Information Security Policy

Version 2 - Approved by Tahmid Awal

Contents

1. Objective
2. Scope
3. Policy Statement
4. Information Security Requirements
5. Information Security Objectives
6. Segregation of Duties
7. Contact with Special Interest Groups
8. Contact with Authorities
9. Information Security in Project Management
10. Reporting of Security Incidents
11. Maintenance of Policy
12. Supporting Policies
13. Document Security Classification
14. Non-Compliance
15. Responsibilities
16. Schedule
17. Version History

1. Objective

While providing PlanSyncAI’s service to clients, PlanSyncAI’s staff members and vendors acquire access to the client's privileged and sensitive information. Each of PlanSyncAI's clients places an enormous amount of trust that their data is created, stored, shared, and transmitted securely.

The loss of any client data or services due to unauthorized access, intrusion, theft, natural or cyber disasters, or cyber-attacks diminishes the client's trust as well as significantly damages PlanSyncAI’s reputation as an advocate for companies to develop, implement and maintain systems to prevent the loss of intellectual property and other confidential information.

The purpose of this policy document is to define the direction, principles, and basic rules for information security management within PlanSyncAI. This document describes the management's vision and commitment to effectively protect "confidentiality," maintain "integrity," and ensure the "availability" of its information assets and to respond and recover from information security incidents when they arise.

Information security is deemed to safeguard three main objectives:

- Confidentiality – Data and information assets must be confined to people authorized to access them and not be disclosed to others.
- Integrity – Keeping the data intact, complete, and accurate, and information systems operational.
- Availability – An objective indicating that information or system is at the disposal of authorized users when needed.

2. Scope

This policy is applicable to the following:

- All staff members working for PlanSyncAI who have access to the organization's and client’s information.
- All staff members, vendors, and third-party employees who have access to PlanSyncAI’s information processing systems and the data contained in them. This includes the data accessed by licensed third parties, which is, in turn, deployed to and used by their clients.
- All stakeholders and interested parties who are relevant to the operations of PlanSyncAI.
- All digital and non-digital assets that play a role in the creation, storage, transmission, and disposal of information come under the purview of this policy.

3. Policy Statement

- PlanSyncAI shall establish, implement, and maintain a holistic and robust Information Security Management System (ISMS). ISMS is defined as the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organizational

structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

- The ISMS shall have adequate and appropriate arrangements which shall enable it to effectively protect "confidentiality," maintain "integrity" and ensure "availability" of its information assets and to respond and recover from information security incidents when they arise.
- While planning the ISMS, PlanSyncAI shall consider its internal and external issues along with the requirements of the interested parties and determine risks and opportunities that could affect the activities supporting the provision of its products and services. The top management shall provide the required resources and sufficiently contribute towards the ISMS, ensuring it achieves its intended outcome(s).

4. Information Security Requirements

- Information and supporting technology - including hardware and software systems, are critical business assets. Confidentiality, integrity, and availability of information are essential to maintaining a better competitive edge, profitability, legal compliance, and reputation.
- Organizations and their information systems and networks increasingly face security threats from a wide range of sources, including external hacking and intrusions, computer-assisted fraud, espionage, sabotage, vandalism, or damage from natural disasters. Due to the dependence on information systems and services, organizations are now more vulnerable to security threats.
- Designing security controls and implementing them requires careful planning and attention. Management policies and administrative controls are needed to supplement technical controls that are implemented to protect data. Information Security Management needs, at a minimum, participation from all employees in the organization. It may also require involvement from suppliers, vendors, service providers, customers, and external specialists.

5. Information Security Objectives

The objectives of the Information Security Policy are:

- To create a coherent system for the management of information security that is aligned with PlanSyncAI’s business strategy.
- To protect and safeguard the information that is important to PlanSyncAI and its clients.
- To reduce risk related to the use of technology and technology outsourcing.
- To ensure that all PlanSyncAI's information assets are accounted for and adequately protected from damage, alteration, loss, and unauthorized use or access.
- To ensure that information and information systems are available only to authorized users.
- To ensure that PlanSyncAI provides its customers with the means to enable them to fulfill their obligation to facilitate the exercise of Personally Identifiable Information (PII) principals’ right to access, correct, or erase PII pertaining to them, defined by the contract.
- To ensure that PII processed under a contract shall not be processed for any purpose independent of the instructions of PlanSyncAI’s customer.
- To be compliant with all information security-related regulatory and statutory requirements pertaining to information collection, storage, processing, transmission, and disclosure.

- To set aside resources to establish, implement, operate, monitor, review, and maintain information security safeguards.
- To create awareness of information security and to ensure that all employees understand their responsibilities for maintaining information security.
- To create detailed information security best practices and guideline documents and ensure compliance with such documents.
- To assess and update the information security policy objectives periodically as per the business need and ensure continuous improvement.

6. Segregation of Duties

- Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.
- While assigning responsibilities, conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
- Care shall be taken that every individual may access, modify, or use assets with proper authorization or detection. The possibility of collusion should be considered while designing the controls.

7. Contact with Special Interest Groups

Based on requirements and proper vendor validation, specialist advice shall be sought whenever required. This could be by having a Security Consultant on a contractual or per-call payable basis. The same could also be sought from non-profit agencies.

8. Contact with Authorities

Where required, the organization shall maintain appropriate contact with law enforcement authorities, regulatory bodies, fire departments, emergency services, telecommunication providers, and others. These contacts shall ensure help can be availed of and is accessible during a crisis.

9. Information Security in Project Management

Information security should be integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character. Examples: a project for a core business process, IT, facility management, and other supporting processes.

10. Reporting of Security Incidents

The person witnessing an information security incident should report the incident in the Sprinto Application.

11. Maintenance of Policy

- Compliance with this policy and supporting policies shall be audited yearly. Exceptions identified during the audit shall be immediately and appropriately addressed.
- The security policy shall be reviewed annually, except in the event of a major change in the organization or the environment affecting the organization, in which case it shall be reviewed on a need basis.
- The security policy shall be reviewed and revised whenever a major security risk or incident is identified.

12. Supporting Policies

The following policy documents shall support the information systems security policy at a minimum:

12.1 Human Resources Security Policy

The purpose of this policy is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

12.2 Risk Assessment & Management Procedure

The purpose of this procedure is to ensure that guidelines related to understanding and managing risks that may affect information security are provided.

12.3 Access Control Policy

The purpose of this policy is:

- To limit access to information and information processing facilities.
- To ensure authorized user access and to prevent unauthorized access to systems and services.
- To make users accountable for safeguarding their authentication information.
- To prevent unauthorized access to systems and applications.
- Segregation of duties.

12.4 Asset Management Policy

The purpose of this policy is:

- To identify PlanSyncAI’s assets and define appropriate protection responsibilities.
- To ensure that information receives an appropriate level of protection in accordance with its importance to PlanSyncAI.
- To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

12.5 Operations Security Policy

The purpose of this policy is to ensure the protection of information through daily operations that take place in providing PlanSyncAI’s services.

12.6 Acceptable Usage Policy

- To ensure that all employees at PlanSyncAI are aware of the acceptable use of assets and formal cybersecurity guidelines to ensure best security practices.
- To ensure that PlanSyncAI's information is protected when accessed, processed, or stored at teleworking sites.

12.7 Compliance Policy

The purpose of this document is to ensure PlanSyncAI complies with all legal and regulatory requirements to ensure the proper functioning of all business domains.

12.8 System Acquisition and Development Policy

The purpose of this policy is to ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems that provide services over public networks.

12.9 Physical and Environmental Policy

This policy helps to prevent unauthorized physical access, damage, and interference to PlanSyncAI's information and information processing facilities.

12.10 Business Continuity Management Policy

The purpose of this policy is to ensure that business continuity is embedded in PlanSyncAI's scope of operations.

12.11 Vendor Management Policy

The purpose of this policy is to ensure the protection of PlanSyncAI's assets that are provided by third-party suppliers.

12.12 Incident Management Policy

This policy helps the management of any information security incidents that may compromise confidentiality, integrity, or availability of data and services by PlanSyncAI.

13. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details)

14. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

15. Responsibilities

- The Information security officer has the ultimate authority over the Information Security Policy and approves and authorizes all changes to the Information Security Policy.
- The Information security officer has executive authority over information security and works with Executive Management to approve, authorize, and issue all documentation.
- The Information security officer is responsible for the development and maintenance of all ISMS documentation.
- The Information security officer shall schedule periodic internal audits with the help of either the internal team or external consultants.
- The Information security officer, along with the Head of Engineering, is responsible for building a strategic and comprehensive privacy program that defines, develops, maintains, and implements policies and processes that enable consistent, effective privacy practices that minimize the risk and ensure the confidentiality of Personally Identifiable Information (PII), paper or electronic, across all media types.

16. Schedule

This document is to be reviewed annually and whenever significant changes occur in the organization.

End of Information Security Policy. For version history, please see the next page.

Version History

Version		Log	Date
2	Current	Policy version reviewed by Cameron Abernethy	04 Aug, 2026
2		Policy version reviewed by Cameron Abernethy	02 Jul, 2025
2		Policy version approved by Tahmid Awal	01 Jul, 2025
2		New policy version created	30 Jun, 2025
1		Policy version approved by Tahmid Awal	23 Jun, 2025
1		New policy version created	23 Jun, 2025