

Incident Response Plan

Policy Owner: Alex Iglesias

Effective Date: September 18th, 2023

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 Finsweet 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:

- Slack message to concerned members in a channel or group chat
- WhatsApp, if the concerned members are unavailable on Slack

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.

1. Copy the [Incident Collection Form](#) Slack template to your Slack account.

2. After the form is filled, share it with the concerned team (including CTO/FSO and CM).
3. [Contact the team on WhatsApp](#), if they're unavailable on Slack.

Severity

The Technical Development 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 Finsweet Security Officer (FSO).

S2 - High Severity: A ticket labeled "Urgent" must be created and the appropriate manager must be notified via Slack with a reference to the ticket number.

S3/S4 - Medium and Low Severity: A 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 a private page in Finsweet's Notion space.

A root cause analysis may be performed on all verified S1 and S2 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 FSO who shall determine if a post-mortem meeting will be called.

Trend analysis of past incidents: Finsweet conducts trend analysis of past incidents to enhance our proactive approach to incident management. This analysis involves a thorough examination of historical incidents, including their nature, impact, and resolution, with the goal of identifying recurring patterns. For a comprehensive overview of the trends in past incidents, staff and users are encouraged to visit our incident status pages at <https://status.wized.com/> and <https://status.finsweet.com/>, which provide real-time information on service availability and incidents. These pages provide transparency into past incidents, their resolutions, and trends.

Incident Response Process

For critical issues, the Technical Development 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

- Technical Development team will manage the incident response effort
- If necessary, a central "War Room" will be designated in Slack
- 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 FSO and Human Resources Office (HRO) 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 a Google Cloud 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 FSO.
- Finsweet shall promptly and properly notify customers, partners, users, affected parties, and regulatory agencies of relevant incidents or breaches in accordance with Finsweet policies, contractual commitments, and regulatory requirements, as determined by the CEO.

- This Incident Response Plan shall be reviewed and formally tested at least once per year. 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

Executive staff shall confer with the Finsweet Security Officer (FSO) and Technical Developer team in the event of unauthorized access to company or customer systems, networks, and/or data. The FSO and 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

The FSO 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 the FSO, 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 Finsweet 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 Finsweet Security Officer (FSO) or Human Resources Officer (HRO).
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.
Technical Developers (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 Finsweet. 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 Finsweet 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.
CEO	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. Finsweet shall seek stakeholder consensus when determining whether a breach has occurred. The Finsweet CEO shall make a final breach determination in the event that consensus cannot be reached.

Management Commitment

Finsweet 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 FSO for approval. Exceptions shall be documented.

Violations & Enforcement

Any known violations of this policy should be reported to the FSO. 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	17-Jul-2023	Submit for approval	Alex Iglesias	Joe Krug
1.1	18-Sep-2023	Added "Trend analysis of past incidents"	Alex Iglesias	Joe Krug
1.2	25-Apr-25	Updated "Reporting" and "Appendix B"	Rohan Ganachari	Alex Iglesias

Appendix A - Contact Information

Contacts for IT and Engineering Management as well as executive staff and can be found <https://www.notion.so/finsweet/deecf64b83dc41d8829a6e05a9ec4a3c?v=5b1f0ae850c4480aa39577f0721fa489&pvs=4>

Appendix B - Incident Collection Form

Incident Collection Form can be found at <https://finsweet.slack.com/docs/T1V13UTS5/F087VQ62UG0>

Incident Response Plan can be found at <https://www.notion.so/finsweet/Incident-Response-Plan-f7cccdca2c44a659443e1caca67ffec?pvs=4>

Appendix D - Google Cloud Account Compromise Playbook

Incident Response Runbook - Root Usage

Objective

The objective of this runbook is to provide specific guidance on how to manage Root Google 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.

Assumptions

- CLI configured and installed.
- Reporting process is already in place.
- Security Command Center.

Indicators of Compromise

- Activity that is abnormal for the account.
 - Creation of IAM users.
 - Cloud Audit Logs turned off.
 - Cloud Monitoring turned off.
- Launching of new or unexpected AMLs.
- Changes to the contacts on the account.

Steps to Remediate - Establish Control

Google Cloud 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 Google Cloud account?](#)

1. Contact Google Cloud 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 may be items that have been created to allow access in the future. Some things to look at:

- IAM Cross account roles.
- IAM Users.
- Cloud Storage buckets.
- App Engine instances.
- Cloud Functions.