



Operations Security Policy

Policy Owner: Alex Iglesias

Effective Date: August 17th, 2023

Purpose

To ensure the correct and secure operation of information processing systems and facilities.

Scope

All Finsweet information systems that are business critical and/or process, store, or transmit company data. This policy applies to all systems used by Finsweet, including but not limited to, desktops, laptops, servers, mobile devices, and any other endpoints used by employees, contractors, third-party vendors, and any other individuals who utilize Finsweet's systems, networks, and resources for work purposes, including those installed on personally-owned devices. The policy encompasses all devices and platforms used in the remote work environment and ensures that appropriate security controls are applied to mitigate risks associated with remote work and the use of personal devices.

Operations Security

Documented Operating Procedures

Both technical and administrative operating procedures shall be documented as needed and made available to all users who need them.

Change Management

Changes to the organization, business processes, information processing facilities, production software and infrastructure, and systems that affect information security in the production environment and financial systems shall be tested, reviewed, and approved prior to production deployment. Changes must meet business requirements, reduce the risk of service disruption, and avoid adverse effects on service quality. All significant changes to in-scope systems and networks must be documented.

Change management processes shall include:

- Processes for planning and testing of changes, including remediation measures
- Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform
- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders
- Documentation of all emergency changes and subsequent review
- A process for remediating unsuccessful changes
- Emergency changes that require expedited approval and implementation must be classified appropriately.
- A retrospective review of the emergency change process should be conducted to identify any improvements that can be made to incorporate into future change management processes.

Capacity Management

The use of processing resources and system storage shall be monitored and adjusted to ensure that system availability and performance meets Finsweet requirements.

Human resource skills, availability, and capacity shall be reviewed and considered as a component of capacity planning and as part of the annual risk assessment process.

Scaling resources for additional processing or storage capacity, without changes to the system, can be done outside of the standard change management and code deployment process.

Separation of Development, Staging and Production Environments

Development and staging environments shall be strictly segregated from production SaaS environments to reduce the risks of unauthorized access or changes to the operational environment. Confidential production customer data must not be used in development or test environments without the express approval of the Finsweet Security Officer (FSO).

Refer to the [Data Management Policy](#) for a description of Confidential data. If production customer data is approved for use in the course of development or testing, it shall be scrubbed of any such sensitive information whenever feasible.

Systems and Network Configuration, Hardening, and Review

Systems and networks shall be provisioned and maintained in accordance with the configuration and hardening standards described in Appendix A to this policy.

Firewalls and/or appropriate network access controls and configurations shall be used to control network traffic to and from the production environment in accordance with this policy.

Production network access configuration rules shall be reviewed at least annually. Prior approval is required for any needed changes.

Protection from Malware

In order to protect the company's infrastructure against the introduction of malicious software, detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Anti-malware protections shall be utilized on all company-issued endpoints except for those running operating systems not normally prone to malicious software. The anti-malware protections utilized shall be capable of detecting all common forms of malicious threats and performing the appropriate mitigation activity (such as removing, blocking or quarantining). Company email is managed under Google Workspace and utilizes threat detection for email communication.

Finsweet should scan all files upon their introduction to systems, and continually scan files upon access, modification, or download. Anti-malware definition and engine updates should be configured to be downloaded and installed automatically whenever new updates are available. Known or suspected malware incidents must be reported as a security incident.

It is a violation of company policy to disable or alter the configuration of anti-malware protections without authorization.

Information Backup

The need for backups of systems, databases, information and data shall be considered and appropriate backup processes shall be designed, planned and implemented. Backup procedures must include procedures for maintaining and recovering customer data in accordance with documented SLAs. Security measures to protect backups shall be designed and applied in accordance with the confidentiality or sensitivity of the data. Backup copies of information, software and system images shall be taken regularly to protect against loss of data. Backups and restore capabilities shall be periodically tested, not less than annually.

Backups must be stored separately from the production data location.

Finsweet does not regularly backup user devices like laptops. Users are expected to store critical files and information in company-sanctioned file storage repositories.

Backups are configured to run daily on in-scope systems. The backup schedules are maintained within the backup application software.

A backup restore test should be performed at least annually to validate the backup data and backup process.

Logging & Monitoring

Production infrastructure shall be configured to produce detailed logs appropriate to the function served by the system or device. Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and reviewed through manual or automated processes as needed. Appropriate alerts shall be configured for events that represent a significant threat to the confidentiality, availability or integrity of production systems or Confidential data.

Logging should meet the following criteria for production applications and supporting infrastructure:

- Log user log-in and log-out
- Log CRUD (create, read, update, delete) operations on application and system users and objects
- Log security settings changes (including disabling or modifying of logging)
- Log application owner or administrator access to customer data (i.e. Access Transparency)
- Logs must include user ID, valid timestamp, type of action performed, and object of this action.
- Logs must be stored for at least 30 days, and should not contain sensitive data or payloads

Protection of Log Information

Logging facilities and log information shall be protected against tampering and unauthorized access.

Administrator & Operator Logs

System administrator and system operator activities shall be logged and reviewed and/or alerted in accordance with the system classification and criticality.

Data Restore Logs

In the event the company needs to restore production data containing PII from backups, either for the purposes of providing services or for testing purposes, shall be logged or tracked in auditable tickets.

Clock Synchronization

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to network time servers using reputable time sources.

File Integrity Monitoring and Intrusion Detection

Finsweet production systems shall be configured to monitor, log, and self-repair and/or alert on suspicious changes to critical system files where feasible.

Alerts shall be configured for suspicious conditions and engineers shall review logs on a regular basis.

Unauthorized intrusions and access attempts or changes to Finsweet systems shall be investigated and remediated in accordance with the [Incident Response Plan](#).

Control of Operational Software

The installation of software on production systems shall follow the change management requirements defined in this policy.

Technical Vulnerability Management

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities shall be evaluated, and appropriate measures taken to address the associated risk. A variety of methods shall be used to obtain information about technical vulnerabilities, including vulnerability scanning, and review of external vendor alerts.

Vulnerability scans shall be performed on public-facing systems in the production environment at least monthly.

The Technical Development department shall evaluate the severity of vulnerabilities identified from any source, and if it is determined to be a risk-relevant critical or high-risk vulnerability, the FSO will be notified and a ticket will be created. The Finsweet assessed severity level may differ from the level automatically generated by scanning software or determined by external researchers based on Finsweet's internal knowledge and understanding of technical architecture and real-world impact/exploitability. Tickets are assigned to the system, application, or platform owners for further investigation and/or remediation.

Vulnerabilities assessed by Finsweet shall be patched or remediated in the following timeframes:

Determined Severity	Remediation Time
Critical	5 Days
High	30 Days
Medium	60 Day
Low	90 Days
Informational	As needed

Tickets for any vulnerability which cannot be remediated within the standard timeline must show a risk treatment plan and planned remediation timeline.

Restrictions on Software Installation

Rules governing the installation of software by users shall be established and implemented in accordance with the Finsweet [Information Security Policy](#).

Information Systems Audit Considerations

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

Systems Security Assessment & Requirements

Risks shall be considered prior to the acquisition of, or significant changes to, systems, technologies, or facilities. Where requirements are formally identified, any relevant security requirements shall be included. The acquisition of new suppliers and services shall be made in accordance with the [Third-Party Management Policy](#).

The company shall perform an annual network security assessment that includes a review of major changes to the environment such as new system components and network topology.

Exceptions

Requests for an exception to this policy must be submitted to the FSO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the FSO or Human Resources Officer (HRO). Violations of this policy can 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	07-Jul-2023	Submit for approval	Alex Iglesias	Joe Krug
1.1	17-Aug-2023	Technical Vulnerability Management: - Vulnerability Scans updated to Monthly - Remediation Time updated for Critical & High (Determined Severity)	Alex Iglesias	Joe Krug
1.2	23-May-2024	Content updated. Refer Notion.	Alex Iglesias	Joe Krug

APPENDIX A - Configuration and Hardening Standards

Application Hardening

The purpose of this Application Hardening policy is to establish guidelines and procedures for securing and hardening applications used by employees of Finsweet. This Application Hardening policy applies to all employees of Finsweet who utilize applications for work-related activities.

Application Access Control

- Only authorized employees should have access to applications based on their job responsibilities and the principle of least privilege.
- Access to applications should be granted through secure authentication mechanisms, such as unique usernames and strong passwords or other multifactor authentication methods.

Removal of Default Passwords

- All applications must be deployed and configured with strong, unique passwords for administrative and user accounts.
- Default passwords provided by application vendors or system administrators must be changed before deploying applications into production.

Password Best Practices

- Passwords used within applications should adhere to Finsweet's password policy, which includes requirements for complexity, length, and regular password changes.
- Passwords should not be shared or reused across multiple applications or systems.

Account Lockout Policy

- Applications should be configured with an account lockout policy that locks user accounts after a specified number of unsuccessful login attempts.
- The lockout duration and reset process should be defined to prevent unauthorized access while allowing legitimate users to regain access.

Address baseline config management and deployment per control 3.4, 7.1

Servers and Virtual Machines

This is the standard for system-level server and virtual server (VM) configuration hardening. Some customization to these settings may be required to configure the system for its specific target environment, such as setting the proper names, groups, authentication settings, and other personalization options.

In addition to the requirements to secure systems to the baseline outlined above, all physical and virtual systems must adhere to the following technical requirements:

- All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, Simple Network Management Protocol (SNMP) community strings, etc.) must be changed before a system is installed on the network.
- Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, SNMP, etc.) must be removed or disabled before a system is installed on the network.
- Only one primary function may be implemented per server or virtual machine to prevent functions that require different security levels from coexisting on the same system.
- Only necessary services, protocols, daemons, etc., may be enabled, and only as required for the function of the system. All unnecessary functionality (such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers) must be disabled.
- Additional security features for any required services, protocols or daemons that are considered to be insecure must be documented in Appendix B of this document, justified, and

tested to ensure that they do not introduce unnecessary risk or vulnerabilities.

- All security patches identified as critical, high, or medium must be applied to systems within SLAs established in this policy.

Network Standards

- Use of insecure services and protocols without justification and documentation of additional security features implemented to mitigate risk is prohibited.
- Remote-access technologies for vendors and business partners used to access production systems must be enabled only when needed for business purposes and immediately deactivated after use.