API SECURITY STANDARDS MANUAL

Summit Digital Solutions, Inc.

Version 2.4 - Last Updated: January 9, 2024

Document Classification: CONFIDENTIAL

1. INTRODUCTION

1. This API Security Standards Manual ("Manual") establishes mandatory security requirements and protocols for all Application Programming Interfaces ("APIs") developed, maintained, or utilized by Summit Digital Solutions, Inc. ("Company") in connection with its Peak Performance Platform and related digital transformation services.

2. This Manual is binding upon all employees, contractors, and third-party integrators accessing or developing Company APIs.

2. DEFINITIONS

1. "API" means any application programming interface that enables interaction with Company systems, including REST APIs, GraphQL endpoints, and WebSocket connections.

2. "Authentication Credentials" means any tokens, keys, certificates, or other access control mechanisms.

3. "Security Event" means any unauthorized access, breach, or attempted compromise of API security controls.

3. API DEVELOPMENT STANDARDS

1. Authentication Requirements

- All APIs must implement OAuth 2.0 or JWT-based authentication
- API keys must be encrypted using AES-256 encryption at rest
- Multi-factor authentication required for administrative access
- Token expiration not to exceed 12 hours for standard access

2. Authorization Controls

- Role-based access control (RBAC) implementation mandatory

- Granular permission sets defined per API endpoint
- Regular audit of authorization matrices
- Principle of least privilege strictly enforced

3. Data Encryption

- TLS 1.3 required for all API communications
- End-to-end encryption for sensitive data transmission
- Field-level encryption for PII and regulated data
- Key rotation every 90 days minimum

4. SECURITY MONITORING AND TESTING

1. Automated Security Scanning

- Daily vulnerability scanning of API endpoints
- Weekly penetration testing of new API deployments
- Monthly security assessment of API documentation
- Quarterly third-party security audits

2. Rate Limiting and Throttling

- Implementation of rate limiting per API key
- Automatic blocking of suspicious traffic patterns
- DDoS protection mechanisms required
- Circuit breaker implementation for cascade failure prevention

5. INCIDENT RESPONSE

1. Security Event Handling

- Immediate notification to Security Operations Center
- Automated threat containment procedures
- Incident documentation and root cause analysis
- Client notification within 24 hours of confirmed breach

2. Recovery Procedures

- API version rollback capabilities

- Backup authentication system activation
- Traffic rerouting protocols
- Service restoration prioritization

6. COMPLIANCE AND DOCUMENTATION

1. Required Documentation

- API specifications in OpenAPI 3.0 format
- Security control documentation
- Integration testing procedures
- Threat modeling documentation

2. Compliance Requirements

- Annual SOC 2 Type II certification
- GDPR compliance for EU data handling
- CCPA compliance for California residents
- Industry-specific regulatory compliance as applicable

7. THIRD-PARTY INTEGRATION REQUIREMENTS

1. Integration Standards

- Mandatory security assessment before integration
- Signed API usage agreements required
- Regular security compliance verification
- Integration testing in sandbox environment

2. Partner Obligations

- Regular security status reporting
- Immediate notification of security events
- Compliance with Company security policies
- Annual security review participation

8. ENFORCEMENT AND UPDATES

1. This Manual shall be reviewed and updated quarterly by the Company's Security Committee.

2. Violations of this Manual may result in immediate API access termination and other remedies available to the Company.

9. LEGAL DISCLAIMER

This Manual is confidential and proprietary to Summit Digital Solutions, Inc. Unauthorized distribution or reproduction is strictly prohibited. The Company reserves the right to modify this Manual at any time without prior notice.

ACKNOWLEDGMENT

The undersigned acknowledges receipt and understanding of this API Security Standards Manual:

```

**Name: _**

**Title: _**

**Date: _**

**Signature: _**

```

Document Control

- Document ID: API-SEC-2.4-2024
- Approved By: Michael Chang, CTO
- Effective Date: January 9, 2024
- Next Review: April 9, 2024