

Products and Services Narrative

IronHub Inc

August 2026

Contents

1 Products and Services Narrative 2

2 Products 2

2.1 IronHub Home-Buying Platform 2

2.1.1 Overview 2

2.1.2 Key Features 2

2.1.3 Architecture 2

2.1.4 Security Considerations 3

3 References 3

3.1 Narratives 3

3.2 Policies 4

3.3 Procedures 4

Table 1: Document history

Date	Comment
Jun 1 2018	Initial document
Apr 21 2026	Replaced placeholder with IronHub-specific product and services description

1 Products and Services Narrative

This narrative describes the key products and services offered by IronHub and the security considerations specific to each.

2 Products

2.1 IronHub Home-Buying Platform

IronHub provides a white-labeled digital home-buying platform offered as a Software-as-a-Service (SaaS) solution to homebuilders across Canada. The platform enables homebuilders to digitize and automate the home reservation and buyer engagement process.

2.1.1 Overview

The IronHub platform is a web-based application that integrates with homebuilders' existing websites and sales workflows. It serves two primary user groups:

- **Homebuilders:** Organizations that configure and embed the IronHub platform into their sales process to manage leads, reservations, and buyer communications.
- **Home Buyers:** Individuals who interact with the platform to explore homes, verify their identity and financial qualification, and complete a home reservation online.

2.1.2 Key Features

1. **Application Automation** — Automates lead capture, buyer engagement workflows, and reservation processing.
2. **Customer Verification** — Identity verification, document verification, and fraud prevention for prospective buyers.
3. **Credit and Financial Verification** — Integration with credit bureaus and financial data providers for income and liability assessment.
4. **Home Personalization Tool** — Allows buyers to explore home options, configure selections, and receive real-time pricing.
5. **Home Reservation Suite** — Enables 24/7 online home reservations with secure deposit processing and digital document execution via DocuSign.
6. **Analytics and Buyer Insights** — Real-time dashboards for homebuilders showing buyer behaviour, lead status, and conversion metrics.

2.1.3 Architecture

The IronHub platform is built on a multi-tenant architecture hosted on Heroku and AWS. Customer data is logically separated at the application and database

layer. The platform communicates with external services (DocuSign, credit bureaus, identity verification providers) via encrypted API connections.

Key architectural components include:

Component	Technology	Purpose
Web Application	Heroku	Application hosting and routing
Database	Heroku Postgres	Primary relational data store (multi-tenant)
Cache	Heroku Redis	Session management and performance caching
Document Storage	AWS S3	Encrypted storage for uploaded documents
Access Management	AWS IAM	Cloud resource access control
DNS / WAF	Cloudflare	Traffic routing, DDoS protection, WAF
Monitoring	DataDog	Uptime monitoring, alerting, anomaly detection
Error Tracking	Rollbar	Application error tracking and alerting
Document Execution	DocuSign	Digital signature and document workflow

2.1.4 Security Considerations

- All data in transit is encrypted using TLS 1.2 or higher.
- All data at rest is encrypted using AES-256 via Heroku and AWS managed encryption.
- Production database access is restricted to the CTO and designated senior engineers via VPN.
- The platform implements input validation, duplicate detection, and authorization controls to ensure processing integrity.
- Buyer identity and financial data is classified as Restricted and handled in accordance with the Data Classification Policy and Privacy Management Policy.
- Integration credentials and API keys are managed via 1Password and rotated on a defined schedule.
- The platform undergoes annual penetration testing and monthly external vulnerability scanning.

3 References

3.1 Narratives

- Organizational Narrative
- Security Architecture Narrative

- System Architecture Narrative

3.2 Policies

- Application Security Policy
- Data Classification Policy
- Encryption Policy
- Log Management Policy
- Password Policy
- Privacy Management Policy
- Processing Integrity Policy
- Security Incident Response Policy
- Vendor Management Policy

3.3 Procedures

- Apply OS Patches
- Review Access
- Review and Clear Low-Priority Alerts
- Vulnerability Scan (External and Internal)
- Penetration Test