Security Event/Incident Response Plan

Version number	3.5
Last Approved	Mar 13, 2024
Classification	PUBLIC

⚠ If you're aware of a potential security issue, or have a security escalation, **please follow the steps here to raise the concern**. We kindly ask that you do not wait until the next working day, and make sure that someone has acknowledged ownership of the concern before you step back from the issue. Working with Hosting | Security Incidents

Overview

Security events 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 events.

The procedures defined in this document ensure that security events 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 events.

Scope

This plan covers any security events involving Company 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 Plan (BCP).

Security Event 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 (which do not classify as Security Incidents)

- observed suspicious behavior 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 (which do not classify as Data Breaches)

- 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

Data Breaches

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

Security Event Response Team

A Security Event Response Team (SERT) is responsible for leading the initial handling and response efforts for all security events. This includes:

- evaluating an event and classifying its severity
- executing event practices based on severity and escalation requirements
- determining extended team members to initially include on the SERT based on the characteristics of a given event

The SERT is led by a Security Event Manager who is responsible for driving the response process and managing the full lifecycle of security events. All communications are routed through the Security Event Manager.

SERT Core Team

Organizational Team/Function	Primary SERT Role
Security/Risk	Security Event 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
CITO	Technical lead on business system impact assessment and remediation efforts

SERT Extended Team

Organizational Team/Function	Primary SERT 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 event 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 events involving financial systems or records; Support assessing/addressing costs associated with events/response efforts.
Facilities	Support for events involving workplace physical security or safety; Support for investigating/addressing internal bad actors; Support for events involving internally managed hosting facilities/infrastructure.
Product Management	Business support for application-related impact assessment and remediation efforts
Executive Management	Informed of significant risk/impact/cost assessments and related event/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 Event Manager may engage any additional internal or external resources as necessary to support the response response process.

Security Event Response Process

The Security Event 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 event. *These process stages do not represent sequential procedural steps for event response efforts.* The response requirements of individual security incidents are wide-ranging and often fluid throughout the event 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-event readiness; Follow-up addresses post-event 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 security events relies on the Security Event Manager being the single point of accountability for running response efforts in alignment with the Security Event Response Process:

The Security Event Manager

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

Stage 1: Preparation

Preparation involves ensuring that event 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 Event 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 then subsequently notifying the SERT Core Team of the events.

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

The Detection stage consists of the following steps

1. A Potential security event 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 event reports it to the SERT Core Team
3. Any SERT Core Team member assesses if sufficient criteria are met to qualify as a security event and if so, accepts security event
4. Security Event Manager creates security event record
5. Security Event Manager assesses and records the initial scope & description of the event and assigns an initial severity classification
6. Security Event Manager determines and initial response team members for the event and then notifies them.

Stage 3: Observation and Containment

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

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

Containment tactics may include measures like

- 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 Event Manager is responsible for brokering agreement from the appropriate business stakeholders to drive a well-informed and decisive containment strategy for each event at a speed and level of urgency aligned with event severity. Ultimately, the decision to implement a containment measure is at the discretion of the Security Event Manager.

The Containment stage consists of the following steps:

1. Security Event Manager starts orchestration of concurrent investigation and containment efforts
2. Security Event Manager ensures that the Scribe is accurately documenting the activities and findings
3. Security Event Manager brokers and documents team agreements on adjustments to event classification, scope, severity, investigative strategy and containment strategy
4. Security Event Manager adjusts scope of Security Response Team as appropriate
5. Security Event Manager communicates to stakeholders on a periodic basis; the Security Event 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 event 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 event 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 Event Manager drives team to final determination of event classification, scope, and severity
2. Security Event Manager coordinates and documents resolution strategy and plan
3. Security Event Manager orchestrates remediation activities and executes recovery plan
4. Security Event Manager determines when resolution criteria have been met, and records when and how they were met
5. Security Event Manager communicates to stakeholders and oversees public communication as appropriate
6. Security Event 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 event response effort.

The scope of opportunities that should be considered include

- Security infrastructure/capabilities
- Reassessment of enterprise risk
- Policies and procedures
- This security event 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-event response tasks that are associated with an event, but not part of recovery or resolution. For example, any legal action pursued because of an event would be outside the scope of the event response process.

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

⚠ Because communicating outside the organization can have legal, ethical, 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 @Sarah Zwicker (Unlicensed) @John Cole	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Mar 13, 2024
Review cycle	ANNUAL	
Next review date	Mar 13, 2025	

Version History

Date	Author(s)	Version	Changes
Nov 1, 2024	@angelina.kilmer	3.5	Changed Policy classification from Confidential to Public
Mar 13, 2024	@Art Machado @Sarah Zwicker (Unlicensed) @Paul Gordon	3.4	Annual review
Feb 23, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	3.3	Annual Review + logo update
Mar 24, 2022	@Sarah Zwicker (Unlicensed)	3.2	Added Privacy considerations and components
Mar 16, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	3.1	Title change for VP InfoSec, Annual Review
Jun 3, 2021	@Art Machado	3.0	Updated data classifications

Mar 15, 2021	@Sarah Zwicker (Unlicensed)	2.9	Changed owner
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	2.8	Reformatting, policies linked
Jan 26, 2021	@John Cole	2.7	Annual review, role title change
Nov 23, 2020	@Sarah Zwicker (Unlicensed)	2.6	Ownership change