

INCIDENT RESPONSE TEMPLATE



**Utah Office of
Data Privacy**

DISCLAIMER

This template is provided by the Utah Office of Data Privacy (ODP) as a resource to assist governmental entities. This template is intended to serve as general guidance and a foundational structure only. Governmental entities are responsible for reviewing, customizing, and adapting this template to ensure compliance with applicable laws, regulations, policies, and organizational needs.

The ODP makes no representations or warranties, express or implied, regarding the legal sufficiency or suitability of this template for any specific purpose. By using this template, governmental entities acknowledge and agree that the ODP is not liable for the use or modification of this template. This template is not legal advice and is not a substitute for consultation with legal counsel. Entities should consult with their own legal counsel before finalizing or executing a document based on this template.

PURPOSE: This template provides a structured framework for documenting, investigating, and reporting security incidents. It is divided into **Part 1 – Statutorily Required** and **Part 2 – Best Practice** ([NIST 800-61](#)).

PART 1 – STATUTORILY REQUIRED INFORMATION

(Fields **REQUIRED** under state statute and Cyber Center guidance; must be completed consistently)

INCIDENT IDENTIFICATION

Incident Name/ID:

Date & Time Incident Occurred:

Date & Time Incident Discovered:

Short Description of Incident:

Provide a concise summary of what happened, e.g., type of incident, systems affected, and immediate impact.

ACCESS AND PERPETRATOR DETAILS

Means of Unauthorized Access:

Explain how the incident occurred (e.g., stolen credentials, phishing, malware, email misdelivery).

Person(s) Responsible (if known):

IMPACT

Total Number of Individuals Affected:

Type(s) of Personal Data Compromised:

Examples: Social Security numbers, data classification, financial account information, health data, driver's license numbers.

MITIGATION STEPS

Actions Taken to Contain or Mitigate Incident:

List immediate actions, e.g., system isolation, password resets, patching vulnerabilities.

PART 2 – BEST PRACTICE

(Recommended fields from NIST 800-61. Other considerations include: [HIPAA](#), [FTI](#), CJIS, [PCI-DSS](#))

INCIDENT CLASSIFICATION AND CONTEXT

Incident Category/Type:

Unauthorized access, malware, phishing, denial-of-service, insider threat, etc.

Incident Severity/Impact Level:

Low, Moderate, High, Critical – based on operational or data impact

Systems, Networks, or Data Repositories Affected:

Incident Source & Indicators (if known):

Include attacker IPs, domains, malicious files, or vectors used

DETECTION & ANALYSIS DOCUMENTATION

Detection Method:

How was the incident first identified (alert, log review, user report, automated tool)?

Logs, Alerts, and Evidence Collected:

Initial Scope & Impact Assessment:

Triage & Prioritization Rationale:

Timeline of Detection and Reporting Events:

Event	Date/Time	Responsible Party	Notes

RESPONSE ACTIONS & TACTICS

Immediate Containment Steps Taken:

Threat Eradication Steps:

Recovery Activities Performed:

Evidence Preservation Methods:

Document chain-of-custody, forensic copies, system snapshots

Tools/Techniques Used in Response:

COMMUNICATION & COORDINATION

Internal Notifications:

Roles notified (i.e. Cyber Center, AG Office etc.), time of notice, method of communication

External Notifications:

Law enforcement, regulators, partners – include dates and contacts

Communication Protocols Used:

Escalation Procedures Followed:

POST-INCIDENT REVIEW & CONTINUOUS IMPROVEMENT

Root Cause Analysis Summary:

Lessons Learned:

Long-term Corrective Actions & Improvements:

Policy, Control, or System Changes to Prevent Recurrence:

Training/Awareness Actions Generated from Incident:

METRICS & REPORTING DATA

Incident Handling Timeline:

Record times for detection, containment, eradication, recovery

Impact on Operations and Services:

Cost and Resource Metrics (if applicable):

INSTRUCTIONS FOR USE:

1. Link statutory obligations
2. Link Cyber Center Reporting Portal
3. Link internal procedure
4. Link additional investigation resources

(i.e. Attestation of Destroyed Data, Incident Response Team, Notice of Breach etc.)