System Architecture Narrative

IronHub Inc

August 2026

Contents

Table 1: Document history

Date	Comment
Jun 1 2018	Initial document
Apr 21 2026	Replaced placeholder with IronHub system architecture description

1 System Architecture Narrative

The following describes the system architecture of IronHub's platform, including its infrastructure components, data flows, boundary protections, and the controls in place to ensure availability, confidentiality, and integrity of the system and the data it processes.

2 System Boundaries

The IronHub system boundary encompasses:

- The IronHub web application and API hosted on Heroku
- The Heroku Postgres primary database and Heroku Redis cache
- AWS S3 file storage and AWS IAM access management
- Cloudflare DNS, WAF, and CDN layer
- DataDog monitoring and alerting infrastructure
- Rollbar error tracking and log aggregation
- IronHub-issued employee workstations and remote access infrastructure

Third-party services that integrate with the platform (e.g., DocuSign, credit bureaus, identity verification providers) are outside the IronHub system boundary but are governed by vendor agreements and assessed under the Vendor Management Policy.

3 Network Architecture

3.1 External Access

All inbound traffic from users (homebuilders and home buyers) passes through Cloudflare, which provides:

- DNS resolution
- TLS termination and certificate management
- Web Application Firewall (WAF) filtering for common web threats (OWASP Top 10)
- DDoS protection and rate limiting

Traffic passing Cloudflare is forwarded to Heroku over encrypted connections. Heroku provides load balancing and routing to application dynos.

3.2 Internal Access

Internal access to production systems (database, cloud consoles, deployment pipelines) is restricted to authorized personnel and requires:

- MFA on all cloud service consoles (Heroku, AWS, Cloudflare, DataDog)
- VPN or SSH tunneling for direct database access
- Role-based access via AWS IAM for S3 and related resources

3.3 Data Flow

1. **Buyer / Builder → Cloudflare → Heroku App**: Encrypted HTTPS request processed by the web application.
2. **Heroku App → Heroku Postgres**: Application queries database for customer and reservation data over an encrypted internal connection.
3. **Heroku App → AWS S3**: Documents and files uploaded or retrieved via encrypted API call using AWS IAM credentials.
4. **Heroku App → Third-party APIs** (DocuSign, identity verification, credit bureaus): Outbound encrypted API calls using service credentials managed in 1Password.
5. **Heroku App → DataDog / Rollbar**: Application metrics, logs, and errors forwarded over encrypted connections for monitoring.

4 Data Classification

IronHub processes the following categories of data within the system boundary:

Data Category	Classification	Examples
Buyer personal information	Restricted	Name, address, date of birth, government ID
Buyer financial data	Restricted	Income, credit score, bank account details
Buyer identity documents	Restricted	Uploaded government-issued ID, pay stubs
Homebuilder business data	Confidential	Lead lists, reservation data, pricing
Application logs	Internal Use	Access logs, error logs, system events
Marketing content	Public	Public-facing website content, brochures

Data handling requirements for each classification level are defined in the Data Classification Policy.

5 Availability Architecture

IronHub's platform relies on Heroku and AWS managed infrastructure, which provide:

- Automatic failover and redundancy for managed database services (Heroku Postgres)
- Geographic redundancy for file storage (AWS S3 with cross-region replication where configured)

- Automated daily backups of the production database, retained for 30 days
- Cloudflare's global anycast network for high-availability DNS and content delivery

Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are defined in the Business Continuity Plan and Disaster Recovery Policy.

6 Change Management

All changes to production systems follow the System Change Policy and IronHub's SCRUM-based software development lifecycle:

1. Changes are planned and reviewed in JIRA sprint planning.
2. Code changes undergo peer review via Bitbucket pull requests before merging.
3. Automated test suites run on all branches prior to merge.
4. Deployments to staging occur first; production deployments follow after validation.
5. Emergency changes follow the Emergency Change process defined in the System Change Policy.

7 Monitoring and Alerting

IronHub uses DataDog and Rollbar to provide continuous monitoring of the production environment:

- **Infrastructure monitoring**: CPU, memory, disk, and network metrics for all Heroku dynos and database instances.
- **Application performance monitoring**: Response times, error rates, and throughput tracked via DataDog APM.
- **Security alerting**: Anomalous access patterns, failed authentication attempts, and WAF events alerted to the ISM.
- **Error tracking**: Application exceptions and stack traces captured and alerted via Rollbar.
- **Log retention**: Application and access logs retained in accordance with the Log Management Policy.

Alerts are reviewed and triaged weekly as part of the Review and Clear Low-Priority Alerts procedure. High-severity alerts trigger immediate response per the Security Incident Response Policy.

8 References

8.1 Narratives

- Products and Services Narrative

- Security Architecture Narrative
- Organizational Narrative

8.2 Policies

- Application Security Policy
- Availability Policy
- Data Classification Policy
- Encryption Policy
- Log Management Policy
- Processing Integrity Policy
- System Change Policy
- Vulnerability Management Policy

8.3 Procedures

- Apply OS Patches
- Review Access
- Review and Clear Low-Priority Alerts
- Backup Testing
- Disaster Recovery Testing
- Vulnerability Scan (External and Internal)