



Information Security Policy

Policy Owner: Rohan Ganachari

Effective Date: November 1st, 2023

Overview

The Finsweet Information Security Program is an overarching framework that encompasses all the policies, procedures, and guidelines housed in the Finsweet Security Center (FSC). It is designed to safeguard the confidentiality, integrity, and availability of Finsweet's information assets. It is intended to protect Finsweet's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfers, are the property of Finsweet. These systems are to be used for business purposes in serving the best interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Finsweet employee or contractor who deals with information and/or information systems. It is the responsibility of every team member to read and understand this policy, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of Finsweet's information and assets. These rules are in place to protect customers, employees, and Finsweet. Inappropriate use exposes Finsweet to risks including virus attacks, compromise of network systems and services, financial and reputational risk, and legal and compliance issues.

This is not a standalone policy but a collection of policies dedicated to our commitment of comprehensive information security. Additional policies are referenced and/or linked within this document.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Finsweet business or interact with internal networks and business systems, whether owned or leased by Finsweet, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Finsweet and its subsidiaries are responsible for

exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Finsweet policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Finsweet, including all personnel affiliated with third parties. This policy applies to all Finsweet-controlled company and customer data as well as all equipment, systems, networks and software owned or leased by Finsweet.

Security Incident Reporting

All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents shall be reported immediately or as soon as possible by Slack in either the team-all channel or via a group DM to Alex Iglesias, Rohan Ganachari and Joe Krug; or email security@finsweet.com.

In your message, please describe the incident or observation along with any relevant details. For more info, refer to [Incidence Response Plan](#).

Whistleblower Anonymous Fraud Reporting

Finsweet is committed to maintaining the highest standards of ethical conduct and integrity. Our Whistleblower Anonymous Reporting Policy is designed to encourage and enable employees, contractors, and other stakeholders to report any suspicion or evidence of unlawful or unethical behavior without fear of retaliation or retribution. Our Whistleblower Policy is intended to encourage and enable employees and others to raise serious concerns internally so that we can address and correct inappropriate conduct and actions. It is the responsibility of all employees to report concerns about violations of our code of ethics or suspected violations of law or regulations that govern our operations.

Anonymous Reporting: Anyone who has information about potential wrongdoing within the company, including but not limited to fraud, theft, conflict of interest, misconduct, violation of laws, regulations or company policies, is encouraged to report it. Send an email to security@finsweet.com from an email address that is anonymous or fill out our whistleblower form at <https://finsweet.com/security/anonymous-whistleblower-channel>

No Retaliation: It is contrary to our values for anyone to retaliate against any employee or who in good faith reports an ethics violation, or a suspected violation of law, such as a complaint of discrimination, or suspected fraud, or suspected violation of any regulation. An employee who retaliates against someone who has reported a violation in good faith is subject to discipline up to and including termination of employment.

Confidentiality: To the extent permitted by law and as far as it does not hinder any investigations, all reports made under this policy will remain confidential.

Protection of Whistleblowers: The anonymity of whistleblowers will be maintained as far as possible, within the limits allowed by law and the needs of any potential investigation.

Reporting Process: Reports should be submitted through Finsweet's designated whistleblower reporting system, which ensures anonymity and confidentiality.

Investigation: All reports will be taken seriously and investigated promptly and impartially by an assigned impartial investigator.

BYOD Policy

The purpose of this Bring Your Own Device (BYOD) policy is to establish guidelines and procedures for employees of Finsweet who use their personal devices for work-related activities. This policy aims to ensure the security, privacy, and integrity of Finsweet's information assets while allowing employees the flexibility to work remotely using their own devices.

Scope: This BYOD policy applies to all employees, contractors, and third-party individuals who work remotely and use their personal devices, such as smartphones, tablets, laptops, or other computing devices, to access, temporarily store, process, or transmit company information or perform work-related tasks. The policy covers both company-owned resources accessed through personal devices and personal resources accessed while connected to Finsweet's network.

Details

Device Requirements: Employees must ensure that their personal devices meet the minimum security requirements set by Finsweet. These requirements may include but are not limited to latest operating systems, antivirus software, device encryption, and strong passwords or biometric authentication.

Security Measures: Employees must implement necessary security measures to protect their personal devices and access to company's data. It is strongly recommended to enable 2FA, MFA, unique device passcodes, and regularly updating software and applications. Employees must not share their device credentials with others.

Acceptable Use: Personal devices used for work purposes must be used responsibly and in accordance with Finsweet's acceptable use policy. Personal devices should be used primarily for work-related purposes while connected to Finsweet's network or systems. Employees must adhere to Finsweet's acceptable use policy and refrain from engaging in activities that may compromise the security or integrity of company systems or data.

Data Protection: Employees must understand and comply with data protection regulations, confidentiality obligations, and intellectual property rights. Company data should be stored securely on approved cloud storage or Finsweet's network infrastructure. Employees can temporarily store company data on their personal devices to carry out a specific task, and that data must be permanently deleted from their personal devices after completion of the said task. In all other scenarios, employees must not store any company data on their personal devices.

Remote Access: Employees must use secure and authorized methods to access company resources remotely. Public Wi-Fi networks should be avoided unless secured through appropriate encryption and security measures.

Incident Reporting and Support: Employees must report any loss, theft, or unauthorized access to their personal devices used for work-related purposes to the Finsweet Security Officer (FSO)

promptly. Employees should promptly seek assistance from the FSO if they suspect a security incident or breach involving their personal device.

Change in Device or Employment Termination: Employees must provide written proof that all company data and access to Finsweet network have been permanently removed from their current work equipment prior to disposal, sale or handoff of their devices, or in case of employment termination.

Compliance and Monitoring: Finsweet reserves the right to monitor and inspect personal devices used for work purposes to ensure compliance with this policy and applicable laws. Monitoring activities will be carried out in accordance with privacy laws and with appropriate notice to employees.

Mobile Device Policy

The purpose of this Mobile Device Policy is to establish guidelines and procedures for the appropriate use, security, and management of mobile devices used by employees of Finsweet. As a fully remote company without a physical office location, employees rely on their own devices for work-related tasks. This policy aims to protect the confidentiality, integrity, and availability of Finsweet's information assets and ensure the secure use of mobile devices in alignment with the organization's overall security objectives.

All end-user devices (e.g., mobile phones, tablets, laptops, desktops, and other portable computing devices) must comply with this policy. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

System level and user level passwords must comply with the [Access Control Policy](#). Providing access to another individual, either deliberately or through failure to secure a device is prohibited.

All end-user, personal (BYOD) or company owned devices used to access Finsweet information systems (i.e. email) must adhere to the following rules and requirements:

- Devices must be locked with a password (or equivalent control such as biometric) protected screensaver or screen lock after 5 minutes of non-use. Multi-factor authentication (MFA) is strongly encouraged for all mobile device access.
- Devices must be locked whenever left unattended
- Users must report any suspected misuse or theft of a mobile device immediately to the FSO.
- Confidential information must not be stored on mobile devices (this does not apply to business contact information, e.g., names, phone numbers, and email addresses)
- The use of any form of removable media such as USB drives, CDs, DVDs, external hard drives, or any other similar devices, to store, transfer, or process Finsweet data, is strictly forbidden.
- Any mobile device used to access company resources (such as file shares and email) must not be shared with any other person.
- System level and user level passwords must comply with the Access Control Policy. Providing access to another individual, either deliberately or through failure to secure a device is prohibited.
- Upon termination users agree to return all company owned devices and delete all company information and accounts from any personal devices

Mobile Device Management Policy

The purpose of this policy is to establish the expectations and requirements for managing and using personal devices in a secure and compliant manner.

Scope: This Mobile Device Management policy applies to all employees of Finsweet who work remotely using their personal equipment. Since there is no physical office location, adherence to this policy is crucial to maintain the security and compliance of Finsweet's systems and data.

Details

Finsweet does not install data wiping or tracking software on personal mobile devices; however, all employees are required to [install the Vanta Agent](#) application on their current work equipment. Employees are required to notify Finsweet if they change their laptop/pc on which Vanta Agent was previously installed.

The Vanta Agent is a lightweight program designed to run in the background of your computers to monitor specific settings and applications as described in [Vanta's documentation](#) to ensure compliance with SOC2. The Vanta Agent does not track nor record personal activities on the mobile device. Finsweet acknowledges and respects the privacy of employees.

Employees are responsible for maintaining their work equipment in compliance with the security standards outlined in the [Finsweet Security Center](#).

Clear Screen Clear Desk Policy

Employees and contractors should maintain a clean and orderly workspace. Individuals must ensure their workspace (physical or virtual) is clear of all sensitive and confidential information when not in use. Specifically, all confidential information must be hidden to prevent exposure of sensitive information. Digital screens must be locked or logged off to prevent unauthorized access. In shared or public spaces, additional care should be taken to prevent visible exposure of confidential information on screens or desks.

Remote Access Policy

The purpose of this Remote Access Controls Policy is to establish guidelines and procedures for the secure and controlled remote access to Finsweet's network, systems, and resources. This policy aims to ensure that remote access is granted only to authorized individuals, and that appropriate security measures are in place to protect the confidentiality, integrity, and availability of Finsweet's information assets. It applies to all employees, contractors, and any other individuals who require remote access to Finsweet's systems or data.

Laptops and other computer resources that are used to access the Finsweet network must conform to the security requirements outlined in Finsweet's Information Security Policies and adhere to the following standards:

- To ensure mobile devices do not connect a compromised device to the company network, Antivirus policies require the use and enforcement of client-side antivirus software

- Antivirus software must be configured to detect and prevent or quarantine malicious software, perform periodic system scans, and have automatic updates enabled
- Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer
- Users are prohibited from changing or disabling any organizational security controls such as personal firewalls, antivirus software on systems used to access Finsweet resources
- Use of remote access software and/or services (e.g., VPN client) is allowable as long as it is provided by the company and configured for multifactor authentication (MFA)
- Unauthorized remote access technologies may not be used or installed on any Finsweet system
- Users shall use a VPN when transmitting confidential information on public Wi-Fi
- If you access from a public computer (e.g., from a business center, hotel, etc.), log out of the session and don't save anything. Don't check "remember me", collect all printed materials and do not download files to a non-Finsweet controlled system

Acceptable Use Policy

This Acceptable Use Policy outlines the acceptable and appropriate use of all technology resources, services, and systems connected to Finsweet operations, including but not limited to, computer systems, email services, networks, software, and hardware. This policy is designed to safeguard Finsweet, its employees, and its customers from harm caused by misuse and to set clear expectations of behavior.

Finsweet proprietary and customer information stored on electronic and computing devices, whether owned or leased by Finsweet, the employee or a third party, remains the sole property of Finsweet for the purposes of this policy. Employees and contractors must ensure through legal or technical means that proprietary information is protected in accordance with the [Data Management Policy](#).

User Responsibilities: Users are responsible for all activities conducted under their accounts. Users must keep their login credentials confidential and must log out from their accounts when they are not actively using them. All sensitive data should be securely stored and transmitted.

Compliance with Laws and Regulations: Users must comply with all applicable local, national, and international laws and regulations. This includes laws related to privacy, data protection, intellectual property, cybercrime, and export control.

Authorized Software Usage: All software applications used within Finsweet must be authorized and approved by the Finsweet Security Officer (FSO) or the designated authority. Employees must [submit a formal request for software approval](#), providing details about the software's purpose, functionality, and potential security implications. The FSO or designated authority will evaluate the request based on compatibility, licensing requirements, security considerations, and potential impact on Finsweet's systems. A list of approved software applications will be maintained by the FSO or designated authority. Only software from this approved list is permitted to be installed and used on devices used for work purposes. The list will be periodically reviewed and updated to ensure its accuracy and relevance.

Resource Usage: Finsweet's resources must be used responsibly and primarily for business-related purposes. Incidental personal use is permitted if it does not interfere with work responsibilities, consume a significant amount of resources, or violate any other policies or laws.

Storage and Backups: The use of Finsweet-approved software file storage is required all individuals accessing Finsweet systems. Storing important documents on the cloud-based software is how you

"backup" your mobile device, such as a laptop.

Remote Work Considerations: Users are responsible for securing their home networks and ensuring the use of secure Wi-Fi connections and up-to-date router firmware. The use of public or unsecured networks should be avoided when accessing Finsweet's resources. Users must ensure that their personal devices used for work purposes are properly protected with up-to-date security software, including antivirus and anti-malware protection. When accessing Finsweet's resources remotely, users must use secure and authorized remote access methods, such as VPN (Virtual Private Network) connections, and comply with the company's Remote Access Controls policy. Users should also follow Finsweet's Mobile Device Policy when using personal devices for work-related tasks.

Theft, Loss, or Unauthorized Use: You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Finsweet proprietary information or equipment.

Reporting Mechanism: Any suspected violation of this policy should be reported immediately to the Finsweet Security Officer (FSO) or the appropriate authority within Finsweet

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities with properly documented approval from both the FSO and CEO. Under no circumstances is an employee of Finsweet authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Finsweet-owned resources or while representing Finsweet in any capacity. The list below is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Finsweet
2. Users must not create, store, share, or transmit any content that is illegal, offensive, abusive, defamatory, obscene, or otherwise inappropriate. This includes content that promotes violence, discrimination, or harassment against individuals or groups based on attributes such as race, religion, gender, age, nationality, or sexual orientation.
3. Using Unauthorized Software, as defined by any software application that has not been approved by the FSO to use within Finsweet. This includes commercial software, freeware, shareware, open-source software, or any other software not explicitly authorized. Prohibition Employees are strictly prohibited from installing, accessing, or using unauthorized software on devices used for work purposes within Finsweet. This prohibition extends to all personal devices utilized for work, as well as any company-owned devices, if applicable.
4. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Finsweet or the end user does not have an active license
5. Accessing data, a server, or an account for any purpose other than conducting Finsweet business, even if you have authorized access, is prohibited
6. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management shall be

- consulted prior to export of any material that is in question
7. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, email bombs, etc.)
 8. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home
 9. Using a Finsweet computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws
 10. Making fraudulent offers of products, items, or services originating from any Finsweet account
 11. Making statements about warranty, expressly or implied, unless it is a part of normal job duties
 12. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
 13. Port scanning or security scanning is expressly prohibited unless prior notification to the Finsweet engineering team is made
 14. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty
 15. Circumventing user authentication or security of any host, network, or account
 16. Introducing honeypots, honeynets, or similar technology on the Finsweet network.
 17. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack)
 18. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means
 19. Providing information about, or lists of: Finsweet employees, contractors, partners, or customers to parties outside Finsweet without authorization

Email and Communication Activities

This policy outlines acceptable practices for using company resources for electronic communication, which includes the use of email, instant messaging, social media, and any other digital communication methods. This policy aims to ensure our communications are secure, responsible, and reflective of our company's values and reputation.

Guidelines to Follow

1. **Company Representation:** All communications sent using company resources must maintain a professional tone and respect the company's image and reputation.
2. **Confidential Information:** Confidential or sensitive company information should never be shared or discussed in any unsecured digital communication.
3. **Security:** Employees must comply with all of Finsweet's security protocols when communicating electronically, including encryption and password protections.
4. **External Communication:** Any communication with media, press, or other external parties must be authorized by the designated company spokesperson.

Prohibited Activities

All users of company systems are prohibited from engaging in the following activities:

1. **Spam:** Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
2. **Harassment:** Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of messages. Harassment is defined as any behavior that is disrespectful, disruptive, or offensive to others.
3. **Forging:** Unauthorized use or forging of email header information. This includes any attempt to mislead the recipient about the sender or source of the message.
4. **Solicitation:** Solicitation of email for any other email address, other than that of the sender's account, with the intent to harass or to collect replies.
5. **Chain Letters and Pyramid Schemes:** Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.
6. **Unsolicited Advertising:** Use of unsolicited email originating from within Finsweet's networks or other service providers on behalf of, or to advertise, any service hosted by Finsweet or connected via Finsweet's network.

Additional Policies and Procedures Incorporated by Reference

Personnel are responsible for reading and complying with all policies relevant to their roles and responsibilities.

Role	Purpose
Access Control Policy	To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.
Asset Management Policy	To identify organizational assets and define appropriate protection responsibilities.
Business Continuity & Disaster Recovery Plan	To prepare Finsweet in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.
Cryptography Policy	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Data Management Policy	To ensure that information is classified and protected in accordance with its importance to the organization.
Human Resources Policy	To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.
Incident Response Plan	Policy and procedures for suspected or confirmed information security incidents.
Operations Security Policy	To ensure the correct and secure operation of information processing systems and facilities.
Physical Security Policy	To prevent unauthorized physical access or damage to the organization's information and information processing facilities.
Risk Management Policy	To define the process for assessing and managing Finsweet's information security risks in order to achieve the company's business and information security objectives.
Secure Development Policy	To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.

Third-Party Management Policy	To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.
-------------------------------	--

Policy Review and Updates

This policy will be reviewed at least annually or as needed to ensure its continued effectiveness, relevance, and alignment with the evolving remote work environment, technological advances, and regulatory requirements. Changes to the policy will be communicated to all stakeholders in a timely manner.

Policy Compliance

Finsweet will measure and verify compliance to this policy through various methods, including but not limited to ongoing monitoring, and both internal and external audits.

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 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	27-Jul-2023	Submit for approval	Rohan Ganachari	Joe Krug
1.1	30-Oct-2023	MDM policy is added	Rohan Ganachari	Joe Krug
1.2	23-May-2024	Updated some text & URLs. Refer Notion for more info.	Rohan Ganachari	Joe Krug