



Secure Development Policy

Policy Owner: Alex Iglesias

Effective Date: July 31st, 2023

Purpose

To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.

Scope

All Finsweet applications and information systems that are business critical and/or process, store, or transmit Confidential data. This policy applies to all internal and external engineers and developers of Finsweet software and infrastructure.

Policy

This policy describes the rules for the acquisition and development of software and systems that shall be applied to developments within the Finsweet organization.

System Change Control Procedures

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. Change control procedures and requirements are described in the Finsweet [Operations Security Policy](#).

Significant code changes must be reviewed and approved by the Finsweet Security Officer (FSO) before being merged into any production branch.

Change control procedures shall ensure that development, testing and deployment of changes shall not be performed by a single individual without approval and oversight.

Patch Management

Patch Identification and Assessment: Finsweet's FSO or designated personnel will be responsible for monitoring security advisories, vendor updates, and other reliable sources of information to

identify relevant patches. Each patch will be assessed based on its criticality, impact, and relevance to Finsweet's environment.

Patch Testing: Before deploying patches to production systems, a testing environment will be used to evaluate the compatibility and stability of the patches. Testing will include verifying that the patches do not introduce conflicts, disruptions, or adverse effects on system functionality.

Patch Deployment: Patches that have been approved through the testing process will be deployed to the appropriate systems within a reasonable timeframe. The deployment process will be planned to minimize disruptions to business operations and may involve phased rollouts or scheduled maintenance windows.

Patch Documentation and Tracking: A centralized patch management system or database will be used to track and document all patch-related activities, including patch identification, assessment, testing, deployment, and verification. The documentation will include details such as patch version, date of installation, responsible personnel, and any associated notes or comments.

Patch Compliance and Verification: Regular audits and assessments will be conducted to ensure compliance with the patch management policy. Verification procedures will be implemented to confirm that patches are applied to all relevant systems and that the systems are up to date. Any instances of non-compliance or unpatched systems will be addressed promptly.

User Responsibilities: Employees and authorized individuals using Finsweet's systems and applications are responsible for promptly applying patches and updates on their devices. Users must comply with patch management procedures, promptly install patches as directed, and report any issues or concerns related to patches to the Finsweet Security Officer or designated personnel.

Software Version Control

All Finsweet software is version controlled and synced between contributors (developers). Access to the central repository is restricted based on an employee's role. All code is written, tested, and saved in a local repository before being synced to the origin repository.

Technical Review of Applications after Operating Platform Changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure that there is no adverse impact on organizational operations or security.

Restrictions on Changes to Software Packages

Modifications to third-party business application packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

Secure System Engineering Principles

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

At a minimum, the following secure-by-design and privacy-by-design principles shall be applied:

Secure-by-design principles:

1. Minimize attack surface area
2. Establish secure defaults
3. The principle of Least privilege
4. The principle of defense in depth
5. Fail securely
6. Don't trust services
7. Separation of duties
8. Avoid security by obscurity
9. Keep security simple
10. Fix security issues correctly

Privacy-by-design principles:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality - Positive-Sum, not Zero-Sum
5. End-to-End Security - Full Lifecycle Protection
6. Visibility and Transparency - Keep it Open
7. Respect for User Privacy - Keep it User-Centric

Engineering documentation and technical references can be found in Notion under Technical.

Software developers are expected to adhere to Finsweet's coding standards throughout the development cycle, including standards for quality, commenting, and security.

Secure Development Environment

Finsweet shall establish and appropriately protect environments for system development and integration efforts that cover the entire system development life cycle. The following environments shall be logically or physically segregated:

- Production
- Test / Staging
- Development

Outsourced Development

Finsweet shall supervise and monitor the activity of outsourced system development. Outsourced development shall adhere to all Finsweet standards and policies.

System Security Testing

Testing of security functionality shall be performed at defined periods during the development life cycle. No code shall be deployed to Finsweet production systems without documented, successful test results and evidence of security remediation activities.

Application Vulnerability Management

Application code should be scanned prior to deployment. Patches to address application vulnerabilities that materially impact security should be deployed within 90 days of discovery.

System Acceptance Testing

Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

Prior to deploying code, a Release Checklist MUST be completed which includes a checklist of all Test Plans which show the completion of all associated tests and remediation of identified issues.

Protection of Test Data

Test data shall be selected carefully, protected and controlled. Confidential customer data shall be protected in accordance with all contracts and commitments. Customer data shall not be used for testing purposes without the explicit permission of the data owner and the FSO.

Acquisition of Third-Party Systems and Software

The acquisition of third-party systems and software shall be done in accordance with the requirements of the Finsweet [Third-Party Management Policy](#).

Developer Training

Software developers shall be provided with secure development training appropriate to their role at least annually. Training content shall be determined by management but shall address the prevention of common web application attacks and vulnerabilities. The following threats and vulnerabilities should be addressed as appropriate:

- prevention of authorization bypass attacks
- prevention of the use of insecure session IDs
- prevention of Injection attacks
- prevention of cross-site scripting attacks
- prevention of cross-site request forgery attacks
- prevention of the use of vulnerable libraries

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. 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	31-Jul-2023	Patch Management added	Alex Iglesias	Joe Krug
1.2	23-May-2024	URL updated in System Change Control Procedures	Alex Iglesias	Joe Krug