pivot

Incident Response Plan

Version: 1.0.0

Updated on: September 23, 2025

Purpose

- To establish the plan for managing information security incidents and events.
- To offer 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 impacting non-public Company data.

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 that 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 employee or contractor 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 or message your supervisor about the event or incident
- Send a message to the Security Delegate

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

Severity and Escalation

The Security Delegate shall monitor security incident notifications and assign a severity based on the following categories.

P2/P3 - Low and Medium Severity

This level of severity pertains to incidents that are unconfirmed or exhibit unusual behavior, necessitating further investigation. There is no definitive evidence suggesting a significant risk to systems. Immediate emergency response is not required. Examples include encrypted laptops that are lost or stolen, suspicious emails, system outages, and unusual activities observed on a laptop.

Escalation: Must be tracked and assigned to the appropriate department for response

P1 - High Severity

High severity issues are those where there's a strong likelihood of an attack or exploitation, even though direct evidence of an adversary's presence or active exploitation hasn't been confirmed. These include scenarios like a lost or stolen laptop without encryption, vulnerabilities that are highly exploitable, threats indicating potential or ongoing unauthorized access to our systems (such as backdoors or malware), and unauthorized access to sensitive business data (like passwords, details of vulnerabilities, or payment information).

Escalation: This must be documented and the appropriate manager (see P0 below) must also be notified via Slack with a reference to more information.

P0 - Critical Severity

Critical issues are those involving active exploitation by a malicious actor, or threats that pose a risk of physical harm to any individual. To be classified under this severity category, there must be clear evidence of ongoing exploitation.

Escalation: Immediate notification to senior management.

Incidents will be closed within the following SLAs, when feasible:

Determined Severity	Remediation Time
Low (P3)	90 Days
Medium (P2)	90 Days
High (P1)	14 Days
Critical (P0)	7 Days

Documentation

All reported security events, incidents, and response activities shall be documented and adequately protected in cloud storage and sharing platform or the ticketing system.

A root cause analysis may be performed on all verified P0 security incidents. A root cause analysis report shall be documented and referenced in the incident documentation. The root cause analysis shall be reviewed by the Security Delegate 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 report including the lessons learned from the incident.

Summary

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

Detailed

- Security Delegate will manage the incident response effort
- If necessary, a dedicated Slack channel will be created for the incident
- A recurring, daily Incident Response Meeting will occur at regular intervals until the incident is resolved
- Legal, staff, and 3rd parties (partners and customers) will be informed as required

Incident Response Meeting Agenda

- Update documentation and timelines
- Document new Indicators of Compromise (IOCs)
- Perform investigative Q&A
- Apply emergency mitigations
- External Reporting / Breach Reporting (if necessary)
- Plan long-term mitigations
- Document or update Root Cause Analysis (RCA)
- Additional items as needed

Special Considerations

Internal Issues

When the suspected malicious actor is an internal employee, contractor, vendor, or partner, the situation demands discreet management. In such cases, the incident manager must directly contact the Security Delegate and refrain from discussing the matter with other employees. These are considered critical issues that require immediate and careful follow-up.

Compromised Communications

If there are IT communication risks, an out-of-band solution will be chosen, and communicated to incident responders via mobile phone messaging.

Root Account Compromise

If a cloud provider root account compromise is known or expected, refer to the playbook in Appendix C.

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 on P0 incidents
- Incident responders shall collect, store, and preserve incident-related evidence in accordance with industry guidance and best practices
- Suspected and confirmed unauthorized access events shall be reviewed by the Incident Response Team to determine if a data breach has occurred. Breach determinations shall only be made by the CEO and Security Delegate.
- The company shall promptly and properly notify customers, partners, users, affected parties, and regulatory agencies of relevant incidents or breaches in accordance with Company policies, contractual commitments, and regulatory requirements, as determined by the CEO and Security Delegate.

External Communications and Breach Reporting

Legal and executive staff shall confer with technical teams and Security Delegate in the event of unauthorized access to company or customer systems, networks, and/or data. Legal staff along with the CEO shall determine if breach reporting or external communications are required. Breaches shall be reported to customers, consumers, data subjects, and regulators without undue delay and in accordance with all contractual commitments and applicable legislation.

No personnel may disclose information regarding incidents or potential breaches to any third party or unauthorized person without the approval of legal and/or executive management.

Mitigation and Remediation

Legal and Security Delegate shall determine any immediate or long-term mitigations or remedial actions that need to be taken as a result of an incident or breach. In the event that mitigations or remedial actions are needed, executive staff shall direct personnel with respect to planning, communicating, and executing those activities.

Cooperation with Customers, Data Controllers and Authorities

As needed and determined by legal and Security Delegate, the company shall cooperate with customers, Data Controllers, and regulators to fulfill all of its obligations in the event of an incident or data breach.

Roles & Responsibilities

Every employee and user of any Company 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
Security Delegate	The primary and ultimate decision maker during the response period. Ultimately responsible for resolving the incident and formally closing incident response actions. See Appendix A for contact information. These responsibilities include: • Ensuring the right people from all functions are actively involved as appropriate • Communicating status updates to the appropriate person or teams at regular intervals • Resolving incidents 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 CEO
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 Security Delegate (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	Company employees and contractors, referred to as 'users', are responsible for adhering to company policies. They must report any issues, suspected problems, vulnerabilities, unusual activities, and security incidents or events.
Customers	Customers are encouraged to report problems with their use of Company services.
Legal Counsel	Responsible, in conjunction with the CEO and Security Delegate, for determining if an incident presents legal or regulatory exposure as well as whether 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. The company shall seek stakeholder consensus when determining whether a breach has occurred. The Company CEO shall make a final breach determination in the event that consensus cannot be reached.

Management Commitment

Company 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 Security Delegate for approval. Exceptions shall be documented.

Violations & Enforcement

Any known violations of this policy should be reported to the Security Delegate. 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.

Appendix A – Contact Information

Contacts for company personnel as well as Security Delegate can be found in Slack.

Appendix B – Incident Collection Form

Incident Detectors Information	
Name	
Title	
Phone	
Email	
Incident Information	
Incident Overview	
Date and Time Detected	
Location Incident Detected From	
Additional Information	
Type of Incident	_ Denial of Service _ Unauthorized Use _ Hoax _ Probe _ Malicious Code _ Unauthorized Access _ Other:
Incident Location	
Site	
Site Point of Contact	
Phone	

Email	
Additional Information	
How was the Incident Detected?	
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 remove from the network? If Yes, please provide the name of Approver If No, provide Reason	_ Yes _ No Name:

	Reason:
Date and Time Removed	
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
Please describe the Vulnerability	
How was eradication validated	

Appendix C – Cloud Provider Root Account Compromise Playbook

Incident Response Runbook – Root Usage

Objective

The objective of this runbook is to provide specific guidance on how to manage Root cloud account usage. This runbook is not a substitute for an in-depth Incident Response strategy. This runbook focuses on the IR lifecycle:

- Establish control.
- Determine impact.
- Recover as needed.
- Investigate the root cause.
- Improve.

The Indicators of Compromise (IOC), initial steps (stop the bleeding), and the detailed CLI commands needed to execute those steps are listed below.

The Indicators of Compromise (IOC) and remediation steps (stop the bleeding) are listed below:

Indicators of Compromise

- Activity that is abnormal for the account:
    - Creation of new users.
    - Monitoring/logging turned off.
    - Notifications paused.
    - Automated actions paused.
- Launching of new or unexpected resources.
- Changes to the contacts on the account.

Steps to Remediate – Establish Control

Cloud provider documentation for a possible compromised account should call out the specific tasks listed below.

1. Contact Cloud provider support as soon as possible.
2. Change and rotate Root password and add an MFA device associated with Root.
3. Rotate passwords, access/secret keys, and CLI commands relevant to remediation steps.
4. Review actions taken by the root user.
5. Open the runbooks for those actions.
6. Close incident.
7. Review the incident and understand what happened.
8. Fix the underlying issues, implement improvements, and update the runbook as needed.

Further Action Items – Determine Impact

Review created items and mutating calls. There may be items that have been created to allow access in the future. Some things to look at:

- Cross-account roles.
- Users.
- Storage.
- Virtual servers.

- Other cloud services in production accounts

Document History

Version	Date	Description	Written by	Approved by
1.0.0	08/14/2025	Initial Version	Ryan Rich	Bishal Das