Security Incident Response Plan

Version number	4.2
Last Approved	Jun 25, 2025
Classification	PUBLIC

Overview

Security incidents present a threat to the confidentiality, integrity, and availability of the Company's systems and data. Successful mitigation of this threat requires not only a best practice approach to managing system vulnerabilities, but also swift and effective response to any security incidents.

The procedures defined in this document ensure that security incident affecting the Company are appropriately and consistently identified and handled.

Applicability

The applicability of this statement falls under purview of the Security Documentation Overview.

Purpose

The purpose of this document is to define a process for responding to physical, data security and privacy events and their potential escalation to security incidents at The Company. This plan outlines who needs to do what for The Company to effectively manage the full life cycle of security incidents .

Scope

This plan covers any security event or incident involving data, systems, or facilities. This includes:

- Company internal data, and customer data that The Company processes and stores;
- Company internal, customer-facing, and public-facing business systems;
- Third-party partner/provider systems used by The Company's processes and systems;
- Physical access to facilities.

Events such as floods, fires, power-related disruptions, excessive heat and other natural disasters that cause system crashes are not within the scope of this document and are addressed in the Business Continuity Planning and Disaster Recovery Policy.

Security Incident Response Plan

Security Classifications:

To clarify the scope of this plan and the scope of each Security Event type, below is a list of examples for each one. The examples are representative of each event type, but not exhaustive.

Security Events

- observed suspicious behaviour of visitors, contractors or employees
- suspected misuse of a computer system
- malicious activity that is being adequately prevented or contained, or that does not present a material impact to Company resources

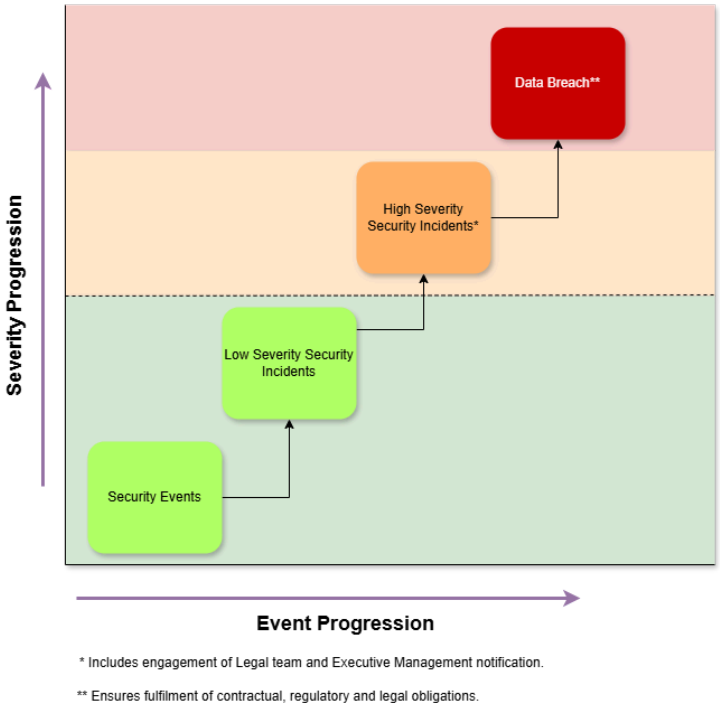
Security Incidents

Security incidents may include but are not limited to the following:

- Suspected and successful hacking attempts
- Loss of sensitive information due to unknown reasons
- Loss of service or data to critical service providers
- Security breach on systems, services, and applications
- Hardware resources and components lost or stolen
- Hardware, software, or operational errors that results in erroneous data
- Failure of critical IT services or equipment
- Malware incidents regarding e-mail and sensitive data
- Virus, worm, or trojan infection
- Exploited weaknesses in existing infrastructure, policies and standards
- Disruption or denial or service through electronic means (DoS or DDos)
- Interception of telecommunications data (network sniffing)
- Malicious probes or scans
- Vendor cloud service levels failures
- Website defacement
- Violation of policies
- Physical breach of facilities

Security Incident Severity

Security incident severity depends almost entirely on the particulars of each incident and the risks they pose to the organization. Similar types of cyber activity such as those listed above may classify either as low or high severity security incidents. Part of the initial triage of any incident involves determining if an incident is low severity or poses a material risk to the Company and is therefore high severity. Low severity incidents are typically handled in isolation through routine Company security processes. High severity incidents require the formalized invocation of this incident response plan, structured documentation and collaboration and communication across a broad group of Company stakeholders.



Data Breaches

High severity security incidents may classify as data breaches if they involve any of the following:

- Unauthorized access to data
- Unauthorized disclosure of data
- Loss or theft of data
- Unauthorized changes to data

Data breaches pose unique risks to the organization and require strict protocols for complying with legal, regulatory and contractual commitments. Therefore the response process for data breaches requires more urgent and rigorous engagement with legal and executive management stakeholders and may involve broader notification requirements to external parties, impacted clients, etc.

Security Incident Response Team

A Security Incident Response Team (SIRT) is responsible for leading the initial handling and response efforts for all security incidents. This includes:

- Evaluating an incident and classifying its severity (low, high or data breach)
- Driving incident response practices based on severity and escalation requirements
- Determining extended team members to initially include on the SIRT based on the characteristics of a given incident

Any member of the core SIRT may perform initial incident triage to determine incident severity and whether or not the severity warrants triggering a formalized response effort. Low severity incidents are handled more informally by routine processes; high severity and data breach incidents always require the designation of a security incident manager and the adherence to a formalized response effort.

The SIRT is led by a Security Incident Manager who is responsible for driving the response process and managing the full lifecycle of high severity security incidents or data breaches. All communications are routed through the Security Incident Manager.

SIRT Core Team

Organizational Team/Function	Primary SIRT Role
Security/Risk	Security Incident Manager; Advisory support on impact assessment and remediation efforts.
Hosting	Technical lead on production environment impact assessment and remediation efforts
Incident Scribe	Lead on documenting the sequence of events of the incident or investigation
Information Technology	Technical lead on business system impact assessment and remediation efforts

SIRT Extended Team

Organizational Team/Function	Primary SIRT Role
Engineering	Technical support for application-related impact assessment, mitigation, and remediation efforts
Quality Assurance	Technical support for application-related impact assessment, mitigation, and remediation efforts
Legal	Advisory support on risk assessment, legal, regulatory, and contractual requirements; advisory support on incident response strategy.
Customer Support & Customer Success	Guidance on assessing customer impact; Support for direct inbound & outbound customer communications
Human Resources	Investigating/addressing internal bad actors, assessing/treating internal workforce impact, internal workforce communication
Public Relations	Support for communications with the media, public, and third-parties/partners/vendors.
Finance/Administration	Guidance on assessing impact; Support for incidents involving financial systems or records; Support assessing/addressing costs associated with events/response efforts.
Facilities	Support for incidents involving workplace physical security or safety; Support for investigating/addressing internal bad actors;

	Support for incidents involving internally managed hosting facilities/infrastructure.
Product Management	Business support for application-related impact assessment and remediation efforts
Executive Management / Board of Directors	Informed of significant risk/impact/cost assessments and related incident/remediation status; Advisory support for significant remediation strategy decisions
Cyber Response Specialist	Advisory support for specialized* cyber incident remediation (*data breach; ransomware); Engages and manages IT Forensics Specialist as appropriate
Cyber Liability Insurance Carrier	Hosts specialized cyber incident hotline; Engages Cyber Response Specialist when appropriate
IT Forensics Specialist	Directs preservation and analysis of information in support of specialized cyber incident investigations/remediations.
Law Enforcement	Support for events involving criminal activity, data breaches, material impact to the Company, or threats to physical safety.
Privacy Legal Specialist	Specialized advisory support on risk assessment, legal, regulatory, and contractual requirements relating to data privacy; advisory support on event response strategy.

The Security Incident Manager may engage any additional internal or external resources as necessary to support the response process.

Security Incident Response Process

The Security Incident Response Process consists of five stages which cover the important conceptual focus areas for an effective end-to-end process:

1. Preparation
2. Detection
3. Observation and Containment
4. Resolution and Recovery
5. Post Mortem and Continuous Improvement

Detection, Observation and Containment, Resolution and Recovery cover the key focus areas during the lifecycle of a security incident. *These process stages do not represent sequential procedural steps for incident response efforts.* The response requirements of individual security incidents are wide-ranging and often fluid throughout the incident lifecycle, requiring iteration and adjustment throughout the response effort. The definitions of the process stages

provide procedural guidance to help direct response efforts and ensure appropriate consideration of each focus area and good form in response execution.

Preparation addresses pre-incident readiness; Follow-up addresses post-incident continuous improvement.

> SOC 2: CC7.4
>
> The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

The high level procedure that applies to all high severity security incidents relies on the Security Incident Manager being the single point of accountability for running response efforts in alignment with the Security Incident Response Process:

The Security Incident Manager

- Builds the team (assembling the incident-specific response team from members of the core and extended team as appropriate)
- Drives the effort (leading team investigation/detection, containment, resolution, and recovery efforts)
- Brokers decisions (orchestrating team assessments/re-assessments of incident classification, scope, and severity, and of remediation strategies and plans)
- Oversees final documentation of the response effort

Stage 1: Preparation

Preparation involves ensuring that incident response procedures are well-defined, current, and effectively communicated to all the appropriate participants/stakeholders so that the organization is ready to execute the procedures crisply.

All key (or potential) participants should undergo annual incident response training and an incident response drill.

The Security Incident Manager is responsible for all aspects of the Preparation stage.

Stage 2: Detection

Detection involves leveraging tools, operational procedures, and communications to quickly and reliably identify security events and incidents, and then subsequently notifying the SIRT Core Team of the incidents.

During the Preparation stage, the Security Incident Manager ensures the readiness of the Detection capability by ensuring that criteria for identifying security incidents are clearly defined and communicated, and that procedures for detecting and reporting incidents are operating effectively.

The Detection stage consists of the following steps

1. A Potential security incident is detected from one or more of many potential channels (for example, a monitoring tool triggers an alert to the DevOps team; an employee reports accidentally exposing sensitive data, etc.)
2. The party who detected the potential security incident reports it to the SIRT Core Team
3. Any SIRT Core Team member assesses if sufficient criteria are met to qualify as a high severity security incident or data breach and if so, accepts security incident
4. Security Incident Manager initiates the security incident documentation process which includes initializing a secure location for the documentation, identifying the incident scribe and communicating guidelines for documenting the response effort

5. Security Incident Manager determines the initial response team members and then assembles the team, briefs them on the incident and relays their responsibilities in supporting the response effort.
6. All high severity security incidents and data breaches require the immediate engagement of the legal team to cooperatively assess potential risk to the organization. The legal team subsequently bears the responsibility to appropriately notify executive management.

Stage 3: Observation and Containment

Containment involves limiting the scope and magnitude of an incident, and should occur alongside further discovery.

The Security Incident Manager is responsible for engaging the support of appropriate extended team members to further investigate the incident while continuously reassessing severity/urgency based on incremental findings to inform a concurrent containment strategy.

Containment tactics may include measures such as:

- Filtering traffic to prevent specific attacks
- Restricting user permissions/system access
- Isolating compromised systems by controlling their access to other resources/systems
- Preserving system information for later review/assessment.

Containment measures often involve significant trade-offs, like disrupting system access to limit potential, but unverified threats. The Security Incident Manager is responsible for brokering agreement from the appropriate business stakeholders to drive a well-informed and decisive containment strategy for each incident at a speed and level of urgency aligned with incident severity. Ultimately, the decision to implement a containment measure is at the discretion of the Security Incident Manager.

The Containment stage consists of the following steps:

1. Security Incident Manager starts orchestration of concurrent investigation and containment efforts
2. Security Incident Manager ensures that the Scribe is accurately documenting the activities and findings
3. Security Incident Manager brokers and documents team agreements on adjustments to incident classification, scope, severity, investigative strategy and containment strategy
4. Security Incident Manager adjusts scope of Security Response Team as appropriate
5. Security Incident Manager communicates to stakeholders on a periodic basis; the Security Incident Manager dictates the cadence of these updates
6. Team iterates on above steps until investigation complete.

Stage 4: Resolution and Recovery

Resolution involves eliminating the threat associated with an incident by identifying and isolating the cause/source and executing remediation efforts to a successful conclusion. Recovery involves restoring the scope of the business impacted by the incident to normal/stable operating conditions.

Examples of Remediation and Recovery measures include:

- Installing patches
- Changing passwords/revoking access
- Adding/adjusting firewall rules
- Removing malware

- Restoring systems from clean backups
- Rebuilding systems from original media
- Replacing compromised files with clean versions
- Following breach notification protocols

The Resolution and Recovery stage consists of the following steps:

1. Security Incident Manager drives team to final determination of incident classification, scope, and severity
2. Security Incident Manager coordinates and documents resolution strategy and plan
3. Security Incident Manager orchestrates remediation activities and executes recovery plan
4. Security Incident Manager determines when resolution criteria have been met, and records when and how they were met
5. Security Incident Manager communicates to stakeholders and oversees public communication as appropriate
6. Security Incident Manager drives and documents final impact assessment.

Stage 5: Post Mortem and Continuous Improvement

Post Mortem involves assessing opportunities for improvement of current capabilities and processes based on learnings from an incident response effort.

The scope of opportunities that should be considered include

- Security infrastructure/capabilities
- Reassessment of enterprise risk
- Policies and procedures
- This security incident response plan

> SOC 2: CC7.5
>
> The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

Post Mortem does not include post-incident response tasks that are associated with an incident , but not part of recovery or resolution. For example, any legal action pursued because of an incident would be outside the scope of the incident response process.

Procedurally, the Security Incident Manager should lead and document follow-up analysis as soon as reasonably possible following incident resolution/recovery.

⚠ Because communicating outside the organization can have legal and business ramifications, **all external breach notifications must be done through the Security Team**, and *only then* **with the advice and consent of Corporate Council** and **Executive Management**.

> SOC 2: CC7.3
>
> The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the Security Documentation Overview.

Document control

> This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	Art Machado	
Author(s)	Art Machado, Angelina Kilmer, Paul Gordon	
Required Approver(s) and Approval Date	Art Machado - VP Information Security	Jun 25, 2025
Review cycle	ANNUAL	
Next review date	Feb 24, 2026	

Version History

Date	Author(s)	Version	Changes
Jun 25, 2025	Art Machado Angelina Kilmer Paul Gordon	4.2	Update on incident classification naming convention
Jun 4, 2025	Art Machado Angelina Kilmer Paul Gordon	4.1	Clarification and update of terminology
Feb 25, 2025	Art Machado Angelina Kilmer Paul Gordon	4.0	Annual review
Nov 1, 2024	Angelina Kilmer	3.5	Changed Policy classification from Confidential to Public
Mar 13, 2024	Art Machado Sarah Zwicker Paul Gordon	3.4	Annual review

Feb 23, 2023	Art Machado Sarah Zwicker	3.3	Annual Review + logo update
Mar 24, 2022	Sarah Zwicker	3.2	Added Privacy considerations and components
Mar 16, 2022	Art Machado Sarah Zwicker	3.1	Title change for VP InfoSec, Annual Review
Jun 3, 2021	Art Machado	3.0	Updated data classifications
Mar 15, 2021	Sarah Zwicker	2.9	Changed owner
Feb 9, 2021	Sarah Zwicker	2.8	Reformatting, policies linked
Jan 26, 2021	John Cole	2.7	Annual review, role title change
Nov 23, 2020	Sarah Zwicker	2.6	Ownership change