Generalized Data Privacy Incident Response Summary (December 2021)

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:

Incidemt Scoring (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.

NOTE: Those tasks above that are highlighted in red are discussed in further in detail in the Data Privacy Incident Response Protocol flowchart (attached) and accompanying procedural narrative.

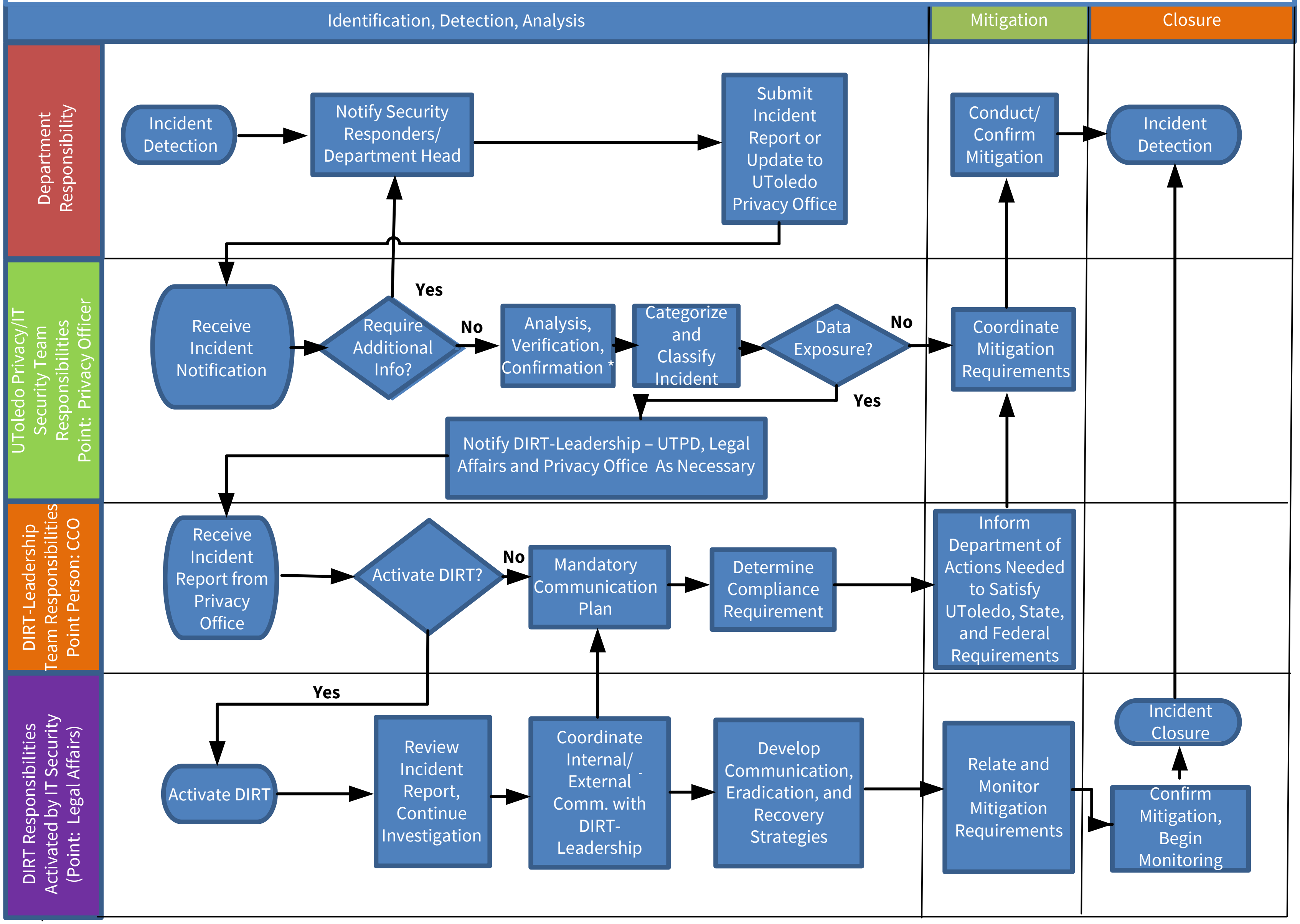
For any given incident, the criteria above will be assessed. The HIGHEST rating for a criterion will be the overall rating for the incident.

Remediation

1. A basic data analysis is completed by the unit and security.
2. Regulatory agencies are notified of suspicion of breach.
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 found, DIRT processes are activated.
   c. If not found, the unit remediates the incident.
   d. DIRT: Data Incident Response Team
5. IS3 incidents are triaged by IT Security.
   a. IT Security/The unit will perform a root cause/forensic analysis.
   b. Concurrently, data analysis completed by IT Security/the unit.
   c. If private/restricted data found, DIRT processes are activated.
   d. If 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/The unit will perform a root cause/forensic analysis.
   c. Concurrently, data analysis completed by IT Security/the unit.
   d. If private/restricted data found, DIRT processes are activated.
   e. A communication plan is developed for ongoing activities.
   f. A lessons-learned exercise is performed.
   g. Results from exercise is shared with stakeholders.
7. DIRT processes activated by IT Security:
   a. Reviewing incident report, continuing investigation
   b. Coordinating communications with DIRT-Leadership team
   c. Developing communication, eradication, recovery strategies
   d. Relating and monitoring mitigation requirements
   e. Confirming mitigation, and beginning monitoring
   f. Closing the incident

All other tasks above (which represent the majority of all security incidents) are within the purview of the IT Security function and their corresponding procedures (https://www.utoledo.edu/it/security/). Regardless of their perceived severity, users should report information security incidents to the University of Toledo IT Help Desk at (419) 530-2400.

Generalized Data Privacy Incident Response Workflow (October 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
Require Additional Info?
Yes
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
Yes
Mandatory Communication Plan
Determine Compliance Requirement
Inform Department of Actions Needed to Satisfy UToledo, State, and Federal Requirements
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.