Compliance Guide

Ensuring Industry Standards & Certifications for Edgesense.io

Introduction

This guide outlines the key compliance requirements relevant to our hardware (IoT gateways) and software (dashboards, APIs, cloud infrastructure) and provides actionable steps to meet them.

---

1. General Compliance Frameworks

ISO/IEC 27001 – Information Security Management

- **What it covers:** A systematic approach to managing sensitive company and customer information to keep it secure.
- **Relevance:** Applies to all data processing within Edgesense's cloud dashboards and APIs.
- **Actionable Steps:**
    - Conduct risk assessments and document mitigations.
    - Implement access control, encryption, and auditing policies.
    - Ensure employee awareness training and incident response plans.

ISO/IEC 27701 – Privacy Information Management

- **What it covers:** Extension of ISO 27001 focused on data privacy.
- **Relevance:** Important for customers subject to GDPR or similar laws.
- **Actionable Steps:**
    - Map personal data collection and processing.
    - Implement data minimization and retention controls.
    - Enable data subject rights like access and deletion.

SOC 2 Type II – Service Organization Control

- **What it covers:** Trust service principles—Security, Availability, Processing Integrity, Confidentiality, and Privacy.

- **Relevance:** Essential for SaaS components like our IoT Dashboard platform.
- **Actionable Steps:**
    - Deploy internal controls over operations and system access.
    - Audit event logs, system uptime, and access privileges.
    - Engage a third-party auditor for annual assessments.

---

2. IoT-Specific Standards

IEC 62443 – Industrial Network and System Security

- **What it covers:** Cybersecurity for Industrial Automation and Control Systems (IACS).
- **Relevance:** Directly applicable to our EdgeNode IoT Gateways.
- **Actionable Steps:**
    - Secure bootloaders and firmware integrity.
    - Enforce device identity and access control.
    - Harden physical ports and OTA update mechanisms.

GSMA IoT Security Guidelines

- **What it covers:** End-to-end security recommendations for IoT products.
- **Relevance:** Good-practice baseline for both device and cloud components.
- **Actionable Steps:**
    - Device authentication and mutual TLS.
    - Secure credential storage in hardware.
    - Encrypted telemetry using MQTT/TLS.

NIST Cybersecurity Framework

- **What it covers:** Five pillars—Identify, Protect, Detect, Respond, Recover.
- **Relevance:** Widely adopted in the US and helpful for risk-based planning.
- **Actionable Steps:**
    - Maintain an asset inventory of devices and gateways.

- Build a log monitoring and anomaly detection system.
- Conduct regular penetration testing and incident simulations.

---

3. Cloud & Data Compliance

GDPR (General Data Protection Regulation)

- **What it covers:** Protection of personal data for EU residents.
- **Relevance:** Required if any customer, factory, or team member is based in the EU.
- **Actionable Steps:**
  - Provide consent-based data collection.
  - Allow data export and deletion for users.
  - Host data in GDPR-compliant cloud regions.

India Digital Personal Data Protection Act (DPDP, 2023)

- **What it covers:** India's personal data protection law.
- **Relevance:** Mandatory for Indian industrial clients using the platform.
- **Actionable Steps:**
  - Notify users of data collection and use purpose.
  - Appoint a data protection officer (DPO) if handling sensitive data.
  - Maintain an audit trail for data transfers.

HIPAA (Health Insurance Portability and Accountability Act)

- **What it covers:** Health data protection (if applicable).
- **Relevance:** Needed if EdgeNode devices or dashboards are deployed in smart hospitals or healthcare-focused plants.
- **Actionable Steps:**
  - Encrypt Protected Health Information (PHI) at rest and in transit.
  - Use role-based access control for dashboards.
  - Ensure auditability of every data access or modification.

---

4. Device Certifications

CE Marking (Europe)

- **Requirement:** Ensures the product meets EU safety, health, and environmental protection standards.
- **Applies to:** EdgeNode gateways shipped to Europe.
- **Steps:**
    - Test against applicable EN directives (EMC, RoHS, LVD).
    - Maintain Declaration of Conformity and Technical Documentation.

FCC Certification (USA)

- **Requirement:** Ensures radiofrequency compliance.
- **Applies to:** Any wireless IoT gateway sold in the U.S.
- **Steps:**
    - Perform EMC testing in accredited labs.
    - Label devices and maintain compliance documents.

BIS Certification (India)

- **Requirement:** Compulsory registration for certain electronic products.
- **Applies to:** Gateways with embedded modules sold in India.
- **Steps:**
    - Ensure components (e.g., power adapters) are BIS-approved.
    - Submit product details to BIS-approved test labs.

---

5. Sustainability & Green Compliance

RoHS (Restriction of Hazardous Substances)

- **What it covers:** Limits usage of specific hazardous materials in electrical products.
- **Applies to:** All IoT hardware produced or sold globally.

- **Steps:**
    - Source RoHS-compliant components.
    - Maintain supplier declarations and materials testing.

WEEE (Waste Electrical and Electronic Equipment Directive)

- **What it covers:** Proper disposal and recycling of electronic devices.
- **Relevance:** Required for environmental compliance in Europe.
- **Steps:**
    - Provide return/recycling options.
    - Label products with crossed-out wheeled bin symbol.

Conclusion

Edgesense.io is committed to full compliance with international and local regulations to ensure secure, ethical, and reliable industrial IoT deployments. This guide should be used by your engineering, compliance, and operations teams to:

- Track certifications
- Implement secure systems
- Maintain audit readiness

Achieving and maintaining compliance is a continuous process and part of our long-term commitment to customer trust and product excellence.

Contact us for any query at :

Email : support@edgesense.io