



Access Control Policy

Policy Owner: Rohan Ganachari

Effective Date: November 1st, 2023

Purpose

To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.

Scope

All Finsweet information systems that process, store, or transmit confidential data as defined in the Finsweet [Data Management Policy](#). This policy applies to all employees of Finsweet and to all external parties with access to Finsweet networks and system resources, including connections made from remote locations and using personal devices. Given that Finsweet operates as a fully remote company with employees working from their homes and using their own devices, this policy recognizes the unique challenges and considerations associated with remote work environments.

Policy

Access to information computing resources is limited to personnel with a business requirement for such access. Access rights shall be granted or revoked in accordance with this Access Control Policy.

Business Requirements of Access Control

Access Control Policy

Finsweet shall determine the type and level of access granted to individual users based on the "principle of least privilege." This principle states that users are only granted the level of access absolutely required to perform their job functions, and is dictated by Finsweet's business and security requirements. Permissions and access rights not expressly granted shall be, by default, prohibited.

Finsweet's primary method of assigning and maintaining consistent access controls and access rights shall be through the implementation of Role-Based Access Control (RBAC). Wherever feasible,

rights and restrictions shall be allocated to groups. Individual user accounts may be granted additional permissions as needed with approval from the system owner or authorized party.

All privileged access to production infrastructure shall use Multi-Factor Authentication (MFA).

Access to Networks and Network Services

The following security standards shall govern access to Finsweet networks and network services:

- Technical access to Finsweet networks must be formally documented including the standard role or approver, grantor, and date
- Only authorized Finsweet employees and third-parties working off a signed contract or statement of work, with a business need, shall be granted access to the Finsweet production networks and resources
- Remote connections to production systems and networks must be encrypted

User Access Management

Finsweet requires that all personnel have a unique user identifier for system access, and that user credentials and passwords are not shared between multiple personnel. Root, service, and administrator accounts may use a password management system to share passwords for business continuity purposes only. Administrators shall only use shared administrative accounts as needed. If a password is compromised or suspected of compromise the incident should be escalated to the Human Resources Officer (HRO) immediately and the password must be changed.

User Registration and Deregistration

Only authorized administrators shall be permitted to create new user IDs, and may only do so upon receipt of a documented request from authorized parties. User provisioning requests must include approval from data owners or Finsweet management authorized to grant system access. Prior to account creation, administrators should verify that the account does not violate any Finsweet security or system access control policies such as segregation of duties, fraud prevention measures, or access rights restrictions.

User IDs shall be promptly disabled or removed when users leave the organization or contract work ends in accordance with SLAs. User IDs shall not be re-used.

User Access Provisioning

- New employees and/or contractors are not to be granted access to any Finsweet production systems until after they have completed all HR on-boarding tasks, which may include but is not limited to signed employment agreement, intellectual property agreement, and acknowledgement of Finsweet's information security policy
- Access should be restricted to only what is necessary to perform job duties
- No access may be granted earlier than official employee start date
- Access requests and rights modifications shall be documented in an access request ticket or email. No permissions shall be granted without approval from the system or data owner or

- management
- Records of all permission and privilege changes shall be maintained for no less than one year

Management of Privileged Access

The purpose of Privileged Access Management is to establish guidelines and procedures for managing and controlling privileged accounts within Finsweet. Privileged accounts pose a significant security risk and require special attention to ensure that access is granted only to authorized individuals and that their activities are monitored and audited. Granting of administrative rights shall be strictly controlled, and requires approval from the asset owner.

User Access Reviews

Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented.

Access reviews may include group membership as well as evaluations of any specific or exception-based permission. Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.

Removal & Adjustment of Access Rights

The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours.

Access Provisioning, Deprovisioning, and Change Procedure

The Access Management Procedure for Finsweet systems can be found in Appendix A to this policy.

Segregation of Duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Finsweet assets. When provisioning access, care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered when determining access levels for individuals and groups.

User Responsibility for the Management of Secret Authentication Information

Control and management of individual user passwords is the responsibility of all Finsweet personnel and third-party users. Users shall protect secret authentication information in accordance with the [Information Security Policy](#).

Password Policy

Where feasible, passwords for confidential systems shall be configured for at least minimum password requirements:

- Passwords must be a minimum of 8 characters in length, must include a combination of uppercase and lowercase alphabetic characters, numeric characters (0 through 9), and at least one non-alphabetic printable characters (e.g., special symbols)
- Initial passwords must be set to a unique value and changed after first log in
- Passwords must be changed yearly
- Passwords must not be reused
- For manual password resets, a user's identity must be verified prior to changing passwords
- User accounts will be locked out after 10 or fewer login attempts
- Do not limit the permitted characters that can be used
- Do not use secret questions (place of birth, etc) as a sole password reset requirement
- Require email verification of a password change request
- Require the current password in addition to the new password during password change
- It's recommended to use a strong random password generator
- Store passwords in a hashed and salted format using a memory-hard or CPU-hard one-way hash function
- Passwords must not be embedded in code, configuration files, batch files, scripts, or any other mechanism that is discoverable by anyone
- Enforce appropriate account lockout and brute-force protection on account access

System and Application Access

Information Access Restriction

Applications must restrict access to program functions and information to authorized users and support personnel in accordance with the defined access control policy. The level and type of restrictions applied by each application should be based on the individual application requirements, as identified by the data owner. The application-specific access control policy must also conform to Finsweet policies regarding access controls and data management.

Prior to implementation, evaluation criteria are to be applied to application software to determine the necessary access controls and data policies. Assessment criteria include, but are not limited to:

- Sensitivity and classification of data.
- Risk to the organization of unauthorized access or disclosure of data
- The ability to, and granularity of, control(s) on user access rights to the application and data stored within the application
- Restrictions on data outputs, including filtering sensitive information, controlling output, and restricting information access to authorized personnel

- Controls over access rights between the evaluated application and other applications and systems
- Programmatic restrictions on user access to application functions and privileged instructions
- Logging and auditing functionality for system functions and information access
- Data retention and aging features

All unnecessary default accounts must be removed or disabled before making a system available on the network. Specifically, vendor default passwords and credentials must be changed on all Finsweet systems, devices, and infrastructure prior to deployment. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, and Simple Network Management Protocol (SNMP) community strings where feasible.

Secure Log-on Procedures

Secure log-on controls shall be designed and selected in accordance with the sensitivity of data and the risk of unauthorized access based on the totality of the security and access control architecture.

Interactive Session Timeout

To prevent unauthorized access, all interactive sessions will automatically timeout after a period of inactivity. The maximum period of inactivity is 15 minutes. Following a timeout, users are required to re-authenticate to resume the session.

Non-interactive Session Timeout

Non-interactive sessions, such as scripts and batch jobs, will automatically timeout after a maximum period of inactivity of 24 hours. Following a timeout, users are required to re-authenticate to initiate the session.

Use of Privileged Utility Programs

Use of utility programs, system files, or other software that might be capable of overriding system and application controls or altering system configurations must be restricted to the minimum personnel required. Systems are to maintain logs of all use of system utilities or alteration of system configurations. Extraneous system utilities or other privileged programs are to be removed or disabled as part of the system build and configuration process.

Management approval is required prior to the installation or use of any ad hoc or third-party system utilities.

Access to Program Source Code

Access to program source code and associated items, including designs, specifications, verification plans, and validation plans shall be strictly controlled in order to prevent the introduction of

unauthorized functionality into software, avoid unintentional changes, and protect Finsweet intellectual property.

All access to source code shall be based on business need and must be logged for review and audit.

Exceptions

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

Compliance Monitoring and Auditing

Finsweet reserves the right to periodically conduct internal or external audits, assessments, or investigations to assess compliance with this policy. Employees and contractors are required to cooperate fully with such audits and provide accurate and timely information as requested.

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	17-Jul-2023	Submit for approval	Rohan Ganachari	Joe Krug
1.1	27-Oct-2023	Password policy updated	Rohan Ganachari	Joe Krug
1.2	23-May-2024	Appendix B URL updated	Rohan Ganachari	Joe Krug

APPENDIX A - Access Management Procedure

At the completion of the onboarding process, HR will send an email that will give the user access to the required company platforms.

The FSO will provision access for all technical company-wide systems as well as engineering systems for the Technical Developers.

Additional access, beyond standard pre-approved access, must be requested and approved by a manager or system owner.

APPENDIX B - Access Matrix

For more information, refer <https://app.vanta.com/access/access-reviews>

