Information Security Policy

IronHub Inc

August 2026

Contents

9 Compliance & Enforcement 7

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.9

Table 2: Document history

Date	Comment
Jun 1 2022	Initial document
Oct 31 2024	Updated roles and responsibilities

1 Purpose and Scope

1.1 Purpose

The purpose of this Information Security Policy is to ensure the confidentiality, integrity, and availability of IronHub's information assets. This policy establishes a framework for managing information security risks and maintaining compliance with relevant security standards.

1.2 Scope

This policy applies to:

- All IronHub employees, contractors, and third-party service providers.
- All information systems, networks, applications, databases, and assets used to process, store, or transmit IronHub's information.
- Any information entrusted to IronHub by customers, partners, and stakeholders.

2 Information Security Management

2.1 Governance & Compliance

- IronHub shall establish an **Information Security Management System (ISMS)** to protect its assets and data.
- IronHub's **Chief Information Security Officer (CISO)** is responsible for enforcing this policy.
- Compliance with **legal, regulatory, and contractual** obligations will be monitored regularly.

2.2 Risk Management

- IronHub shall conduct **annual risk assessments** to identify threats, vulnerabilities, and their impact.
- A **risk register** shall be maintained to track identified risks and treatment plans.
- Security controls will be designed based on the **principle of least privilege (PoLP)** and **zero trust architecture**.

3 References

a. Encryption Policy

b. Data Center Security Policy
c. Disaster Recovery Policy
d. Password Policy
e. Remote Access Policy
f. Removable Media/Cloud Storage/BYOD Policy
g. Risk Assessment and Management Policy
h. Security Incident Response Policy
i. Software Development Lifecycle Policy
j. System Availability Policy
k. Workstation Security Policy

4 Roles & Responsibilities

4.1 Chief Information Security Officer (CISO)

- Oversees the development and enforcement of security policies.
- Ensures compliance with regulatory and contractual obligations.
- Leads risk management and security incident response.
- Provides regular security reports to executive leadership.

4.2 IT Security Team

- Implements and maintains security controls and technologies.
- Monitors networks, systems, and logs for security incidents.
- Conducts vulnerability assessments and penetration testing.
- Manages access control mechanisms and enforces security policies.

4.3 Department Managers

- Ensure team compliance with security policies and procedures.
- Identify and mitigate security risks within their respective areas.
- Report security incidents and enforce access control measures.

4.4 Employees & Contractors

- Follow company security policies and guidelines.
- Complete required security awareness training.
- Report any suspicious activity or security incidents promptly.
- Secure company assets and protect sensitive information.

4.5 Third-Party Vendors

- Adhere to security requirements defined in contracts.
- Implement appropriate security measures to protect IronHub's data.
- Report security breaches or incidents affecting IronHub's systems.

5 Security Controls

5.1 Access Control

- Employees and third parties must be **authenticated and authorized** before accessing company assets.
- **Multi-factor authentication (MFA)** is required for all critical systems.
- **Periodic access reviews** shall be conducted to ensure proper user permissions.

5.2 Data Protection & Encryption

- **Encryption** must be applied to data **at rest** and **in transit** using industry-standard cryptographic algorithms.
- **Confidential data classification** shall be enforced with appropriate handling procedures.

5.3 Network & Infrastructure Security

- IronHub will implement **firewalls, intrusion detection systems (IDS), and endpoint detection response (EDR)** solutions.
- Secure **network segmentation** will be enforced to limit access to critical environments.
- **Logging and monitoring** of system activity shall be maintained for security analysis.

5.4 Endpoint & Mobile Device Security

- All company-owned and BYOD devices must have **endpoint security software**.
- Devices must adhere to **Mobile Device Management (MDM)** policies.

5.5 Vendor & Third-Party Security

- IronHub shall conduct **due diligence and security assessments** for vendors handling sensitive data.
- All third parties must sign **non-disclosure agreements (NDAs)** before accessing IronHub's systems.

6 Security Awareness & Human Resources

6.1 Employee Training

- **Annual security awareness training** will be mandatory for all employees.
- Employees must undergo **security policy acknowledgment** during onboarding.

6.2 Secure Offboarding

- Access to systems shall be revoked immediately upon termination or role change.
- IronHub IT must retrieve company-issued devices and ensure secure data disposal.

7 Incident Management

7.1 Security Incident Response

- IronHub shall maintain an **Incident Response Plan (IRP)** for detecting, responding, and recovering from security incidents.
- Security events must be **reported within 24 hours** to the IT Security team.
- In the event of a **data breach**, affected customers must be notified per **legal and contractual requirements**.

8 Business Continuity & Disaster Recovery

- IronHub shall maintain a **Business Continuity Plan (BCP)** and **Disaster Recovery Plan (DRP)** to ensure operations can continue after a security event.
- Backups shall be **encrypted, tested quarterly, and stored in a secure location**.

9 Compliance & Enforcement

- IronHub shall conduct **internal audits annually** to validate security controls.
- Non-compliance with this policy may result in **disciplinary action** or **termination of employment/contracts**.

This **Information Security Policy** will be reviewed and updated **annually** to reflect new security risks and regulatory changes.