Warmbox

Incident Response Plan

Effective Date: 02/01/2025

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 aWarmbox 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 contact@warmbox.ai 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

Warmbox Support Team shall monitor incident and event tickets and shall assign a ticket severity based on the following categories.

P2/P3 - 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.

P1 - 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).

P0 - Critical Severity

Critical issues relate to actively exploited risks and involve a malicious actor or threats that put any individual at risk of physical harm. Identification of active exploitation is required to meet this severity category.

Escalation and Internal Reporting

P0 - Critical Severity: P0 issues require immediate notification to IT and/or Engineering management.

P1 - High Severity: A support ticket must be created and the appropriate manager (see P0 above) must also be notified via email or Slack with a reference to the ticket number.

P2/P3 - Medium and Low Severity: A 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 and adequately protected in the ServiceDesk or Salesforce ticket 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 ticket. The root cause analysis shall be reviewed by the 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 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

- IT Manager or VP of Support will manage the incident response effort
- If necessary, 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 required

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 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 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 cell phone.

Root Account Compromise

If an AWS root account compromise is known or expected, refer to the playbook in Appendix B.

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
- Incident responders shall collect, store, and preserve incident-related evidence in accordance with industry guidance and best practices such as NIST SP 800-86 'Guide to Integrating Forensic Techniques into Incident Response'
- Suspected and confirmed unauthorized access events shall be reviewed by the Incident Response Team. Breach determinations shall only be made by the CEO and legal counsel in coordination with executive management
- Warmbox shall promptly and properly notify customers, partners, users, affected parties, and regulatory agencies of relevant incidents or breaches in accordance withWarmbox policies, contractual commitments, and regulatory requirements, as determined by the CEO, Legal Department
- This Incident Response Plan shall be reviewed and formally tested at least annually. Results of IR plan testing activities including findings and lessons learned will be formally documented and maintained to support security, compliance and audit requirements

External Communications and Breach Reporting

Legal and executive staff shall confer with technical teams 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 incident or potential breaches to any third party or unauthorized person without the approval of legal and/or executive management.

Mitigation and Remediation

Legal and executive staff 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.

Roles & Responsibilities

Every employee and user of anyWarmbox 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. 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 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 ofWarmbox. 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 ofWarmbox 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 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. Warmbox shall seek stakeholder consensus when determining whether a breach has occurred. TheWarmbox CEO shall make a final breach determination in the event that consensus cannot be reached.

Management Commitment

Warmbox 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 IT Manager for approval. Exceptions shall be documented.

Violations & Enforcement

Any known violations of this policy should be reported to the 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
1.0	02/01/2025	First Version

Appendix A – Incident Collection Form

General Information

Incident Detector's Information

Name: ______________________

Title: ______________________

Phone: ______________________

E-mail: ______________________

Date and Time Detected: ______________________

Location Incident Detected From: ______________________

____

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:

Appendix B – AWS 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 AWS 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.

Assumptions

- CLI configured and installed.

- Reporting process is already in place.
- Trusted Advisor is active.
- Security Hub is active.

Indicators of Compromise

- Activity that is abnormal for the account.
  - Creation of IAM users.
  - CloudTrail turned off.
  - Cloudwatch turned off.
  - SNS paused.
  - Step Functions paused.
- Launching of new or unexpected AMIs.
- Changes to the contacts on the account.

Steps to Remediate – Establish Control

AWS documentation for a possible compromised account calls out the specific tasks listed below. The documentation for a possible compromised account can be found at: What do I do if I notice unauthorized activity in my AWS account?

1. Contact AWS Support and TAM 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 are may be items that have been created to allow access in the future. Some things to look at:

- IAM Cross account roles.
- IAM Users.
- P2 buckets.
- EC2 instances.
- [Your application and infrastructure will drive this list.]