Incident Response Plan

Policy Owner: Leonard Henriquez

Effective Date: December 22, 2022

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 Capsule SAS 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 leonard@capsule.io 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., Capsule SAS 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).

S1 - 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

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

S1 - Critical Severity: S1 issues require immediate notification to Engineering management.

S2 - High Severity: A support ticket must be completed and the appropriate manager (see S1 above) must also be notified via email or Slack with a reference to the ticket number.

S3/S4 - 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 Notion.

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 CTO 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
- External Reporting / Breach Reporting
- 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 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 D.

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 in coordination with executive management
- Capsule SAS shall promptly and properly notify customers, partners, users, affected parties, and regulatory agencies of relevant incidents or breaches in accordance with Capsule SAS policies, contractual commitments, and regulatory requirements, as determined by the CEO
- 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.

Cooperation with Customers, Data Controller and Authorities

As needed and determined by legal and executive staff, 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 Capsule SAS 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 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 CTO
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 Capsule SAS. 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 Capsule SAS 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. Capsule SAS shall seek stakeholder consensus when determining whether a breach has occurred. The Capsule SAS CEO shall make a final breach determination in the event that consensus cannot be reached.

Management Commitment

Capsule SAS 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 CTO for approval. Exceptions shall be documented.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO. 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	22-dec-2022	First Version	Léonard Henriquez	Dan Elkaïm

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:

- Dan Elkaïm - CEO : +33 6 34 44 00 54
- Robin Philibert - COO : +33 6 80 89 36 12
- Léonard Henriquez - CTO : +33 6 01 75 37 67

Appendix B - Incident Collection Form

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:				

Appendix C - HIPAA Breach Procedures for Protected Health Information (PHI)

Procedures

In the event that [customer name] identifies a potential breach of PHI occurs, the following procedures shall be followed.

Step 1: Identification (Discovery)

A breach of PHI will be deemed "discovered" as of the first day [customer name] knows of the breach or, by exercising reasonable diligence, would or should have known about the breach.

If a potential breach is discovered, it is very time sensitive and must be immediately reported.

The following is full description of what constitutes PHI

- PHI is any health information that can be tied to an individual to include the following:

1. Names (Full or last name and initial)
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) directly related to an individual including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers (including serial numbers and license plate numbers)
13. Device identifiers and serial numbers
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

There are also additional standards and criteria to protect individual's privacy from reidentification. Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. For example, a subject's initials cannot be used to code their data because the initials are derived from their name. Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study. In other words, the information would still be considered identifiable if there was a way to identify the individual even though all of the 18 identifiers were removed.

Step 2: Initial Reporting / Escalation

If there is belief that a potential breach of PHI has occurred, the designated Security and/or Privacy Officer, or their designated representative, must be immediately notified.

Please provide all of the information available at the time of the initial regarding the potential breach, to include the following:

- Names
- Dates
- The nature of the PHI potentially breached
- The manner of the disclosure (fax, email, mail, verbal)
- All employees involved
- The recipient
- All other persons with knowledge
- Any associated written or electronic documentation that may exist.

Notification and associated documentation may itself contain PHI and should only be given to the designated Security and/or Privacy Officer, or their designated representative.

Do not discuss the potential breach with anyone else, and do not attempt to conduct an investigation as these tasks will be performed by the designated Security and/or Privacy Officer, or their designated representative.

Step 3: Investigation

Upon receipt of notification of a potential breach the designated Security and/or Privacy Officer, or their designated representative shall promptly conduct an investigation.

The investigation shall include the following activities:

- Interviewing employees involved
- Collecting written documentation
- Completing all appropriate documentation
- Forensic investigation (optional depending on incident)

The designated Security and/or Privacy Officer, or their designated representative, shall retain all documentation related to potential breach investigations, in accordance with established record retention requirements, or for a minimum of six years, whichever is greater.

Step 4: Risk Assessment and Recommendation

Upon completion of the investigation, the designated Security and/or Privacy Officer, or their designated representative, shall perform a Risk Assessment to determine if the use or disclosure of PHI constitutes a breach and requires further notification to the Covered Entity.

The designated Security and/or Privacy Officer, or their designated representative, shall appropriately document the Risk Assessment and make a recommendation to executive management and/or legal counsel regarding whether notification to the Covered Entity of the potential breach would be prudent.

When executing the risk assessment, a "reasoned judgment" standard will be applied to the incident which shall be fact specific, and shall include consideration of the following factors:

- Did the disclosure involve Unsecured PHI in the first place?
- Who impermissibly used or disclosed the Unsecured PHI?
- To whom was the information impermissibly disclosed?
- Was it returned before it could have been accessed for an improper purpose?
- What type of Unsecured PHI is involved and in what quantity?
- Was the disclosure made for any improper purpose?
- Is there the potential for significant risk of financial, reputational, or other harm to the individual whose PHI was disclosed?
- Was immediate action taken to mitigate any potential harm?
- Do any of the specific breach exceptions apply?

Step 5: Final Determination

[customer name]'s executive management in collaboration with legal counsel shall, after review of the evidence and risk assessment, have final authority to determine whether a breach of PHI occurred and what, if any, further action is warranted.

Step 6: Notification

In the event that [customer name]'s executive management and/or legal counsel determines that notice to the Covered Entity is warranted, [customer name]'s executive management and/or legal counsel or the designated representative shall promptly prepare and transmit a notice to the Covered Entity.

Timing of Notification

[customer name] shall notify the Covered Entity "without unreasonable delay" but no later than 60 days after discovery and/or notification of the breach, as required by law.

[customer name] Service and Business Associate Agreements provides that [customer name] is an independent contractor; therefore, the Covered Entity's time to provide the requisite notice begins to run on the date that [customer name] notifies the Covered Entity of the breach.

Delay of Notification

Unjustified Delay

If it appears to the designated Security and/or Privacy Officer, or their designated representative, that their investigation will not be completed within a reasonable time, executive management and/or legal counsel shall be informed to ensure that the Covered Entity will be notified before completion of the investigation.

Law Enforcement Delay

A delay in notification is permissible if a law enforcement official states that a breach notification would impede a criminal investigation or cause damage to national security

1. If a law enforcement request is received, the law enforcement statement must be in writing and must specify the length of the delay required.
2. If the request for a delay in notification is oral, [customer name] must document the statement and request written confirmation within 30 days. If no written request for a delay is received within that time, [customer name] must send notification of the breach to the Covered Entity.

Content of Notification

Any notification to the Covered Entity (CE) provided by [customer name] shall include all information as required by law, but at a minimum, will contain the following content:

- Identification of each individual whose PHI is believed to have been breached
- The date of the incident discovery
- The date of disclosure
- The facts and circumstances surrounding the disclosure
- All associated documentation
- All other available information known to [customer name] that the Covered Entity will be required to include in its own Notice to the individual(s).

Any additional information regarding the breach that [customer name] discovers after the initial notice to the Covered Entity be promptly provided to the Covered Entity as required by law.

Any notice to the Covered Entity shall be sent via first class mail with a return receipt requested and the return receipt as well as a copy of the Covered Entity Notice shall be kept with related documentation and retained in accordance with established record retention requirements or for a minimum of six years, whichever is greater.

Step 7: Documentation

All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate that all appropriate steps were completed. All supporting documentation associated with the potential breach shall be kept on file in accordance with established record retention requirements or for a minimum of six years, whichever is greater.

HIPAA Breach Check List

- Following any actual or suspected breach of unsecured electronic protected health information (ePHI), [customer name] must notify the affected Covered Entity (CE).
- Notify the Security Officer and/or Privacy Officer and Legal of a suspected ePHI breach, within four (4) hours.
- Incident Response Team investigates suspected breach and execute risk assessment to verify if ePHI data has been compromised.
- Incident Response Team shall complete a Breach Notification Report
- Incident Response Team provides the completed Breach Notification Report to the Security Officer and/or Privacy Officer for review and approval
- Security and/or Privacy Officer review and approve the submitted Breach Notification Report
- Security and/or Privacy Officer provide a copy of the final Breach Notification Report to [customer name] Legal department within one (1) business day after approval
- Legal reviews Breach Notification Report and submits the report to the Covered Entity through approved communication channels
- Legal will ensure that notification to the Covered Entity occurs no later than sixty (60) calendar days following the initial discovery of a breach or suspected breach, unless delayed by an appropriate law enforcement agency.

HIPAA Breach Notification Content and Template

The Breach Notification Report to the Covered Entity (CE) notification must include the following information.

- Identification of each individual associated with the affected Covered Entity (CE) whose ePHI was suspected to have been accessed, acquired, used, or disclosed (to the extent possible).
- Any other information that the covered entity is required to include in notification to the affected individual under CFR 164.404(c) which includes:
    - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
    - A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
    - Any steps individuals should take to protect themselves from potential harm resulting from the breach.

HIPAA Breach Notification Template

Information Security: HIPAA / ePHI Breach Notification Report	
Incident Number: [###-MMYYYY or Ticket #]	
Other Incidents Related to this Incident:	
Breach Incident Status	(i.e., New, In progress, Forwarded for investigation, Resolved)
Incident Summary	Description of what happened and is known to date
Incident Description	Date and Time Incident Discovered:
Date and Time Incident Reported:	
Date and Time Incident Occurred:	
Place of Incident:	
Personnel Involved in Incident:	
Type and Volume of Information Involved:	
Accessibility/Vulnerability of ePHI / Protective Controls in Place: (e.g. Encryption, etc.):	
Indicators of Compromise Related to the Incident:	
Root Cause of Incident:	
Awareness of Incident (who knows about it now):	
Initial Risk Assessment	Number of Individuals Potentially Affected:
Potential Privacy Breach (Yes/No):	
Risk to Individuals (Types and Extents):	
Financial Risk to Organization:	
Legal/Contractual Risk to Organization:	
Regulatory Risk to Organization:	
Public Relations Risk to Organization:	
ePHI Accessed or Modified in an Unauthorized Manner (Yes / No):	
Steps Taken	Current Actions Taken:
Evidence Gathered / Chain of Custody:	
People Contacted: (e.g., system owners, system administrators, Law enforcement, outside counsel, forensics investigators):	
Data Breach Services Provider Contacted:	
Agencies Notified:	
Close or Move to Investigation Phase and Why:	
Notification	Covered Entity(s) (CE) Affected:
Date Covered Entity(s) (CE) Notified:	
Method(s) used to Notify Covered Entity(s) (CE):	
Notification Record (Ticket # Documenting Notification):	
System Generated List of Individuals Affected Attached (Required):	
Supporting Details:	
Recommendations	Immediate Notification Requirements: Affected Covered Entities MUST be notified within sixty (60) days of a suspected breach.

Priorities and Considerations for Further Investigation	
Next Steps to be Taken (e.g., Rebuild the host, upgrade an application, implement additional controls, etc.).	
Recommendations for Affected Individuals:	

Appendix D - 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.
- S3 buckets.
- EC2 instances.