

Privacy Management Policy

IronHub Inc

August 2026

Contents

1 Purpose and Scope	3
2 Background	3
3 Definitions	3
4 Policy	3
4.1 Privacy Notice and Transparency (P1.1)	3
4.2 Consent and Choice (P2.1)	4
4.3 Collection of Personal Information (P3.1, P3.2)	4
4.4 Use, Retention, and Disposal (P4.1, P4.2, P4.3)	5
4.5 Data Subject Access and Amendment (P5.1, P5.2)	5
4.6 Disclosure to Third Parties (P6.1–P6.7)	5
4.7 Accuracy (P7.1)	6
4.8 Dispute Resolution and Complaints (P8.1)	6
5 Roles and Responsibilities	7
6 Enforcement	7

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	P1.1, P2.1, P3.1, P3.2, P4.1, P4.2, P4.3, P5.1, P5.2, P6.1, P6.2, P6.3, P6.4, P6.5, P6.6, P6.7, P7.1, P8.1

Table 2: Document history

Date	Comment
Jun 1 2022	Initial document

Date	Comment
Apr 21 2026	Completed policy in full to satisfy SOC 2 Privacy TSC

1 Purpose and Scope

- a. The purpose of this policy is to establish IronHub's commitment to protecting the privacy of personal information collected, processed, stored, and disclosed in the course of its operations.
- b. This policy applies to all personal information handled by IronHub, including information about customers, employees, contractors, and other individuals, regardless of the format in which it is held.
- c. This policy applies to all employees, contractors, vendors, and third parties who collect, access, process, or transmit personal information on behalf of IronHub.

2 Background

- a. IronHub collects and processes personal information as part of delivering its products and services. This policy establishes the principles and controls that govern how IronHub manages personal information in alignment with applicable privacy laws and regulations, including but not limited to PIPEDA (Canada), GDPR (where applicable), and other regional privacy frameworks.

3 Definitions

- a. **Personal Information:** Any information about an identifiable individual, including name, email address, phone number, financial data, location data, online identifiers, and any other data that can identify a natural person directly or indirectly.
- b. **Data Subject:** An individual whose personal information is collected or processed by IronHub.
- c. **Processing:** Any operation performed on personal information, including collection, storage, use, disclosure, transfer, and deletion.
- d. **Data Controller:** IronHub, as the entity that determines the purposes and means of processing personal information.

4 Policy

4.1 Privacy Notice and Transparency (P1.1)

- a. IronHub must provide clear and accessible privacy notices to data subjects at or before the point of collection. Privacy notices must describe:
 - i. The categories of personal information collected.

- ii. The purposes for which personal information is collected and used.
 - iii. The legal basis for processing (where applicable).
 - iv. How long personal information is retained.
 - v. Whether personal information is shared with third parties, and for what purposes.
 - vi. Data subjects' rights regarding their personal information.
 - vii. Contact information for privacy inquiries or complaints.
- b. Privacy notices must be reviewed and updated whenever there is a material change to IronHub's data practices. Data subjects must be notified of material changes in a timely manner.

4.2 Consent and Choice (P2.1)

- a. Where consent is the legal basis for processing, IronHub must obtain explicit, informed, and freely given consent from data subjects prior to collecting or processing their personal information.
- b. Data subjects must be informed of the consequences of withholding consent. Consent must not be a condition of service where processing is not strictly necessary.
- c. Data subjects must be provided with meaningful choices regarding the collection, use, retention, disclosure, and disposal of their personal information.
- d. Consent must be documented and retained as evidence. Data subjects may withdraw consent at any time; withdrawal must be honoured promptly and without detriment.

4.3 Collection of Personal Information (P3.1, P3.2)

- a. IronHub must collect only the minimum personal information necessary to fulfill the stated purpose (data minimization principle).
- b. Personal information must be collected through lawful and fair means.
- c. For categories of personal information requiring explicit consent (e.g., sensitive personal data such as health information, biometric data, or financial account details), IronHub must:
 - i. Clearly communicate to the data subject why such information is needed.
 - ii. Inform the data subject of the consequences of not providing consent.
 - iii. Obtain explicit consent before collection.

4.4 Use, Retention, and Disposal (P4.1, P4.2, P4.3)

- a. Personal information must only be used for the purposes for which it was collected, as described in the applicable privacy notice, or as otherwise permitted by law.
- b. Personal information must not be used for secondary purposes without obtaining fresh consent or establishing another lawful basis for processing.
- c. Personal information must be retained only for as long as necessary to fulfill the purposes for which it was collected, or as required by law. Retention periods are defined in IronHub's Data Retention Policy.
- d. Upon expiry of the retention period, personal information must be securely disposed of using methods that prevent reconstruction or recovery, in accordance with IronHub's Data Classification Policy and Data Retention Policy.

4.5 Data Subject Access and Amendment (P5.1, P5.2)

- a. Data subjects have the right to request access to their personal information held by IronHub. Upon verified request, IronHub must:
 - i. Confirm whether personal information is held.
 - ii. Provide a copy of the personal information in a readable format within the timeframe required by applicable law (generally 30 days).
 - iii. If access is denied (e.g., where it would affect the rights of others), inform the data subject of the denial and the reason.
- b. Data subjects have the right to request correction or amendment of inaccurate or incomplete personal information. IronHub must:
 - i. Correct or append the record promptly upon verified request.
 - ii. Notify any third parties to whom the information was disclosed of the correction, where required.
 - iii. If a correction request is denied, inform the data subject and provide the reason.

4.6 Disclosure to Third Parties (P6.1–P6.7)

- a. Personal information must not be disclosed to third parties without the explicit consent of the data subject, unless disclosure is:
 - i. Required by law or court order.
 - ii. Necessary for the delivery of services via an authorized sub-processor.
 - iii. Otherwise permitted under applicable privacy law.

- b. IronHub must maintain a record of all authorized disclosures of personal information, including the recipient, purpose, date, and legal basis.
- c. IronHub must maintain a record of any detected or reported unauthorized disclosures (including data breaches), in accordance with the Security Incident Response Policy.
- d. All third parties and vendors who access personal information must provide contractual privacy and security commitments (e.g., via a Data Processing Agreement). Vendor compliance with these commitments must be assessed at least annually for Tier 1 vendors.
- e. IronHub must obtain commitments from vendors that they will notify IronHub immediately upon discovery of actual or suspected unauthorized disclosure of personal information. Such notifications must be handled in accordance with the Security Incident Response Policy.
- f. In the event of a personal data breach, IronHub must notify affected data subjects, applicable regulatory authorities, and other required parties in accordance with the Security Incident Response Policy and applicable law.
- g. Data subjects may request an accounting of disclosures of their personal information. IronHub must provide such an accounting within the timeframe required by applicable law.

4.7 Accuracy (P7.1)

- a. IronHub must take reasonable steps to ensure that personal information is accurate, complete, up-to-date, and relevant for the purposes for which it is used.
- b. Employees who become aware of inaccurate personal information must report it to the relevant data owner for correction.

4.8 Dispute Resolution and Complaints (P8.1)

- a. IronHub must maintain a process for receiving, addressing, and resolving privacy inquiries, complaints, and disputes from data subjects.
- b. A designated Privacy Contact (the ISM or appointed delegate) must be responsible for receiving and responding to privacy complaints.
- c. Complaints must be acknowledged within 5 business days and resolved within 30 calendar days, or as required by applicable law. Data subjects must be informed of the outcome.
- d. If a complaint cannot be resolved internally, data subjects must be informed of their right to escalate to the applicable regulatory authority.
- e. IronHub must monitor compliance with this policy and take corrective action where deficiencies are identified.

5 Roles and Responsibilities

- a. The **Information Security Manager (ISM)** serves as the Privacy Contact and is responsible for overseeing compliance with this policy, responding to data subject requests and complaints, and coordinating breach notification.
- b. All **employees and contractors** are responsible for handling personal information in accordance with this policy and for reporting any suspected privacy incidents or breaches immediately to the ISM.
- c. **Managers** are responsible for ensuring their teams understand and follow this policy.

6 Enforcement

- a. Violations of this policy may result in disciplinary action up to and including termination of employment or contract. Violations that constitute a breach of applicable law may be referred to the appropriate regulatory authority.