Incident Response Plan

Policy Owner: <Policy owner>

Effective Date: <Effective date>

Purpose

This document establishes the plan for managing information security incidents and events, and offers guidance for employees or incident responders who believe they have discovered, or are responding to, a security incident.

Scope

This policy covers all information security or data privacy events or incidents.

Incident and Event Definitions

A security event is an observable occurrence relevant to the confidentiality, availability, integrity, or privacy of company controlled data, systems or networks.

A security incident is a security event which results in loss or damage to the confidentiality, availability, integrity, or privacy of company controlled data, systems or networks.

Incident Reporting & Documentation

Reporting

If a <Company Name> employee, contractor, user, or customer becomes aware of an information security event or incident, possible incident, imminent incident, unauthorized access, policy violation, security weakness, or suspicious activity, then they shall immediately report the information using one of the following communication channels:

- Email help@<Company Name>.com information or reports about the event or incident

Reporters should act as a good witness and behave as if they are reporting a crime. Reports should include specific details about what has been observed or discovered.

Severity

<Team or role responsible for monitoring reports of security incidents or events, e.g., <Company Name> Support Team> shall monitor incident and event tickets and shall assign a ticket severity based on the following categories.

S3/S4 - Low and Medium Severity

Issues meeting this severity are simply suspicions or odd behaviors. They are not verified and require further investigation. There is no clear indicator that systems have tangible risk and do not require emergency response. This includes lost/stolen laptop with disk encryption, suspicious emails, outages, strange activity on a laptop, etc.

S2 - High Severity

High severity issues relate to problems where an adversary or active exploitation hasn't been proven yet, and may not have happened, but is likely to happen. This may include lost/stolen laptop without encryption, vulnerabilities with direct risk of exploitation, threats with risk or adversarial persistence on our systems (e.g.: backdoors, malware), malicious access of business data (e.g.: passwords, vulnerability data, payments information), or threats that put any individual at risk of physical harm.

S1 - Critical Severity

Critical issues relate to actively exploited risks and involve a malicious actor. Identification of active exploitation is required to meet this severity category.

Escalation and Internal Reporting

The incident escalation contacts can be found below in Appendix A.

S1 - Critical Severity: S1 issues require immediate notification to <describe the role/team that should be immediately notified about S1 issues, e.g., IT and/or Engineering> management.

S2 - High Severity: A <type of ticket that should be created in the event of a S2 event or incident, e.g., support> ticket must be completed and the appropriate manager (see S1 above) must also be notified via <channel for notifying the appropriate contact, e.g., email or Slack> with a reference to the ticket number.

S3/S4 - Medium and Low Severity: A <type of ticket that should be created in the event of a S2 event or incident, e.g., support> ticket must be created and assigned to the appropriate department for response.

Documentation

All reported security events, incidents, and response activities shall be documented in <describe where this will be documented, e.g., the ServiceDesk or Salesforce ticket system>.

A root cause analysis may be performed on all verified <S1> security incidents. A root cause analysis report shall be documented and referenced in the incident ticket. The root cause analysis shall be reviewed by the <reviewer of root cause analysis decider of requirement for a port-mortem, e.g., VP of Support, VP of Engineering, and/or the IT Manager> who shall determine if a post-mortem meeting will be called.

Incident Response Process

For critical issues, the response team will follow an iterative response process designed to investigate, contain exploitation, eradicate the threat, recover system and services, remediate vulnerabilities, and document a post-mortem with the lessons of an incident.

Summary

- Event reported
- Triage and analysis
- Investigation
- Containment & neutralization (short term work)
- Recovery & vulnerability remediation
- Hardening & Detection improvements (lessons learned, long term work)

Detailed

- IT Manager or VP of Support will manage the incident response effort
- A central "War Room" will be designated, which may be a physical or virtual location (i.e Slack channel)
- A recurring Incident Response Meeting will occur at regular intervals until the incident is resolved.
- Legal and executive staff will be informed as needed

Incident Response Meeting Agenda

- Update Incident Ticket and timelines
- Document new Indicators of Compromise (IOCs)
- Perform investigative Q&A
- Apply emergency mitigations
- Plan long term mitigations
- Document Root Cause Analysis (RCA)
- Additional items as needed

Special Considerations

Internal Issues

Issues where the malicious actor is an internal employee, contractor, vendor, or partner requires sensitive handling. The incident manager shall contact <direct contact for sensitive information, e.g., HR or the CEO> directly and will not discuss with other employees. These are critical issues where follow-up must occur.

Compromised Communications

Incident responders must have <communication method, e.g., Slack messaging> arranged before listing themselves as incident members. If there are IT communication risks, an out of band solution will be chosen, and communicated to incident responders via <how changes to communication will be communicated if needed, e.g., cell phone>.

Additional Requirements

- Suspected and reported events and incidents shall be documented.
- Suspected incidents shall be assessed and classified as either an event or an incident.
- Incident response shall be performed according to this plan and any associated procedures.
- All incidents shall be formally documented, and a documented root cause analysis shall be performed.
- Suspected and confirmed unauthorized access events shall be reviewed by the Incident Response Team. Breach determinations shall only be made by the <who determines if a breach occurred, e.g., CEO and legal counsel in coordination with executive management>.
- <Company Name> shall promptly and properly notify customers, partners, users, affected parties, and regulatory agencies of relevant incidents or breaches in accordance with <Company Name> policies, contractual commitments, and regulatory requirements.
- This Incident Response Plan shall be reviewed and tested at least <how often the Incident Response Plan will be reviewed, e.g., annually>.

Roles & Responsibilities

Every employee and user of any <Company Name> information resources has responsibilities toward the protection of the information assets. The table below establishes the specific responsibilities of the incident responder roles.

Response Team Members

Role	Responsibility
Incident Manager	The Incident Manager is the primary and ultimate decision maker during the response period. The Incident Manager is ultimately responsible for resolving the incident and formally closing incident response actions. See Appendix A for Incident Manager contact information. These responsibilities include: ● Ensuring the right people from all functions are actively involved at all times ● Status updates are communicated to the appropriate persons at regular intervals ● Incidents are resolved in the immediate term ● Determining necessary follow-up actions ● Assigning follow-up activities to the appropriate people ● Promptly reporting incident details which may trigger breach reporting, in writing to the <person that receives incident details and decides on breach reporting requirement, e.g., Chief Information Officer>.

Incident Response Team (IRT)	The individuals who have been engaged and are actively working on the incident. All members of the IRT will remain engaged in incident response until the incident is formally resolved, or they are formally dismissed by the Incident Manager.
Engineers (Support and Development)	Qualified engineers will be placed into the on-call rotation and may act as the Incident Manager (if primary resources are not available) or a member of the IRT when engaged to respond to an incident. Engineers are responsible for understanding the technologies and components of the information systems, the security controls in place including logging, monitoring, and alerting tools, appropriate communications channels, incident response protocols, escalation procedures, and documentation requirements. When Engineers are engaged in incident response, they become members of the IRT.
Users	Employees and contractors of <Company Name>. Users are responsible for following policies, reporting problems, suspected problems, weaknesses, suspicious activity, and security incidents and events.
Customers	Customers are responsible for reporting problems with their use of <Company Name> services. Customers are responsible for verifying that reported problems are resolved.
Legal Counsel	Responsible, in conjunction with the CEO and executive management, for determining if an incident shall be considered a reportable breach. Counsel shall review and approve in writing all external breach notices before they are sent to any external party.
Executive Management	Responsible, in conjunction with the CEO and legal counsel, for determining if an incident shall be considered a reportable breach. An appropriate company officer shall review and approve in writing all external breach notices before they are sent to any external party. <Company Name> shall seek stakeholder consensus when determining whether a breach has occurred. The <Company Name> CEO shall make a final breach determination in the event that consensus cannot be reached.

Management Commitment

<Company Name> management has approved this policy and commits to providing the resources, tools and training needed to reasonably respond to identified security events and incidents with the potential to adversely affect the company or its customers.

Exceptions

Requests for an exception to this Policy must be submitted to and authorized by the <approver of exceptions to this policy, e.g., IT Manager> for approval. Exceptions shall be documented.

Violations & Enforcement

Any known violations of this policy should be reported to the <receivers of policy violation reports, e.g., IT Manager or the CEO>. Violations of this policy may result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
<1.0>	<29-Apr-2020>	<First Version>	<OWNER>	<APPROVER>

Appendix A – Contact Information

Contacts for IT and Engineering Management as well as executive staff and can be found <where contacts for IRT members can be found, e.g., at the bottom of the On-Call list here: <link>>

Appendix B – Incident Collection Form

Commented [1]: This form can be used to collect information about a security incident. If your process does not include this form, remove this appendix.

General Information	
Incident Detector's Information	
Name:	**Date and Time Detected:**
Title:	
Phone:	**Location Incident Detected From:**
E-mail:	
	Additional Information:

Incident Summary				
Type of Incident Detected:				
Denial of Service	Unauthorized Use	Espionage	Probe	Hoax
Malicious Code	Unauthorized Access	Other:		

Incident Location:	
Site:	
Site Point of Contact:	
Phone:	
Email:	

How was the Incident Detected:	
Additional Information:	
Location(s) of affected systems:	
Date and time incident handlers arrived at site:	

Describe affected information system(s) (one form per system is recommended):

Hardware Manufacturer:	
Serial Number:	
Corporate Property Number (if applicable):	

Is the affected system connected to a network?	Yes	No

Describe the physical security of the location of affected information systems (locks, security alarms, building access, etc.):

Isolate affected systems:

Approval to removal from network?	Yes	No

If YES, Name of Approver:

Date and Time Removed:

If NO, state the reason:

Backup of Affected System(s):

Last System backup successful?	Yes	No

Name of persons who did backup:

Date and time last backups started:

Date and time last backups completed:

Backup Storage Location:

Incident Eradication:

Name of persons performing forensics:

Was the vulnerability (root cause) identified:	Yes	No

Describe:

How was eradication validated: