SMART SENSOR DEPLOYMENT GUIDELINES

Summit Digital Solutions, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

Classification: Confidential

1. PURPOSE AND SCOPE

1. These Smart Sensor Deployment Guidelines ("Guidelines") establish the mandatory procedures and requirements for the deployment, configuration, and maintenance of Internet of Things ("IoT") sensors as part of Summit Digital Solutions, Inc.'s ("Company") Peak Performance Platform implementation.

2. These Guidelines apply to all Company employees, contractors, and authorized third parties involved in sensor deployment activities for client engagements.

2. DEFINITIONS

1. "Smart Sensor" means any IoT-enabled device deployed as part of the Company's solution stack that collects, processes, or transmits data.

2. "Deployment Zone" refers to the designated physical or virtual space where Smart Sensors are installed and operated.

3. "Security Perimeter" means the defined boundary within which Smart Sensors operate and communicate with the Peak Performance Platform.

3. DEPLOYMENT REQUIREMENTS

1. Pre-Deployment Assessment

a) Conduct site survey and RF interference analysis

b) Document existing network infrastructure

c) Verify power availability and requirements

d) Assess environmental conditions

e) Identify potential security vulnerabilities

2. Physical Installation

a) Follow manufacturer specifications for mounting and positioning

b) Maintain minimum separation distances between sensors

c) Install protective enclosures where required

d) Label all sensors with unique identifiers

e) Document exact installation locations and configurations

3. Network Configuration

a) Configure sensors according to Company security standards

b) Implement approved encryption protocols

c) Establish secure communication channels

d) Verify network connectivity and signal strength

e) Test failover and redundancy systems

4. SECURITY PROTOCOLS

1. All Smart Sensors must implement:

a) AES-256 encryption for data transmission

b) Unique device certificates

c) Secure boot mechanisms

d) Automated security updates

e) Intrusion detection capabilities

2. Access Control

a) Multi-factor authentication for administrative access

b) Role-based access control

c) Audit logging of all configuration changes

d) Regular access review and revocation

5. DATA MANAGEMENT

1. Data Collection

a) Collect only data specified in client agreement

b) Apply data minimization principles

c) Implement data retention policies

d) Maintain data quality standards

2. Data Transmission

a) Use secure protocols for all data transmission

b) Implement data compression where appropriate

c) Monitor transmission latency

d) Maintain backup communication channels

6. MAINTENANCE AND MONITORING

1. Regular Maintenance

a) Quarterly physical inspection

b) Monthly firmware updates

c) Battery replacement schedule

d) Calibration verification

e) Performance optimization

2. Monitoring Requirements

a) 24/7 automated monitoring

b) Real-time alert system

c) Performance metrics tracking

d) Anomaly detection

e) Capacity planning

7. COMPLIANCE AND DOCUMENTATION

1. Maintain records of:

a) Deployment configurations

b) Security assessments

c) Maintenance activities

d) Incident reports

e) Compliance audits

2. Review and update documentation:

a) Quarterly procedure review

b) Annual policy updates

c) Change management logs

d) Training materials

8. INCIDENT RESPONSE

1. In the event of sensor failure or security breach:

a) Implement immediate containment measures

b) Notify designated response team

c) Document incident details

d) Execute recovery procedures

e) Conduct post-incident analysis

9. DISCLAIMER AND LIMITATIONS

1. These Guidelines are confidential and proprietary to Summit Digital Solutions, Inc.

2. The Company reserves the right to modify these Guidelines at any time.

3. Compliance with these Guidelines does not guarantee against all potential risks or failures.

10. EXECUTION AND APPROVAL

APPROVED AND ADOPTED by Summit Digital Solutions, Inc.

By:

Dr. Alexandra Reeves

Chief Executive Officer

Date: _

By:

Michael Chang

Chief Technology Officer

Date: _