    e. A lessons-learned exercise is performed.
6. IS4 incidents are triaged by IT Security.
    a. DIRT is notified.
    b. IT Security will perform a scope, vulnerability, root cause, and forensic analysis, in partnership with the unit.
    c. Concurrently, data analysis is completed by IT Security and the unit.
    d. If private/restricted data is found, DIRT processes are activated by IT Security.
    e. Appropriate office develops a communication plan for any ongoing activities.
    f. A lessons-learned exercise is performed.
    g. Results from lessons-learned exercise is shared with appropriate stakeholders.
7. DIRT processes activated by IT Security:
    a. Reviewing incident report, continuing investigation
    b. Coordinating internal/external communications with DIRT-Leadership team
    c. Developing communication, eradication, and recovery strategies
    d. Relating and monitoring mitigation requirements
    e. Confirming mitigation, and beginning monitoring
    f. Closing the incident

## 8.3. Containment and Recovery

When an incident is reported to the IT Security team(s), there are three activities that need to occur: containment of the incident, investigation of the incident, and recovery of the data systems according to the unit's business continuity and/or disaster recovery plans.

IT is responsible for ensuring that, to the extent possible, any evidence of the incident is preserved. IT can contain an event by:

- Restricting network access
- Disabling remote access
- Keeping machine(s) out of use

IT teams can begin to activate their business continuity/disaster recovery plans to respond to the incident; however, modification of systems or data should only occur after the IT Security teams have confirmed they have obtained the required evidence. Units should not:

- Run antivirus software. The IT Security team should be notified if malware or antivirus software was run prior to the incident being reported.
- Power down the machine(s).
- Attempt any other mitigation procedure.

Once the IT Security team(s) is notified of the incident, the IT Security team(s) will activate their evidence gathering activities, including gathering forensic images of impacted hosts, interviewing impacted staff, etc.

If the incident reveals a persistent presence on a UToledo system, the IT Security team(s) may work with external support teams, and law enforcement as required, to observe and contain the activities of the attacker. Additionally, recovery operations may need to be conducted at the direction of the CIO and UToledo senior leadership response teams.

When responding to an incident it may be necessary, subject to applicable laws and UToledo policies, to require the suspension of involved or targeted services/systems to:

- Protect students, faculty, staff, IT resources, other systems, data, and UToledo 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 IT Security team(s), as designated by the university CIO.

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

Any equipment not owned by UToledo, which is using UToledo IT resources, and is found to be the target, source, or party to an 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. The IT department is responsible for maintaining effective procedures for tracking and quantifying this type of equipment.

In all cases, it is the IT Security team(s) who shall determine when a service suspension may be lifted.

### Ransomware

In the case of incidents involving ransomware or "payment for recovery" activities, the Provost, General Counsel, Chief Financial Officer, and the CIO will determine whether payment will be made.

## 8.4. Investigation

All investigations are conducted by the IT Security team(s); local IT or other groups should not attempt to conduct investigations without direction of the IT Security team(s).

After receiving a report, assessing its accuracy, determining whether the event constitutes an incident, and classifying the incident, the IT Security team(s) will determine if the incident warrants a formal UToledo response. Incidents that do not warrant a formal response will be referred to the reporting unit or other appropriate group for handling. All reported events or incidents must be documented throughout the response process.

If an event report does warrant formal incident response procedures by the IT Security team(s), it is the responsibility of IT Security to coordinate the appropriate resources for such response.

At any point during an incident, any UToledo user found to be violating UToledo policies may be referred to the appropriate UToledo administrative adjudicating authority.

Violations of local, State, or Federal law will typically be referred to UTPD, who will work alongside those relevant UToledo officials that are aware of how to apply the local, State, and Federal laws in this area. IT Security team(s) will confer with the Privacy Office and the Office of Legal Affairs prior to referring violations to UTPD or external law enforcement.

The IT Security team(s) will keep impacted units, UToledo leadership and other stakeholders informed as their investigation progresses.

Investigatory incidents referred to the Privacy Office will be coordinated with the Office of Legal Affairs, Risk Management, Marketing and Communications, and IT.

## 8.5. Reporting

After reporting suspected incidents to IT Security, units should ensure their unit leadership is informed according to their unit incident response plans. Unit security responders are responsible for ongoing unit reporting unless otherwise directed by the IT Security team(s).

During an incident investigation:

- IT Security team(s) will provide interim reports to the CIO, Privacy Office, and impacted units.
- All communications with media will be managed by UToledo Marketing and Communications, in partnership with the Privacy Office and IT Security team(s).
- Vendors and UToledo partners or other entities required by contract will be notified by local units, at the direction of the IT Security team(s).
- CIO will ensure the DIRT-Leadership or full DIRT committee are informed, based on the incident categorization.
- In the case where external law enforcement is engaged, UToledo may limit notification of the incident until permission is granted by law enforcement.
- Internal notifications will be made according to incident classification:

| | IS1 (Public Data) | IS2 (Internal Data) | IS3 (Private Data) | IS4 (Restricted Data) |
|---|---|---|---|---|
| See Customer Notification/Credit Monitoring Vendor | None | None | Put vendor on Alert | Put vendor on Alert |
| Cybersecurity Insurance | None | None | Immediate | Immediate |
| DIRT | None | None | Per DIRT-Leadership guidance | Immediate |
| DIRT-Leadership | None | None | Immediate | Immediate |
| Security Advisory Board | None | Standard Reporting Schedule | Standard Reporting Schedule | Standard Reporting Schedule |
| Unit Leadership | Standard Reporting Schedule | Standard Reporting Schedule | Immediate | Immediate |
| University Senior Leadership | None | None | Standard Reporting Schedule | Immediate |

- Regulatory notifications will be made according to data classification:

| Immediately | Within 48 Hours | Within 72 Hours | Within 45 Days | Other |
|---|---|---|---|---|
| • GLBA (on suspicion of incident) | • PCI (on suspicion of incident) | • GDPR (on suspicion of incident) | • General Protected Information (State of Ohio)<br>• If >1000 disclosed records -- also consumer reporting agencies | • FERPA<br>• HIPAA<br>• Notify State of Ohio for any computer crimes |

Reporting after an investigation is completed:

- The incident summary and the final lessons-learned results will be shared with security responders and UToledo IT leadership. Additional groups will be informed as appropriate.
- Quarterly reports of aggregated incident activities will be reported to the UTMC Privacy and Security Committee and the University Privacy and Information Security Committee.
- Yearly reports of aggregated incidents will be shared with the Board of Trustees as part of the annual Information Security Program report.
- Regulatory and State agencies will be notified according to the data classifications included in the incident.
- At the direction of DIRT, notifications will be shared with any impacted individuals, including any credit monitoring or repair services. The Privacy Officer will receive any reports generated by the vendor providing the notification service and will share these reports with impacted units.
- The CIO and/or the Privacy Officer will notify/apprise the President/senior leadership as appropriate within the notification process.

## 8.6. Post-Incident Activity

A full "lessons-learned" analysis will be conducted for IS3 and IS4 incidents, led by the Privacy Officer, with impacted units and stakeholders. These results will be shared with teams as listed in the "Reporting" section, above.  This analysis will be prepared regardless of whether the source data resided on UToledo resources or were disclosed by UToledo employees.

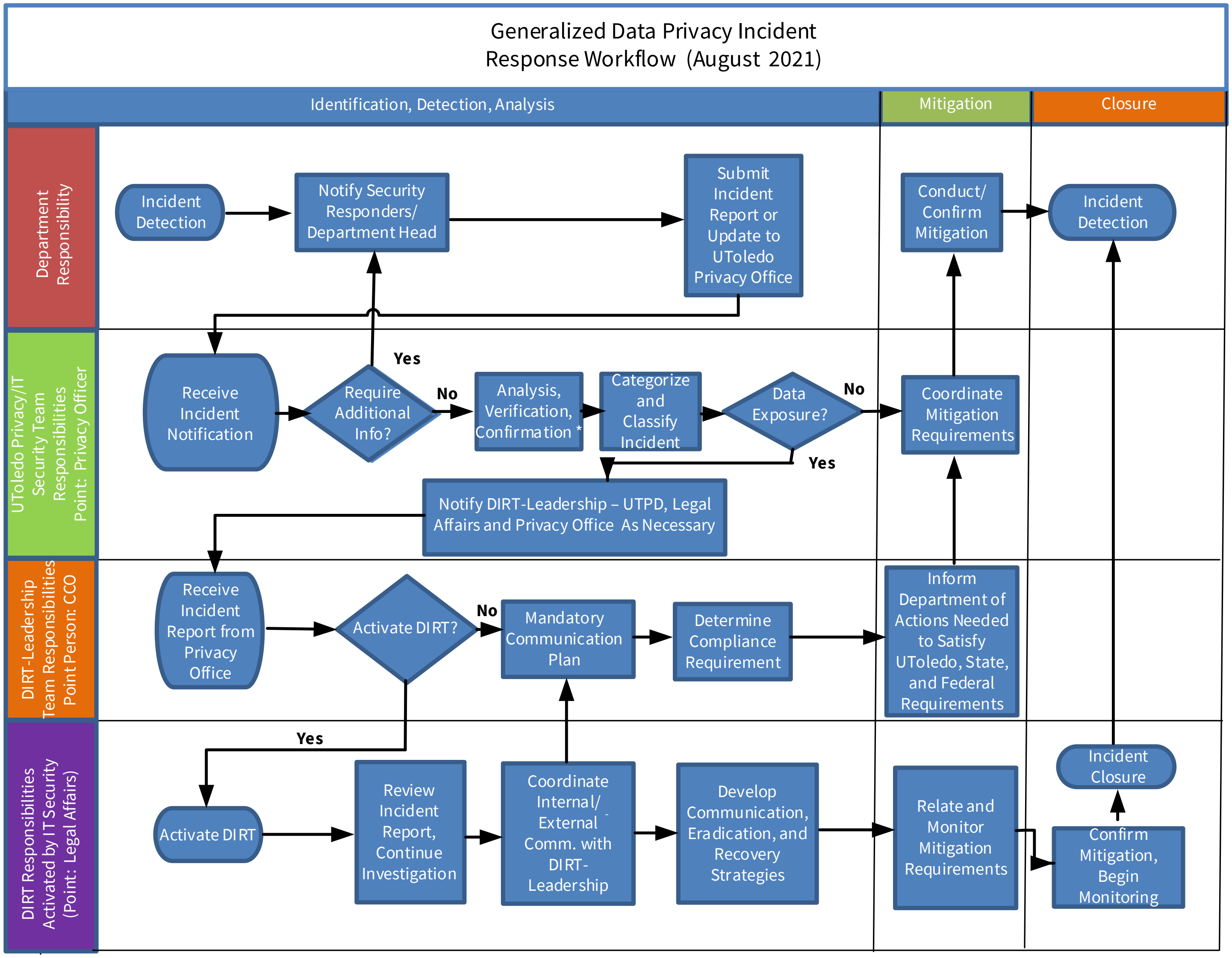
The Privacy Officer will ensure all evidence related to the incident is preserved in accordance with records retention policies or other legal requirements.

## 9. Appendix A: Responsibilities

| Position or Office | Responsibilities |
|---|---|
| All individuals who suspect or believe a security event has occurred | Report alleged or suspected security events to the IT Security team, the IT Help Desk, or the Privacy Office immediately according to this procedure. Additional details of acceptable reporting procedures are defined on the IT Security webpage. |
| CIO | 1. Manage this Data Privacy Incident Response Protocol and its derivative works to support proper reporting and notification of information security incidents and engagement with the Privacy Office when necessary.<br>2. Work in conjunction with the IT Security team and the Privacy Office to determine whether a DIRT or potential breach notification committee should be convened. |
| DIRT | 1. Convene to determine whether an information security breach has occurred and if notification is required.<br>2. DIRT Leadership will determine appropriate action. |
| DIRT-Leadership | Convene to determine if a breach of PHI or Personally Identifiable Information has occurred and if notification is required. |
| IT Security Team | 1. Investigate and substantiate an information security incident.<br>2. Work in conjunction with the CIO to determine whether a DIRT or potential breach notification committee should be convened. |
| Privacy Office | 1. Accept all data privacy/breach incidents presented by the CIO and/or the IT Security team.<br>2. Coordinate all investigatory, notification, remediation, and communication activities with Marketing and Communications, Office of Legal Affairs, Risk Management, UTPD, and other stakeholder departments. |
| Security Responders | 1. Complete training provided by the IT Security team.<br>2. Respond to information security events that occur within their university organization.<br>3. Coordinate the response pursuant to their incident response plan. |
| Unit Management | Designate individuals to be security responders. |
| UToledo organizations with institutional data | 1. Develop an information security incident response plan.<br>2. Designate security responders to respond to information security events.<br>3. Establish how and when to include the IT Security team. |

# 10. Appendix B: Process Diagram

This diagram visually depicts the process steps set forth above.


Generalized Data Privacy Incident
Response Workflow (August 2021)
Identification, Detection, Analysis
Mitigation
Closure
Department Responsibility
UToledo Privacy/IT Security Team Responsibilities Point: Privacy Officer
DIRT-Leadership Team Responsibilities Point Person: CCO
DIRT Responsibilities Activated by IT Security (Point: Legal Affairs)
Incident Detection
Notify Security Responders/ Department Head
Submit Incident Report or Update to UToledo Privacy Office
Conduct/ Confirm Mitigation
Incident Detection
Receive Incident Notification
Yes
Require Additional Info?
No
Analysis, Verification, Confirmation *
Categorize and Classify Incident
Data Exposure?
No
Yes
Coordinate Mitigation Requirements
Notify DIRT-Leadership – UTPD, Legal Affairs and Privacy Office As Necessary
Receive Incident Report from Privacy Office
Activate DIRT?
No
Mandatory Communication Plan
Determine Compliance Requirement
Inform Department of Actions Needed to Satisfy UToledo, State, and Federal Requirements
Yes
Activate DIRT
Review Incident Report, Continue Investigation
Coordinate Internal/ External Comm. with DIRT-Leadership
Develop Communication, Eradication, and Recovery Strategies
Relate and Monitor Mitigation Requirements
Incident Closure
Confirm Mitigation, Begin Monitoring

* Note that the "Analyze, Verification, Confirmation" task referred to above includes the forensics process during an incident, such as collecting the data around any incident involving electronically stored data.