Security Best Practices

Robust Protection for Your EdgeSense.io IoT Environment

At EdgeSense.io, security is woven into the core of our platform—from device-level firmware to cloud-level services. This document outlines best practices, compliance protocols, and implementation strategies to ensure your data, devices, and infrastructure remain secure.

---

1. Security Best Practices

1.1. Device Authentication

- **All devices must authenticate using secure credentials (e.g., token or X.509 certificates).**
- **Each device should have a unique identity (Device ID or Serial Key).**

1.2. Encrypted Communication

- **MQTT over TLS (MQTTS): All telemetry and command data must be encrypted using TLS 1.2+.**
- **HTTPS API Access: REST API endpoints are accessible only via HTTPS to ensure end-to-end encryption.**

1.3. Data Integrity & Confidentiality

- **Payloads sent from devices are signed with HMAC SHA-256.**
- **Data at rest is encrypted using AES-256 encryption.**

1.4. Role-Based Access Control (RBAC)

- **Users should be assigned roles with limited permissions.**
- **Admin access should be restricted to authorized personnel only.**

1.5. Audit Trails & Logging

- **Every activity in the system is logged.**
- **Log files are stored securely and retained per compliance policies (e.g., 90 days or more).**

1.6. Device Command Authorization

- **Write/command APIs require signed requests from trusted applications.**
- **Web-based dashboards and mobile apps use token-based access (JWT with expiration).**

---

2. Compliance Standards

2.1. ISO/IEC 27001

- **Our infrastructure and processes are aligned with ISO/IEC 27001 for Information Security Management.**

2.2. GDPR (EU)

- **User and device data privacy policies are compliant with GDPR.**
- **All personal data can be exported or deleted upon request.**

2.3. SOC 2 (Type I & II) – Optional Integration

- **For enterprise clients, SOC 2-compliant hosting and operations are available on request.**

2.4. HIPAA (US) – Optional for Healthcare Use-Cases

- **HIPAA-compliant infrastructure available for specific medical device use-cases.**
- **Supports PHI encryption and access logs.**

---

3. Platform-Level Security Measures

Layer	Security Measures
Device Layer	TLS 1.2+, Secure Boot, Firmware Signing, Auth Token
Network Layer	VPN, Private Subnets, Firewalls, IP Whitelisting
Application	HTTPS, Rate Limiting, Input Validation, CSRF/XSS Protection
Data Layer	AES-256 at rest, HMAC-SHA256 in transit, DB access controls
Infrastructure	DDoS Mitigation, Geo-Redundancy, Disaster Recovery Plan

---

4. User & Admin Security Recommendations

Use Strong Passwords & MFA

- **Enforce minimum password length (12+ characters).**
- **Enable Multi-Factor Authentication (MFA) for all admin users.**

Token Expiry and Rotation

- **JWT and access tokens should have a short TTL.**
- **Support automatic token revocation and refresh.**

Inactivity Timeout

- **Automatic logout after inactivity (configurable; e.g., 15 minutes).**

Regular Penetration Testing

- **Run annual or quarterly security audits and vulnerability scans.**
- **Fix CVEs promptly across infrastructure and SDKs.**

---

5. Data Privacy and Retention Policy

Data Type	Retention Period	Encryption	Deletion Upon Request
Device Telemetry	90 days (default)	AES-256	Yes
User Information	As long as account is active	AES-256	Yes
Logs & Activity	90–180 days	AES-256	Yes

Custom retention policies are available for enterprise plans.

---

6. Disaster Recovery & Business Continuity

- **Daily backups with redundancy across regions.**
- **RPO: ≤ 5 minutes | RTO: ≤ 30 minutes.**
- **Systems are load-balanced and auto-scaled to handle failover.**

---

7. Secure Your Ecosystem

Security is a shared responsibility.

- **Integrators & OEMs: Must validate firmware and enforce access controls.**
- **End Users: Should follow password hygiene and use secure browsers/apps.**
- **Third-Party Integrators: Should use signed tokens and secure endpoints only.**

Contact us for any query at :

Email : support@edgesense.io