Vendor Management Policy

IronHub Inc

August 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.2

Table 2: Document history

Date	Comment
Jun 1 2022	Initial document

1 Purpose and Scope

a. This policy defines the rules for relationships with the organization's Information Technology (IT) vendors and partners.

b. This policy applies to all IT vendors and partners who have the ability to impact the confidentiality, integrity, and availability of the organization's technology and sensitive information, or who are within the scope of the organization's information security program.

c. This policy applies to all employees and contractors that are responsible for the management and oversight of IT vendors and partners of the organization.

2 Background

a. The overall security of the organization is highly dependent on the security of its contractual relationships with its IT suppliers and partners. This policy defines requirements for effective management and oversight of such suppliers and partners from an information security perspective. The policy prescribes minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management.

3 References

a. Information Security Policy

b. Security Incident Response Policy

4 Policy

a. IT vendors are prohibited from accessing the organization's information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.

b. All IT vendors must comply with the security policies defined and derived from the Information Security Policy (reference (a)).

c. All security incidents by IT vendors or partners must be documented in accordance with the organization's Security Incident Response Policy (reference (b)) and immediately forwarded to the Information Security Manager (ISM).

d. The organization must adhere to the terms of all Service Level Agreements (SLAs) entered into with IT vendors. As terms are updated, and as new

ones are entered into, the organization must implement any changes or controls needed to ensure it remains in compliance.

e. **Vendor Risk Tiering:** All IT vendors must be classified into one of the following risk tiers based on their access to organizational systems and data:

   i. **Tier 1 – Critical Vendors**: Vendors with direct access to production systems, sensitive data, or personal information. These vendors present the highest risk and require the most rigorous due diligence.

   ii. **Tier 2 – Significant Vendors**: Vendors with indirect or limited access to organizational systems, or whose service failures would have moderate business impact.

   iii. **Tier 3 – Standard Vendors**: Vendors with no access to organizational systems or sensitive data.

f. **Vendor Due Diligence Requirements by Tier:**

   i. **Tier 1 Vendors** must, before access is granted and annually thereafter:

      1. Provide a current SOC 2 Type II report or equivalent third-party security certification (ISO 27001, PCI DSS, etc.). The report must be reviewed by the ISM or delegate.
      2. Complete a vendor security questionnaire.
      3. Undergo a supply chain risk assessment identifying sub-processors and sub-suppliers.
      4. Sign a Data Processing Agreement (DPA) if processing personal data.

   ii. **Tier 2 Vendors** must complete a vendor security questionnaire before access is granted and annually thereafter.

   iii. **Tier 3 Vendors** require basic contractual security clauses only.

g. Before entering into a contract and gaining access to organizational information systems, all IT vendors must undergo a risk assessment proportional to their tier classification.

   i. Security risks related to IT vendors and partners must be identified during the risk assessment process.

   ii. The risk assessment must identify risks related to information and communication technology, as well as risks related to IT vendor supply chains, including sub-suppliers.

h. **Annual Vendor Review:** All Tier 1 vendors must be reviewed annually. The ISM is responsible for maintaining a vendor register and scheduling reviews. Reviews must confirm continued compliance with security requirements and assess any changes in risk.

i. IT vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely. The organization strictly adheres to all applicable legal, regulatory, and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally-Identifiable Information (PII).

j. The organization may audit IT vendors and partners at any time to ensure compliance with applicable security policies, as well as legal, regulatory, and contractual obligations.