Incident Response Plan

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.

Reporting

If a Freelance Labs Inc. DBA Braintrust 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:

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

IT Department shall monitor incident and event tickets and shall assign a ticket severity based on the following categories.

P2/P3 - Medium and Low 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

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

Severity	Escalation Path
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 Jira 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 ticket. The root cause analysis shall be reviewed by the CEO or CISO 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 CHRO directly and will not discuss with other employees. These are critical issues where follow-up must occur.

Compromised communication

Incident responders must have Slack messaging arranged before listing themselves as part of the incident response team. 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

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 Freelance Labs Inc. DBA Braintrust 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:

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 Freelance Labs Inc. DBA Braintrust. 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 Freelance Labs Inc. DBA Braintrust 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. Freelance Labs Inc. DBA Braintrust shall seek stakeholder consensus when determining whether a breach has occurred. The Freelance Labs Inc. DBA Braintrust CEO shall make a final breach determination in the event that consensus cannot be reached.

Management commitment

Freelance Labs Inc. DBA Braintrust 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 CEO for approval. Exceptions shall be documented.

Violations & enforcements

Any known violations of this policy should be reported to the CISO. 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 history

Version	Date	Description	Author	Approver
2.0	Jul 7, 2025	Version 2.0	Michael Saukulak	[Approver]

Appendix A — Contact information

Contacts for IT and Engineering Management as well as executive staff and can be found Braintrust Communications Protocols Policy: https://docs.google.com/document/d/1k84mbcLMfc6V3MTTIhFIisrlGUefdzvGrWEPMCy48HU/edit?tab=t.0#bookmark=id.6zgoh61asxwc.

Appendix B — Incident collection form

General Information

Incident detector's information

Name:	_____	**Date and time detected:**	_____
Title:	_____	**Location incident detected from:**	_____
Phone:	_____	**Additional information:**	_____
Email:	_____		

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 Yes No

system connected to a network?

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

_____
_____
_____

_____
_____
_____

Isolate affected systems

Approval to remove 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 the 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 Freelance Labs Inc. DBA Braintrust 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 Freelance Labs Inc. DBA Braintrust 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

There are also additional standards and criteria to protect individuals' 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:

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:

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:

Step 5: Final Determination

Freelance Labs Inc. DBA Braintrust'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 Freelance Labs Inc. DBA Braintrust's executive management and/or legal counsel determines that notice to the Covered Entity is warranted, Freelance Labs Inc. DBA Braintrust's executive management and/or legal counsel or the designated representative shall promptly prepare and transmit a notice to the Covered Entity.

Any additional information regarding the breach that Freelance Labs Inc. DBA Braintrust 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

HIPAA Breach Notification Content and Template

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

HIPAA breach notification template

Appendix D — AWS root account compromise playbook

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:

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

Assumptions

Indicators of Compromise

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?

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: