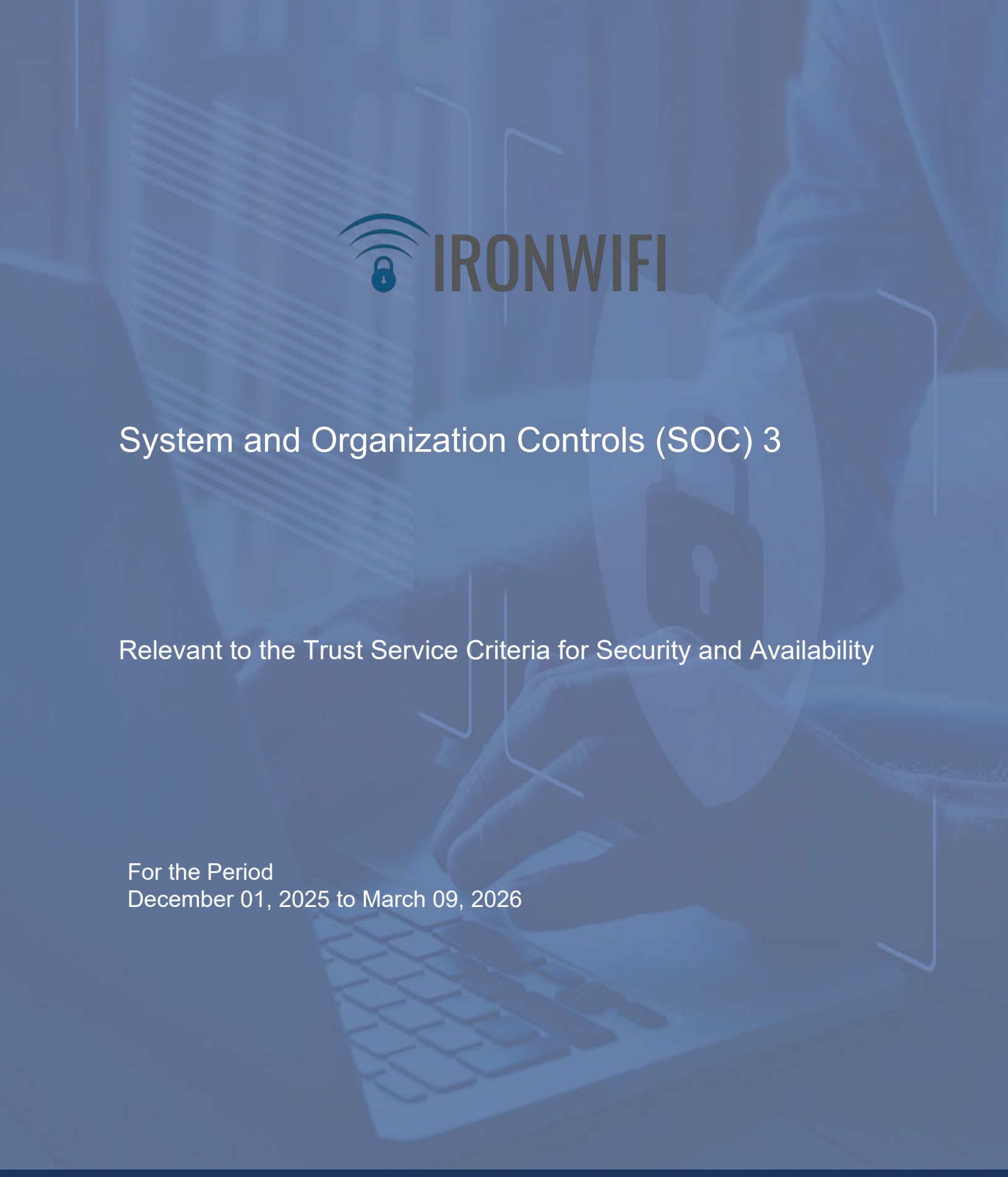


IRONWIFI

System and Organization Controls (SOC) 3

Relevant to the Trust Service Criteria for Security and Availability

For the Period
December 01, 2025 to March 09, 2026

JOHANSON GROUP

johansonllp.com

Table of Contents

I.	**Independent Service Auditor's Report**	**3**
II.	**Assertion of IronWifi LLC Management**	**6**
III.	**Description of the IronWifi Platform**	**8**



Section I
Independent Service Auditor's Report

I. Independent Service Auditor's Report

IronWifi LLC

Scope

We have examined IronWifi LLC's accompanying assertion titled "Assertion of IronWifi LLC Management" (assertion) that the controls within IronWifi LLC's IronWifi Platform (system) were effective throughout the period December 01, 2025 to March 09, 2026, to provide reasonable assurance that IronWifi LLC'sservice commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria.

Service Organization's Responsibilities

IronWifi LLC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that IronWifi LLC's service commitments and system requirements were achieved. IronWifi LLC has provided an assertion titled "Assertion of IronWifi LLC's Management" (assertion) about the description and the suitability of the design and operating effectiveness of the controls stated therein. IronWifi LLC is responsible for preparing the description and assertion; including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description, and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

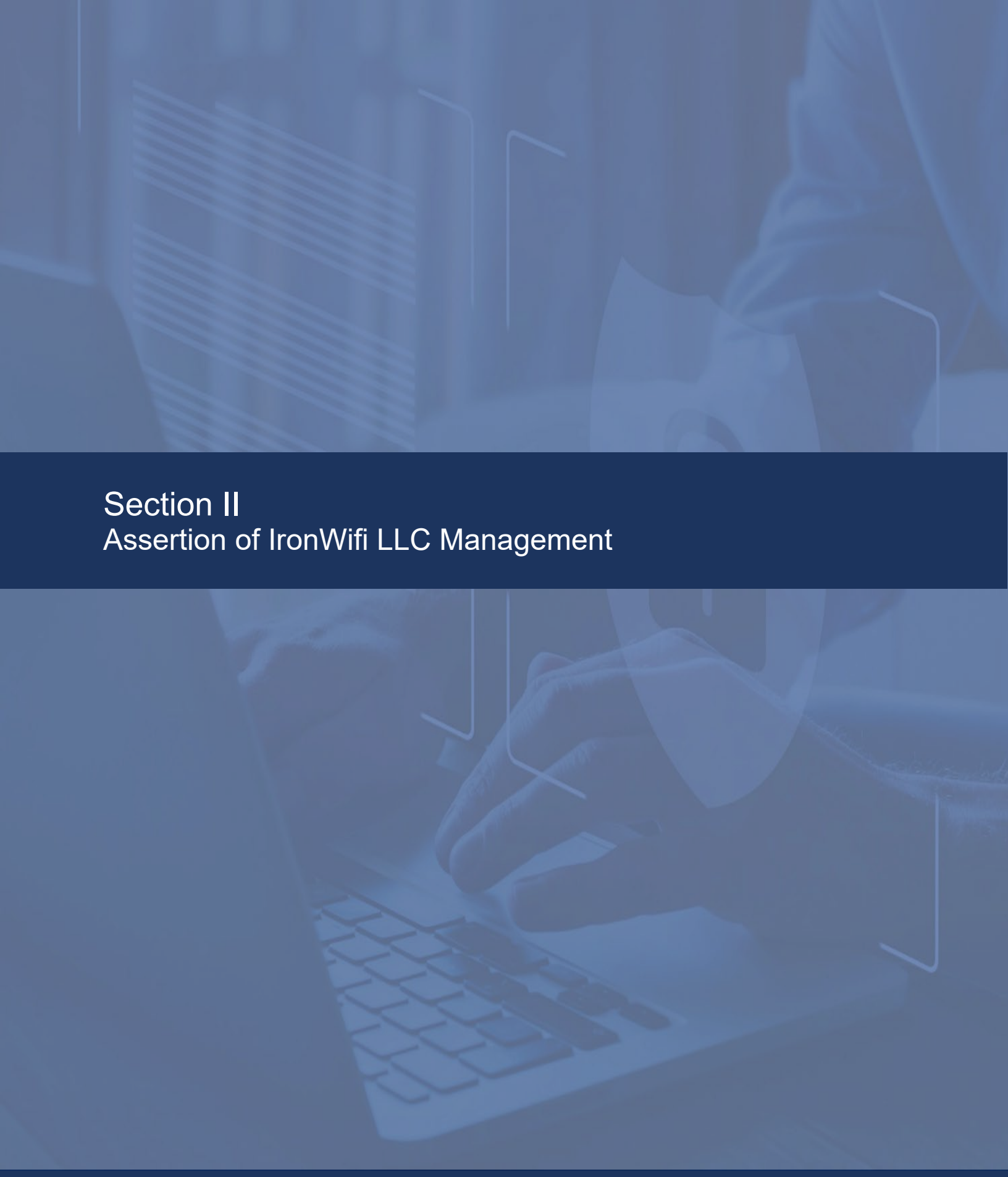
Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within IronWifi LLC'sIronWifi Platform (system) were effective throughout the period December 01, 2025 to March 09, 2026, to provide reasonable assurance that IronWifi LLC service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
May 7, 2026



Section II
Assertion of IronWifi LLC Management

II. Assertion of IronWifi LLC Management

We are responsible for designing, implementing, operating, and maintaining effective controls within IronWifi LLC IronWifi LLC's IronWifi Platform (system) throughout the period December 01, 2025 to March 09, 2026, to provide reasonable assurance that IronWifi LLC's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of IronWifi Platform" and identifies the aspects of the system covered by our assertion.

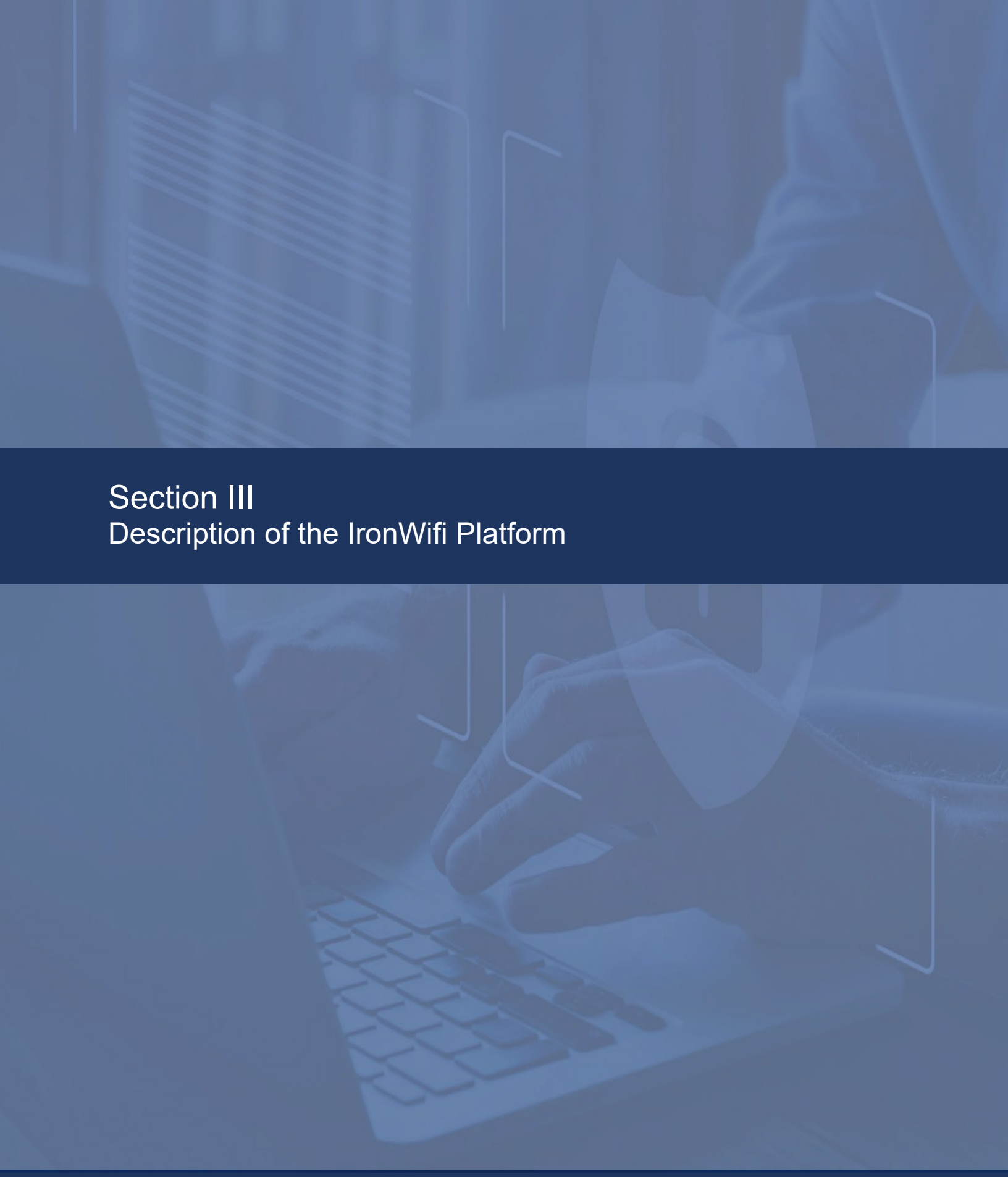
We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 01, 2025 to March 09, 2026, to provide reasonable assurance that IronWifi LLC IronWifi LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria.

IronWifi LLC's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 01, 2025 to March 09, 2026, to provide reasonable assurance that IronWifi LLC's service commitments and system requirements were achieved based on the applicable trust services criteria.

IronWifi LLC Management
May 7, 2026



Section III
Description of the IronWifi Platform

III. Description of the IronWifi Platform

Company Background

IronWifi was founded in 2014 by Martin Benuska with the objective of making enterprise WiFi authentication simple, secure, and accessible for organizations of all sizes. The company is headquartered at 100 E Pine St, Ste 110, Orlando, FL 32801, USA, and operates as a fully remote organization with team members distributed globally.

IronWifi serves as the identity infrastructure layer enabling federated WiFi, providing trust, identity, and policy enforcement for seamless global connectivity. The platform delivers cloud-based RADIUS authentication, captive portal, and certificate management services to over 1,000 organizations across 108 countries, processing more than 50 million authentications per month.

IronWifi LLC operates with six in-scope personnel during the audit period: one full-time employee and one W-2 contractor in the United States, and one full-time employee and three contractors in the United Kingdom. The team carries 100+ combined years of networking and security expertise (Two external advisors and one on-leave contractor are excluded from the in-scope count). Industries served include coworking and shared workspaces, hospitality, enterprise, education, healthcare, retail, manufacturing, service providers, and government agencies.

Description of Services Overview or Services Provided

IronWifi provides a cloud-based RADIUS Authentication, Authorization, and Accounting (AAA) platform and Captive Portal solution that protects wired and wireless networks of any size. The IronWifi Platform is delivered as a multi-tenant software-as-a-service (SaaS) application accessible through a secure web console and REST API. The platform enables organizations to authenticate users and devices connecting to their networks without deploying or maintaining on-premises RADIUS servers.

The IronWifi Platform includes the following core services:

- **Cloud RADIUS Server (RADIUS-as-a-Service):** Hosted RADIUS authentication deployed across multiple global regions for low-latency authentication. Supports WPA-Enterprise (WPA2/WPA3), 802.1X authentication protocols including EAP-TLS, PEAP-MSCHAPv2, EAP-TTLS, and MAC Authentication Bypass. Provides 99.9% uptime SLA with automatic failover between regions.
- **Captive Portal:** Customizable login pages for guest WiFi access supporting social login (Google, Facebook, LinkedIn, Apple), email/SMS registration, voucher codes, and payment integration (Stripe, PayPal, Square, Braintree). Includes marketing data collection and CRM integration capabilities.
- **WPA-Enterprise/802.1X Authentication:** Individual user credential management replacing shared WiFi passwords. Integrates with identity providers, including Azure AD/Entra ID, Okta, Google Workspace, OneLogin, and Active Directory/LDAP for centralized user authentication.
- **Cloud PKI/Certificate Management:** Private certificate authority with automatic lifecycle management. Provides SCEP auto-enrollment and an enrollment portal supporting Windows, Mac, iOS, Android, and ChromeOS devices for certificate-based EAP-TLS authentication.
- **IoT Authentication:** Certificate-based or MAC-based device onboarding with automatic VLAN segmentation for IoT devices.

- Roaming and Mobility: Passpoint / Hotspot 2.0 support for automatic WiFi connections. OpenRoaming (WBA) federation providing access to over 3 million global hotspots. WiFi Calling with SIM-based authentication for carrier-grade voice offload.

- **Policy and Analytics:** Conditional access with a visual policy builder and pre-built compliance templates. Device trust with real-time posture checks and auto-quarantine. Network intelligence with authentication analytics and anomaly detection. Identity provisioning with SCIM sync from major identity providers.

Information is shared with user entities through the secure web console, REST API with real-time webhooks, email notifications, and encrypted support channels.

Principal Service Commitments and System Requirements

IronWifi designs its processes and procedures related to its platform to meet its objectives for cloud RADIUS authentication and captive portal services. Those objectives are based on the service commitments that IronWifi makes to user entities, the laws and regulations that govern the provision of IronWifi services, and the financial, operational, and compliance requirements that IronWifi has established for the services. The services of IronWifi are subject to the security and privacy requirements of GDPR, CCPA, HIPAA (with BAA), and other applicable state, federal, and international privacy and security laws and regulations in the jurisdictions in which IronWifi operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online at ironwifi.com.

Security Commitments

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the IronWifi Platform are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of TLS 1.3 encryption technologies to protect customer data in transit and AES-256 encryption to protect customer data at rest.
- Multi-region deployment with automatic failover to maintain 99.9% service availability.
- RadSec (RADIUS over TLS) for secure transport of authentication traffic between customer network equipment and the IronWifi cloud.
- Certificate-based authentication (EAP-TLS) is the highest security option for network access.

IronWifi establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in IronWifi's system policies and procedures, system design documentation, and contracts with customers.

Availability Commitments

IronWifi is committed to maintaining the availability of its platform in accordance with service level commitments. Performance and availability are monitored continuously using Prometheus, Grafana, Google Cloud Monitoring, and UptimeRobot. Customer-reported issues are responded to in a timely manner in accordance with documented support procedures. IronWifi maintains a Business Continuity and Disaster Recovery (BC/DR) plan with a tiered internal target of Recovery Time Objective (RTO) of 1 hour for critical functions, 4 hours for full; a target Recovery Point Objective (RPO) of 5 minutes for transactional and 1 hour for analytics considering customer SLA disclaimer

and leveraging Google Cloud Spanner's multi-region replication and automated failover capabilities. Operational procedures, including incident response, escalation, and communication, are documented and tested to ensure rapid restoration of services in the event of a disruption.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the IronWifi Platform.

Components of the System

Infrastructure

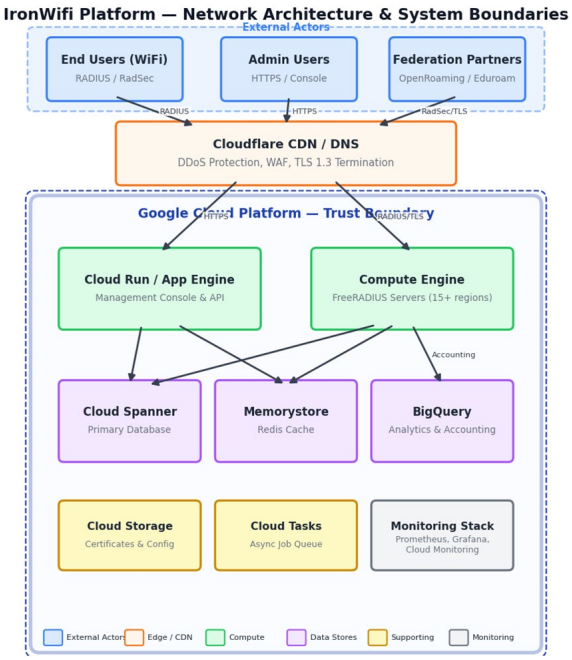
The IronWifi Platform's infrastructure is hosted entirely on Google Cloud Platform (GCP), ensuring scalability, reliability, and global reach. The platform is deployed across multiple GCP regions to provide low-latency service worldwide and automatic failover capabilities.

Primary infrastructure components include:

- **Google App Engine/Cloud Run:** The IronWifi management console is deployed on Google App Engine with automatic scaling across multiple global regions, including us-central1, us-east1, us-west1, europe-west1, europe-west2, asia-southeast1, asia-east1, australia-southeast1, and africa-south1.
- **Google Compute Engine:** FreeRADIUS authentication server instances run on Compute Engine virtual machines deployed across 15+ global regions, including North America, South America, Europe, Asia, Australia, and Africa. Multiple RADIUS instances per server provide redundancy with process supervision.
- **Google Cloud Spanner:** The primary globally-distributed database providing automatic replication across regional instances. Cloud Spanner serves as the backend for RADIUS authentication lookups via its PostgreSQL-compatible interface.
- **Google BigQuery:** Used for authentication analytics, accounting data storage, and log aggregation.
- **Google Cloud Memorystore (Redis):** Dedicated Redis instances deployed per region for caching authentication data and session information.
- **Google Cloud Storage:** Used for file storage, static content delivery, and CDN.
- **Google Cloud Tasks:** Asynchronous task processing for background operations.
- **Cloudflare:** DNS management and CDN services for the web console and API endpoints.

Primary Infrastructure		
Hardware/Service	**Type**	**Purpose**
Cloud Run	PaaS / Serverless	Management console hosting with automatic scaling.
Google Compute Engine	IaaS (Virtual Machines)	FreeRADIUS authentication server instances across multiple regions.
Google Cloud Spanner	Managed Database	Globally-distributed primary database with automatic multi-region replication.
Google BigQuery	Data Warehouse	Authentication analytics, accounting data, and log aggregation.
Google Cloud Memorystore	Managed Cache (Redis)	Per-region caching for authentication data and session state.
Google Cloud Storage	Object Storage	File storage, static content delivery, and CDN.
Google Cloud Tasks	Task Queue	Asynchronous background task processing.
Cloudflare	CDN/DNS	DNS management and CDN for web console and API endpoints.

Figure 1: IronWifi Platform Network Architecture and System Boundaries



Software

Primary software used to provide the IronWifi Platform includes the following:

- **FreeRADIUS 3.x:** The core RADIUS authentication engine, RFC 2865 compliant, supporting EAP-TLS, PEAP-MSCHAPv2, EAP-TTLS, PAP, CHAP, and MAC Authentication Bypass.
- **radsecproxy:** RADIUS over TLS proxy used for OpenRoaming and Eduroam federation connections.

- **IronWifi Management Console:** Custom-built PHP 8.2 web application built on the Laminas (formerly Zend) framework, providing the administrative interface for account management, RADIUS configuration, captive portal design, certificate management, and analytics.
- **Prometheus and Grafana:** Infrastructure and RADIUS server monitoring with custom exporters for authentication metrics.
- **Bugsnag:** Application error tracking and reporting for the management console.
- **Google Cloud Monitoring:** Cloud infrastructure monitoring and alerting via the GCP Ops Agent.
- **UptimeRobot:** External uptime monitoring of production services and endpoints.
- **Snyk and Dependabot:** Automated vulnerability scanning for application dependencies and open-source components.
- **GitHub Actions:** CI/CD pipeline for automated testing (PHPUnit, Playwright), security scanning, code style enforcement, and canary deployments to production.

Primary Software		
System/Application	**Operating System**	**Purpose**
FreeRADIUS 3.x	Debian Linux	Core RADIUS authentication engine (RFC 2865, EAP-TLS, PEAP, EAP-TTLS).
Radsecproxy	Debian Linux	RADIUS over TLS proxy for OpenRoaming and Eduroam federation.
IronWifi Management Console	Cloud Run	PHP 8.2 web application (Laminas framework) for platform management.
Prometheus	Debian Linux	Infrastructure and RADIUS server monitoring.
Grafana	Debian Linux	Monitoring dashboards and alerting visualization.
Bugsnag	SaaS	Application error tracking and reporting.
Google Cloud Monitoring	GCP Managed	Cloud infrastructure monitoring and alerting.
UptimeRobot	SaaS	External uptime monitoring of production services.
Snyk	SaaS	Automated vulnerability scanning for application dependencies.

Compute Engine VMs run Debian Linux as the base operating system.

People

IronWifi has a staff of six in-scope professionals with over 100 combined years of networking and security expertise, organized into the following functional areas:

- **Management:** Executive leadership includes CEO Martin Benuska and CTO Seb Adamski. Leadership is responsible for strategic direction, enabling employees to perform their roles effectively, and establishing the organization's security, availability, and confidentiality commitments.
- **Product Development:** Software engineers who design and maintain the IronWifi Platform, including the management console, RADIUS server configurations, captive portal engine, certificate management system, API endpoints, and all integration modules. This team designs and implements new functionality, assesses and remediates any issues or bugs, and architects and deploys the underlying cloud infrastructure on which IronWifi runs. Members of the product team are responsible for peer reviews of code and infrastructure changes.

- **Technical Operations:** The monitoring and maintenance of the IronWifi production environment is handled by the operations role, which involves proactively designing and deploying monitoring software and tools (Prometheus, Grafana, UptimeRobot) to identify errors in the platform and remediate them. The operations team responds to alerts generated by the system, identifies issues with RADIUS authentication, captive portal services, and cloud infrastructure, and determines the best path to resolution. Operations personnel also ensure that authentication services are performing optimally with high throughput and low latency across all global regions. Finally, operations are responsible for responding to any potential security incidents and notifying affected customers if applicable.

- **Customer Success:** Individuals who work to support IronWifi customers. They are the primary point of contact for customer inquiries and help identify which parts of the IronWifi Platform are most useful to prospective customers. The customer success team assists customers with onboarding, network equipment configuration, identity provider integration, and proactively identifies any issues that occur during deployment and ongoing operations.

- **Business Development and Marketing:** Individuals responsible for marketing, sales, and expanding the IronWifi customer base. They identify best practices for secure WiFi authentication and provide that information to customers and prospective customers through documentation, webinars, and other channels.

- **Quality Assurance:** Personnel responsible for testing platform functionality, ensuring software quality through automated and manual testing processes, and validating that changes meet acceptance criteria before production deployment.

IT management responsibilities, including infrastructure provisioning, access management, and security operations, are managed within the Technical Operations team. IronWifi operates as a fully remote workforce; there are no on-premises IT facilities or physical office infrastructure to manage.

Data

There are four major types of data used by the IronWifi Platform:

- Configuration Data: Data used to configure RADIUS authentication, captive portals, certificates, and network policies.
- Authentication Data: Credentials, certificates, and identity attributes used to authenticate users and devices.
- Accounting Data: Session records produced during network access sessions, including timestamps, data usage, and connection metadata.
- Log Data: Logs, traces, and monitoring data produced by the RADIUS servers and management console during operation.

Configuration Data is stored in IronWifi's primary Cloud Spanner databases and includes: customer account information (email addresses, names, company names); credentials for accessing identity providers and external authentication sources (OAuth tokens, LDAP connection strings); network access server (NAS) definitions including shared secrets; RADIUS policies, VLAN assignments, and attribute configurations; captive portal templates and customizations; certificate authority configurations; and audit logs covering changes to each of the above items.

Configuration Data is treated as sensitive by IronWifi. Access controls enforce data isolation between customer accounts using owner_id-based segmentation at the database level. Customers can invite other people in their

organization to access their IronWifi account and read and write configuration data. IronWifi operators may access configuration data to troubleshoot customer issues with appropriate authorization and audit logging.

Authentication Data includes usernames, passwords (stored as hashed values), MAC addresses, device identifiers, and X.509 certificates used for EAP-TLS authentication. This data is stored in Cloud Spanner with strict access controls. Passwords are stored using industry-standard hashing algorithms. Certificates are managed through the built-in PKI system with automated lifecycle management. External authentication sources (Azure AD, Okta, Google Workspace, LDAP) are accessed in real-time during authentication, and IronWifi does not persistently store external identity provider credentials.

Accounting Data consists of RADIUS accounting records generated during network access sessions. These records include session identifiers, start and stop timestamps, session duration, bytes transferred (in and out), calling station ID (MAC address), NAS identifiers, and assigned IP addresses. Accounting data is stored in BigQuery for analytics and reporting purposes and is subject to data retention policies.

Log Data is produced by the RADIUS servers and management console to make it easier for IronWifi operators to monitor the health of the system and track down any issues. Log data includes authentication event traces, error messages, stack traces, and performance metrics. Log data is stored in Google Cloud Logging and BigQuery with limited retention periods. IronWifi endeavors to minimize the inclusion of sensitive data in log records.

All data types processed by IronWifi are encrypted in transit using TLS 1.3. RADIUS authentication traffic between customer network equipment and IronWifi servers can be secured using RadSec (RADIUS over TLS). All data stored by IronWifi is encrypted at rest using AES-256 encryption managed through Google Cloud KMS.

Data Classification

Category	Description	Examples
Public	Information intended for public distribution that poses no risk if disclosed.	Marketing materials, public-facing documentation, published API specifications
Internal	Operational information not intended for external distribution.	Internal policies, architecture documentation, meeting notes
Customer Data	Data belonging to or originating from IronWifi customers requires the highest level of protection.	RADIUS credentials, authentication logs, captive portal configurations, and certificate data
Company Data	Proprietary business information requiring protection from unauthorized disclosure.	Source code, financial records, employee information, security configurations

Data Retention

IronWifi retains data in accordance with its Data Retention Policy. Authentication and accounting data are retained for a minimum of 12 months to support operational and compliance needs. Log data is retained for 90 days in active storage and archived for up to 12 months. Customer configuration data is retained for the duration of the customer's active subscription and for 30 days following account termination. Upon expiration of retention periods, data is disposed of through secure deletion methods appropriate to the storage medium, including cryptographic erasure for data stored in Google Cloud Spanner and secure deletion for data in Google Cloud Storage and BigQuery.

Processes and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the IronWifi policies and procedures that define how services should be delivered. These are maintained in the company's internal documentation systems and can be accessed by any IronWifi team member.

Physical Security

All production data and infrastructure are hosted by Google Cloud Platform (GCP). GCP data centers do not allow IronWifi employees physical access. Physical security of data centers is managed entirely by Google and is subject to Google's SOC 2 report and other applicable certifications.

IronWifi reviews GCP's SOC 2 attestation reports on at least an annual basis to ensure that physical security and environmental controls at GCP data centers continue to meet IronWifi's requirements.

IronWifi operates as a fully remote organization and does not maintain physical office space. All work is conducted remotely by team members using company-approved devices with full-disk encryption and endpoint monitoring tools installed.

Logical Access

IronWifi employees and contractors are granted access to infrastructure via a role-based access control system, to ensure uniform, least-privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

IronWifi infrastructure runs entirely on cloud and SaaS-based systems, and as such, the resources used by employees to perform their roles are accounts and permissions within those systems. Access levels follow the principle of least privilege, with administrative access restricted to personnel whose roles require it.

IronWifi identifies employees primarily by their Google Workspace account, which functions as the corporate directory and SSO provider. The IronWifi security policy mandates that employees and contractors use their Google Workspace accounts to sign in to SaaS and cloud tools when supported. When Google Workspace sign-in is not available, employees authenticate using strong, unique passwords stored in an approved password manager.

Multi-factor authentication (MFA) is required for all access to GCP, GitHub, and other critical systems. Any SaaS applications used by the company that do not support Google Workspace SSO must be configured to use a second factor when possible.

When an employee is onboarded, management provisions the appropriate accounts based on the employee's role and performs a background check. The employee is responsible for reviewing IronWifi's policies, completing security awareness training, and successfully enrolling a device for multi-factor authentication.

When an employee is terminated, management is responsible for revoking all of the employee's accounts within one business day. Access reviews are conducted quarterly to verify that access levels remain appropriate and follow the principle of least privilege.

Access Levels and Policies

IronWifi defines the following access levels for system resources: Administrator (full access to infrastructure and configuration), User (standard access to perform role-specific duties), Read-Only (view-only access for monitoring and audit purposes), and No Access (default for systems outside an individual's role). Access levels are assigned based on the principle of least privilege.

New employee accounts are provisioned prior to start date. Access requests are submitted by management and approved based on the employee's role and responsibilities.

Password policy requires a minimum of 8 characters with complexity requirements including uppercase letters, lowercase letters, numbers, and special characters. Password reuse is prohibited for the last 5 passwords.

Passwords expire every 180 days. Multi-factor authentication is required for all corporate Google Workspace accounts. All credentials are stored in an approved password manager.

Full-disk encryption is required on all devices used to access IronWifi systems. Upon employee termination, company-owned devices are wiped, and all credentials and access tokens are revoked within one business day.

Computer Operations - Backups

Customer data is backed up automatically through Google Cloud Spanner's built-in replication across multiple availability zones and regions. Cloud Spanner provides automatic, synchronous replication of data across zones within a region, ensuring high availability and data durability.

Additional backup infrastructure is maintained in GCP, with physical access restricted according to applicable Google Cloud policies. All backups are encrypted at rest using Google Cloud KMS-managed encryption keys, with access restricted to key personnel via GCP IAM permissions. Database backups are retained for 30 days per the data retention policy.

The Technical Operations team monitors backup health through automated alerting and periodic review. Backup failures trigger immediate notification to the operations team for investigation and resolution.

When a backup exception occurs, the Technical Operations team performs troubleshooting to identify the root cause. Failed backups are rerun manually when feasible, or deferred to the next scheduled backup window if the issue is transient. Persistent failures are escalated for resolution.

Backup restore procedures are tested periodically to validate the integrity and recoverability of backed-up data.

Computer Operations - Availability

IronWifi maintains an Incident Response Policy that gives any IronWifi employee the ability to initiate a response to a potential security incident by notifying the internal security team through designated channels and assists in classifying the severity of the incident.

External parties (customers and third-party security researchers) are given channels to report potential issues to the IronWifi team at support@ironwifi.com.

Internally, the IronWifi operations team monitors the health of all applications and infrastructure using Prometheus, Grafana, Google Cloud Monitoring, and UptimeRobot. Monitoring includes the availability and performance of the management console, the throughput and latency of RADIUS authentication servers, Redis cache health, Cloud Spanner database performance, and any faults or errors encountered during authentication processing. Critical incidents trigger automated alerts to on-call personnel.

IronWifi maintains a Business Continuity Plan with target Recovery Time Objectives (RTO) of 1 hour for critical functions and 4 hours for full-service restoration. Recovery Point Objectives (RPO) are 5 minutes for transactional data and 1 hour for analytics data. The multi-region deployment architecture ensures that if one region experiences an outage, authentication traffic is automatically routed to healthy regions.

IronWifi employs vulnerability scanning tools, including Snyk, Dependabot, and Composer audit, that check application dependencies for known vulnerabilities. Automated security scanning runs weekly and, on every dependency, change through the CI/CD pipeline.

IronWifi maintains a patch management process for operating systems and infrastructure components. Critical security patches are applied within 72 hours of release. Non-critical patches are applied during scheduled maintenance windows. Patch deployment follows the standard change control process, including testing in a non-production environment before production rollout.

Change Management

IronWifi maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

GitHub is utilized as both a version control system and a change management platform. All changes to the IronWifi codebase are tracked through pull requests, which require peer review and approval before merging. Automated testing through GitHub Actions validates changes, including unit tests (PHPUnit), end-to-end tests (Playwright), security scans, and code style enforcement.

Development and testing are performed in environments that are logically separated from the production environment. The CI/CD pipeline enforces a canary deployment pattern for production releases, where new versions initially receive zero traffic and are gradually promoted after validation. The pipeline includes safety checks such as holiday blackout windows and off-hours deployment warnings.

Version control software maintains a complete history of code changes to support rollback capabilities and tracks all changes to individual developers.

Data Communications

IronWifi utilizes Google Cloud Platform's infrastructure-as-a-service and platform-as-a-service offerings to run its production infrastructure, leveraging GCP's built-in network security controls, including VPC networking, firewall rules, and DDoS protection.

All external communications are encrypted using TLS 1.3. RADIUS authentication traffic between customer network equipment and IronWifi servers supports RadSec (RADIUS over TLS) for encrypted transport. The management console and API endpoints are accessible only via HTTPS connections through Cloudflare CDN, which provides an additional layer of DDoS protection and web application firewall capabilities.

IronWifi engages an external security firm to perform annual penetration testing covering both network and application layer testing. Automated vulnerability scanning runs continuously via Snyk, Dependabot, and Composer audit, with weekly infrastructure scans. Results are reviewed by the Technical Operations team, and identified vulnerabilities are triaged and remediated according to their severity.

IronWifi does not maintain a corporate network, intranet, or VPN, but instead opts to use SaaS and cloud applications hosted on the public internet and secured by TLS connections and SSO with MFA.

Vendor Management

IronWifi maintains a vendor management program to assess and monitor the security posture of third-party service providers. The program applies to all vendors that process, store, or have access to customer data or critical infrastructure components.

Vendor risk assessments are performed prior to engagement and consider factors including: the type and sensitivity of data the vendor will access, the vendor's security certifications and attestation reports (SOC 2, ISO 27001, or equivalent), the vendor's security policies and incident response capabilities, and the vendor's data handling and encryption practices.

Ongoing vendor monitoring includes annual review of vendor SOC 2 or equivalent attestation reports, monitoring of vendor security advisories and service status communications, and periodic reassessment of vendor risk based on changes in services consumed or data shared.

Contractual agreements with vendors include security requirements covering data protection, confidentiality obligations, incident notification, and data return or destruction upon termination of the engagement.

Boundaries of The System

The scope of this report includes the IronWifi Platform services, including Cloud RADIUS authentication, Captive Portal, Certificate Management, and the Management Console. This report does not include the data center hosting services provided by Google Cloud Platform (GCP).

IronWifi operates as a fully remote organization with no physical office facilities in scope for this examination.

Production workloads run in the following Google Cloud Platform regions: us-central1 (Iowa), europe-west1 (Belgium), asia-east1 (Taiwan), and australia-southeast1 (Sydney). Google Cloud Spanner instances are configured for multi-region replication to ensure data durability and low-latency access.

The Applicable Trust Services Criteria and The Related Controls

Common Criteria (to the Security and Availability Categories)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage, and ii. systems that use electronic information to process, transmit, or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of IronWifi's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of IronWifi's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties, is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

IronWifi's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for jobs and translated the required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions, including annual security awareness training for all employees.

Management’s Philosophy and Operating Style

The IronWifi management team must balance two competing interests: continuing to grow and develop in the rapidly evolving network security and WiFi authentication space while remaining excellent and conservative stewards of the highly sensitive authentication data and network access workflows that customers entrust to the platform.

The management team regularly reviews technology changes that impact WiFi authentication standards (including WPA3, Passpoint/Hotspot 2.0, and OpenRoaming), new security technologies that can help protect customer networks, and regulatory changes that may require IronWifi to alter its platform to maintain legal compliance. Major planned changes to the business are reviewed by the management team to ensure they are compatible with core service offerings and duties to customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility

IronWifi is organized in a lean, flat structure appropriate for its size. The organizational structure ensures that employees clearly understand their role in the organization, how they and their team are responsible for furthering company-wide initiatives, and channels for reporting. As the team grows, management will continue to build an organizational structure that maintains clear lines of authority and responsibility.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

IronWifi's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. IronWifi's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement during onboarding.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process, including revocation of all system access within one business day.

Risk Assessment Process

IronWifi's risk assessment process identifies and manages risks that could potentially affect IronWifi's ability to provide reliable and secure services to customers. As part of this process, IronWifi maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates, the commitments, agreements, and responsibilities of IronWifi's system, as well as the nature of the components of the system, result in risks that the criteria will not be met. IronWifi addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, IronWifi's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communication Systems

Information and communication are an integral component of IronWifi's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

IronWifi uses several information and communication channels internally to share information with management, employees, contractors, and customers. IronWifi uses Slack and email as the primary internal communication channels. Customer communication is handled through the support system at support@ironwifi.com and through the IronWifi documentation portal.

Structured data is communicated internally via SaaS applications and project management tools. IronWifi uses video meetings to communicate company priorities and goals from management to all employees. General updates to security policies and procedures are communicated to appropriate personnel via email and internal documentation systems.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. IronWifi's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

IronWifi's management conducts quality assurance monitoring on a regular basis, and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective action through team meetings, internal communications, and direct notifications.

Management's close involvement in IronWifi's operations helps to identify significant variances from expectations regarding internal controls. Management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of IronWifi's operations.

Reporting Deficiencies

Internal tracking tools are utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System

The following summarizes significant changes to the IronWifi system during the period December 1, 2025, through March 9, 2026:

Q1 2026 (January – March)

- Migrated primary database from PostgreSQL to Google Cloud Spanner (v2.0.0, initiated Dec 2025 — fully rolled out Q1 2026).
- Launched Policies engine with pre-computed RADIUS attribute materialization.
- Deployed MSP Tenant Lifecycle API with suspend/resume and tenant tagging.
- Implemented ITDR (Identity Threat Detection & Response) Phase 2 with playbooks and response actions.
- Added WebAuthn backup codes and TOTP authenticator two-factor authentication.
- Introduced multi-tenant Okta OAuth2 SSO for the admin console.
- Deployed zero-downtime automated deployment pipeline (dev → staging → production).
- Applied security patch PT-2025-003 (license bypass prevention).

Q4 2025 (October – December)

- Added multi-region deployment support and fleet management for aviation customers.
- Implemented two-factor authentication, HTTPS enforcement, and enhanced XSRF protection.
- Added comprehensive security documentation aligned with ISO 27001.

Q3 2025 (July – September)

- No significant infrastructure changes recorded in the changelog.

Q2 2025 (April – June)

- Launched Reports module with 50+ report types and BigQuery analytics integration.

For a complete changelog, see: https://us-central1.ironwifi.com/changelog

Incidents

No significant incidents have occurred in the services provided to user entities during the review period.

Criteria Not Applicable to the System

All Common Criteria/Security and Availability trust services criteria were applicable to IronWifi's system.

Subservice Organizations

This report does not include the data center hosting services provided by Google Cloud Platform (GCP).

Subservice Description of Services

Google Cloud Platform provides the foundational infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) capabilities upon which the IronWifi Platform operates. GCP services consumed by IronWifi include Compute Engine, App Engine, Cloud Run, Cloud Spanner, BigQuery, Cloud Memorystore, Cloud Storage, Cloud Tasks, and Cloud Monitoring. GCP maintains its own SOC 2 Type II report covering the Security and Availability, Confidentiality, and Privacy trust services criteria.

Complementary Subservice Organization Controls

IronWifi's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to IronWifi's services to be solely achieved by IronWifi's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of IronWifi.

The following subservice organization controls should be implemented by Google Cloud Platform (GCP) to provide additional assurance that the trust services criteria described within this report are met:

Subservice Provider – GCP		
Category	**Criteria**	**Control**
Security	CC 6.4	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors have been established.
		Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps/portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24/7 by security personnel.
Availability	A 1.2	The Datacenter Management team maintains and tests the data center-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

IronWifi management, along with the subservice provider, defines the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, IronWifi performs monitoring of the subservice organization controls, including the following procedures.

- Reviewing and reconciling output reports.
- Holding periodic discussions with vendors and subservice organization(s).
- Making regular site visits to the vendor and subservice organization(s) facilities.
- Testing controls performed by vendors and subservice organization(s).
- Reviewing attestation reports over services provided by vendors and subservice organization(s).
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations.

Complementary User Entity Controls

IronWifi's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to IronWifi's services to be solely achieved by IronWifi's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of IronWifi.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to IronWifi.
2. User entities are responsible for notifying IronWifi of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own network infrastructure, including access points, switches, and controllers that connect to the IronWifi RADIUS service.
4. User entities are responsible for ensuring the supervision, management, and control of the use of IronWifi services by their personnel.
5. User entities are responsible for properly configuring their network equipment to communicate with IronWifi RADIUS servers using secure protocols (RadSec/TLS, where supported).
6. User entities are responsible for safeguarding RADIUS shared secrets and not sharing them with unauthorized parties.
7. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize IronWifi services.
8. User entities are responsible for immediately notifying IronWifi of any actual or suspected information security breaches, including compromised user accounts or RADIUS shared secrets.
9. User entities are responsible for managing the lifecycle of user accounts and promptly deprovisioning access for terminated employees within their IronWifi-authenticated networks.