Control Environment Narrative

IronHub Inc

August 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC2.1, CC2.2, CC2.3, CC4.1, CC4.2, CC5.1, CC5.2, CC5.3

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document
Apr 21 2026	Updated to reflect current control environment, policies, and procedures

1 Control Environment Narrative

The following provides a description of the control structure of IronHub.

The intent of this description is to enumerate the logical, policy, and procedural controls that serve to monitor IronHub's application and data security. Changes uncovered by these procedures in the logical, policy, procedural, or customer environment are addressed by remediations specific to the noted change.

2 Logical Controls

IronHub employs several logical controls to protect confidential data and ensure normal operation of its core product.

- Mandatory data encryption at rest and in transit (TLS 1.2+ in transit; AES-256 at rest via Heroku and AWS)
- Multi-factor authentication (MFA) required for access to all cloud infrastructure and administrative systems
- Role-based access control (RBAC) with least-privilege provisioning via AWS IAM and SSO
- Activity and anomaly monitoring on production systems via DataDog
- Vulnerability management program including automated scanning and annual penetration testing
- Web Application Firewall (WAF) and DDoS protection via Cloudflare
- Error tracking and log aggregation via Rollbar and DataDog

3 Policy Controls

IronHub employs the following policies to protect confidential data and ensure normal operation of its core product:

- Access Onboarding and Termination Policy
- Application Security Policy
- Asset Management Policy
- Availability Policy
- Business Continuity Policy
- Code of Conduct Policy
- Confidentiality Policy
- Cyber Risk Assessment Policy
- Data Classification Policy
- Data Retention Policy
- Datacenter Policy
- Disaster Recovery Policy
- Encryption Policy
- Information Security Policy
- Log Management Policy

- Office Security Policy
- Password Policy
- Policy Training Policy
- Privacy Management Policy
- Processing Integrity Policy
- Remote Access Policy
- Removable Media and Cloud Storage Policy
- Risk Assessment and Management Policy
- Security Awareness Training Policy
- Security Incident Response Policy
- Software Development Policy
- System Change Policy
- Vendor Management Policy
- Vulnerability Management Policy
- Workstation Policy

4 Procedural Controls

IronHub has numerous scheduled procedures to monitor and tune the effectiveness of ongoing security controls, and a series of event-driven procedures to respond to security-related events.

4.1 Scheduled Security and Audit Procedures

- Review Access [quarterly]
- Review Security Logs [weekly]
- Review and Clear Low-Priority Alerts [weekly]
- Apply OS Patches [monthly]
- Vulnerability Scan — External-Facing Systems [monthly]
- Vulnerability Scan — Internal Systems and Infrastructure [quarterly]
- Review Asset Register [quarterly]
- Review Data Classification [quarterly]
- Review Devices and Workstations [quarterly]
- Backup Testing [quarterly]
- Verify Data Disposal per Retention Policy [quarterly]
- Review Security Monitoring and Alerting Configuration [quarterly]
- Vendor Assessment — Tier 1 Vendors [annual]
- Conduct Security Awareness Training [annual]
- Phishing Simulation [semi-annual]
- Disaster Recovery Testing [annual]
- Penetration Test [annual]
- Review Cyber Risk Assessment [annual]
- SOC 2 Audit [annual]

4.2 Event-Driven Security and Audit Procedures

- Onboard Employee
- Offboard Employee
- Investigate Security Alert
- Investigate and Respond to Security Incident
- Respond to Vulnerability Finding
- Process Data Subject Access Request

5 Remediations

IronHub uses the outcomes of the aforementioned controls and procedures to identify shortcomings in the existing control environment. Once identified, these shortcomings are remediated by improving existing controls and procedures, and creating new controls and procedures as needed. Findings from penetration tests, vulnerability scans, and audits are tracked to resolution by the Information Security Manager (ISM).

6 Communications

IronHub communicates relevant information regarding the functioning of the above controls with internal and external parties on an as-needed basis and according to statutory requirements.

6.1 Internal

IronHub communicates control outcomes, anomalies, and remediations internally using the following channels:

- Slack
- Email
- JIRA
- Zoho Desk

6.2 External

IronHub communicates relevant control-related information to external parties including shareholders, customers, contractors, regulators, and government entities as needed according to contractual and regulatory/statutory obligation.