DATA ENCRYPTION STANDARDS AND PROTOCOLS

Summit Digital Solutions, Inc.

Effective Date: January 9, 2024

Document Version: 2.4

Classification: Confidential

1. PURPOSE AND SCOPE

1. This document establishes the mandatory encryption standards and protocols for Summit Digital Solutions, Inc. ("Company") to ensure the security and integrity of client data, proprietary information, and system communications across the Peak Performance Platform and related digital transformation solutions.

2. These standards apply to all Company employees, contractors, systems, and third-party integrators accessing or processing Company or client data.

2. DEFINITIONS

1. "Encryption" means the process of encoding information using cryptographic algorithms to prevent unauthorized access.

2. "Peak Performance Platform" refers to the Company's proprietary digital transformation platform incorporating AI, ML, and IoT capabilities.

3. "Sensitive Data" includes but is not limited to client proprietary information, personal data, authentication credentials, and system configuration data.

3. DATA ENCRYPTION REQUIREMENTS

1. Data at Rest

- All sensitive data stored in Company systems must use AES-256 encryption
- Database encryption using transparent data encryption (TDE)
- File-level encryption for documents containing sensitive information
- Hardware Security Module (HSM) integration for key management

2. Data in Transit

- TLS 1.3 or higher for all external communications
- IPSec VPN with AES-256 for inter-facility data transfer
- End-to-end encryption for all API communications
- Secure FTP with explicit TLS for file transfers

3. Key Management

- Minimum 2048-bit RSA key pairs for asymmetric encryption
- Key rotation every 90 days for symmetric keys
- Hardware-based key storage using FIPS 140-2 Level 3 certified devices
- Separate key hierarchies for development, staging, and production environments

4. PLATFORM-SPECIFIC PROTOCOLS

1. Peak Performance Platform

- Dedicated encryption for IoT sensor data streams
- Real-time encryption of ML model inputs and outputs
- Secure enclave implementation for AI processing
- Encrypted configuration management system

2. Client Integration Requirements

- Mandatory encryption handshake protocols
- Client-specific key management policies
- Encrypted backup and disaster recovery systems
- Secure key exchange mechanisms

5. COMPLIANCE AND MONITORING

1. Audit Requirements

- Quarterly encryption compliance audits
- Continuous monitoring of encryption performance
- Annual third-party security assessment
- Regular penetration testing of encryption systems

2. Documentation

- Maintenance of encryption key inventories
- Documentation of all encryption exceptions
- Regular updates to encryption standards
- Incident response procedures for encryption failures

6. ROLES AND RESPONSIBILITIES

1. Chief Technology Officer

- Overall responsibility for encryption standards
- Approval of encryption exceptions
- Strategic direction for encryption technologies

2. Security Team

- Implementation of encryption controls
- Key management operations
- Monitoring and reporting
- Incident response coordination

7. ENFORCEMENT AND EXCEPTIONS

1. Non-compliance with these standards may result in disciplinary action up to and including termination of employment or service agreements.

2. Exceptions to these standards must be:

- Documented in writing
- Approved by the CTO and Security Team
- Reviewed quarterly
- Time-limited with specific expiration dates

8. REVIEW AND UPDATES

1. This document shall be reviewed and updated annually or upon significant changes to:

- Regulatory requirements
- Industry standards
- Technology capabilities

- Business requirements

9. LEGAL DISCLAIMER

The information contained in this document is confidential and proprietary to Summit Digital Solutions, Inc. This document may not be reproduced, distributed, or transmitted in any form without express written permission from the Company. The Company reserves the right to modify these standards at any time without notice.

10. APPROVAL AND EXECUTION

APPROVED AND ADOPTED by the undersigned, effective as of the date first written above.

SUMMIT DIGITAL SOLUTIONS, INC.

By:

Name: Michael Chang

Title: Chief Technology Officer

By:

Name: James Henderson

Title: Chief Digital Officer