

IoT Device Management Protocol

Summit Digital Solutions, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

Internal Reference: SDS-IDMP-2024-01

1. Purpose and Scope

1. This IoT Device Management Protocol ("Protocol") establishes the governing framework for the deployment, management, and security of Internet of Things ("IoT") devices within Summit Digital Solutions, Inc.'s ("Company") Peak Performance Platform(TM) and related service offerings.
2. This Protocol applies to all IoT devices, sensors, and connected endpoints ("Devices") deployed by the Company in client environments or utilized within Company operations.

2. Definitions

1. "Authorized Device" means any IoT device registered in the Company's device management system and approved for deployment under this Protocol.
2. "Device Credentials" means the unique identifiers, certificates, and authentication tokens assigned to each Authorized Device.
3. "Management Platform" refers to the Company's proprietary IoT device management infrastructure within the Peak Performance Platform(TM).

3. Device Registration and Onboarding

1. All Devices must undergo the following registration process:
 - a) Hardware verification against approved device registry
 - b) Security baseline assessment
 - c) Firmware validation and update
 - d) Assignment of unique Device Credentials
 - e) Integration with Management Platform
2. Device registration must be performed by authorized Company personnel with appropriate system

access rights.

4. Security Requirements

1. Each Device shall maintain:
 - a) Encrypted communication channels using TLS 1.3 or higher
 - b) Unique device certificates with automatic rotation
 - c) Secure boot mechanisms
 - d) Tamper detection capabilities
 - e) Regular security patches and updates
2. The Management Platform shall enforce:
 - a) Zero-trust network architecture
 - b) Role-based access control
 - c) Real-time device monitoring
 - d) Automated threat detection and response
 - e) Comprehensive audit logging

5. Data Management

1. Device data collection and transmission shall comply with:
 - a) Client data governance requirements
 - b) Applicable privacy regulations
 - c) Company data retention policies
 - d) Industry-specific compliance standards
2. Data storage and processing shall implement:
 - a) End-to-end encryption
 - b) Secure key management
 - c) Data segregation by client
 - d) Backup and recovery procedures

6. Operational Requirements

1. Device Monitoring

- Continuous health monitoring
- Performance metrics collection
- Automated alerting system
- Predictive maintenance scheduling

2. Updates and Maintenance

- Scheduled firmware updates
- Security patch deployment
- Configuration management
- Version control

7. Incident Response

1. Security Incidents

- Immediate device isolation
- Incident classification and escalation
- Root cause analysis
- Client notification procedures
- Remediation tracking

2. Performance Issues

- Automated diagnostics
- Performance optimization
- Issue resolution tracking
- Client impact assessment

8. Compliance and Audit

1. Regular compliance assessments shall verify:

- Security controls effectiveness
- Policy adherence
- Risk management practices
- Documentation completeness

2. Annual audits shall examine:

- Device inventory accuracy
- Security incident records
- Performance metrics
- Policy implementation

9. Protocol Updates

1. This Protocol shall be reviewed and updated annually or upon:

- Significant technology changes
- New security threats
- Regulatory requirements
- Client requirements

10. Disclaimer and Limitation of Liability

1. This Protocol is confidential and proprietary to Summit Digital Solutions, Inc.

2. The Company reserves the right to modify this Protocol at any time to maintain security and operational effectiveness.

3. Nothing in this Protocol shall create any warranty or guarantee beyond those explicitly stated in applicable client agreements.

Execution

IN WITNESS WHEREOF, this Protocol is executed by authorized representatives of Summit Digital Solutions, Inc.

Approved by:

Dr. Alexandra Reeves

Chief Executive Officer

Summit Digital Solutions, Inc.

Michael Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

Date: January 15, 2024