Vendor Management Policy

Version 2 - Approved by Tahmid Awal

Contents

1. Objective
2. Scope
3. Policy Statement
4. Vendor Management
5. Document Security Classification
6. Non-Compliance
7. Responsibilities
8. Schedule
9. Version History

1. Objective

PlanSyncAI depends on third-party vendors for a range of services. Some of these services are critical for PlanSyncAI to meet its security commitments and provide uninterrupted services to its customers. This policy provides the guidelines for managing vendor relationships that affect the services we provide with an aim to minimize the risk associated with using third parties.

2. Scope

This policy applies specifically to vendors whose services are critical to the operational integrity and availability of PlanSyncAI's services to its customers or with whom critical data is shared.

3. Policy Statement

PlanSyncAI is committed to exercising caution when sharing critical data with third-party vendors. It is essential to recognize that each instance of data shared with a vendor expands the potential attack surface of that data. Given our reliance on multiple third-party services, there is a need to share specific data. This policy establishes a deliberate process for evaluating critical third-party vendors, ensuring we maintain the highest data security and risk assessment standards.

4. Vendor Management

4.1 Information Security in Vendor Relationships

- Information security requirements for mitigating the risks associated with the vendor’s access to PlanSyncAI’s assets shall be agreed upon with the supplier and documented in the form of agreements or contracts.
- Resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party shall be defined within these agreements or contracts.
- For third-party personnel who have access to PlanSyncAI’s assets, it is essential that they acknowledge the latest version of PlanSyncAI’s information security policies.
- Security controls and service levels specified in the contracts or agreements shall be implemented, operated, and maintained by the vendor.
- Contracts/Agreements shall include information security requirements to ensure compliance with PlanSyncAI’s security policies and procedures.
- Non-Disclosure / Confidentiality agreements to protect PlanSyncAI’s information assets shall be signed by vendors, third parties, contractors, and subcontractors of the vendors, as applicable.

4.2 Vendor Risk Assessments and Service Delivery Reviews

- A list of all vendors critical to PlanSyncAI’s services and vendors with whom critical data is shared – needs to be maintained.

- For each vendor in the list, a vendor assessment shall be performed, and their risk/criticality to PlanSyncAI's services and sensitivity of data shared.
- Where required, PlanSyncAI may also perform reviews of vendor's services through periodic review calls or audits of vendors. Please note that this may only be required in extreme cases.

4.3 Review Vendors and Managing Changes to Vendor Services

- Periodic reviews of the list of vendors and their risk assessment shall be performed at least annually.
- It is the responsibility of the managers of business functions always to keep the Information Security officer informed of any changes in vendors or the level of service that a particular vendor is providing.
- All such changes shall be accompanied by a review or update of the list of vendors as applicable and a re-assessment of risks.

5. Document Security Classification

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

6. 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.

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

8. Schedule

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

End of Vendor Management 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