SECURITY COMPLIANCE FRAMEWORK

Summit Digital Solutions, Inc.

Last Updated: January 9, 2024

Document Version: 3.2

1. INTRODUCTION

1 This Security Compliance Framework ("Framework") establishes the comprehensive security controls, protocols, and compliance requirements governing Summit Digital Solutions, Inc.'s ("Company") technology infrastructure, data handling practices, and service delivery operations.

2 This Framework applies to all Company employees, contractors, systems, and third-party vendors involved in the development, deployment, or maintenance of the Peak Performance Platform and related digital transformation services.

2. DEFINITIONS

1 "Controlled Data" means any customer data, proprietary information, or regulated data processed through Company systems.

2 "Critical Infrastructure" means the core technology components supporting the Peak Performance Platform, including AI/ML models, IoT gateways, and analytics engines.

3 "Security Event" means any actual or suspected unauthorized access, disclosure, or compromise of Company systems or Controlled Data.

3. SECURITY CONTROL REQUIREMENTS

1 Access Control and Authentication

- Multi-factor authentication required for all system access
- Role-based access control (RBAC) implementation
- Quarterly access review and certification
- Privileged account management protocols
- Automatic session timeout after 15 minutes of inactivity

2 Data Protection

- AES-256 encryption for data at rest
- TLS 1.3 for data in transit
- Regular key rotation and management
- Data classification and handling procedures
- Secure backup and recovery protocols

3 Network Security

- Network segmentation and microsegmentation
- Next-generation firewall deployment
- Intrusion detection/prevention systems
- Regular vulnerability scanning
- Quarterly penetration testing

4. COMPLIANCE OBLIGATIONS

1 Regulatory Requirements

- SOC 2 Type II certification maintenance
- ISO 27001 compliance
- GDPR compliance for EU customer data
- CCPA compliance for California residents
- Industry-specific requirements as applicable

2 Audit and Assessment

- Annual third-party security assessments
- Quarterly internal security reviews
- Continuous compliance monitoring
- Documentation of all audit findings
- Remediation tracking and verification

5. INCIDENT RESPONSE

1 Security Event Management

- 24/7 security operations center
- Documented incident response procedures

- Maximum 1-hour initial response time
- Customer notification within 72 hours
- Post-incident analysis and reporting

2 Business Continuity

- Recovery Time Objective (RTO): 4 hours
- Recovery Point Objective (RPO): 15 minutes
- Regular disaster recovery testing
- Alternate processing facilities
- Crisis management procedures

6. VENDOR MANAGEMENT

1 Third-Party Requirements

- Security assessment prior to engagement
- Annual security reviews
- Contractual security obligations
- Monitoring of vendor compliance
- Right to audit provisions

2 Technology Integration

- Secure API implementation
- Vendor access restrictions
- Integration security testing
- Continuous monitoring
- Regular security reviews

7. TRAINING AND AWARENESS

1 Security Training Program

- Mandatory new hire security training
- Annual security awareness refresher
- Role-specific security training
- Phishing simulation exercises

- Compliance training documentation

8. ENFORCEMENT AND UPDATES

1 This Framework shall be reviewed and updated annually or upon significant changes to the technology environment or regulatory requirements.

2 Violations of this Framework may result in disciplinary action up to and including termination of employment or vendor relationships.

9. APPROVAL AND EXECUTION

IN WITNESS WHEREOF, this Security Compliance Framework has been approved and adopted by the authorized representatives of Summit Digital Solutions, Inc.

SUMMIT DIGITAL SOLUTIONS, INC.

By:

Name: Michael Chang

Title: Chief Technology Officer

Date: January 9, 2024

By:

Name: James Henderson

Title: Chief Digital Officer

Date: January 9, 2024

10. DISCLAIMER

This document contains confidential and proprietary information of Summit Digital Solutions, Inc. Unauthorized disclosure, reproduction, or use is strictly prohibited. All rights reserved.