Platform Security Controls & Access Management Framework

Summit Digital Solutions, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Classification: Confidential

1. Purpose and Scope

1. This Platform Security Controls & Access Management Framework ("Framework") establishes the governing principles, requirements, and procedures for securing Summit Digital Solutions' Peak Performance Platform ("Platform") and managing access controls across all integrated systems and data environments.

2. This Framework applies to all Platform components, including but not limited to:

a) Core analytics engine

b) Machine learning modules

c) IoT integration layers

d) Client-facing interfaces

e) Administrative control systems

f) Data storage environments

2. Definitions

1. "Access Control" means the selective restriction of access to Platform resources.

2. "Authentication Credentials" means unique identifiers, passwords, tokens, certificates, or other mechanisms used to verify identity.

3. "Security Event" means any observable occurrence in a system or network indicating a potential breach of security policy or failure of safeguards.

4. "Privileged Access" means elevated system permissions exceeding standard user rights.

3. Security Architecture

1. The Platform shall implement a defense-in-depth security architecture incorporating:

a) Multi-layer perimeter security

b) Network segmentation

c) Encryption at rest and in transit

d) Application-level security controls

e) Identity and access management

f) Security monitoring and logging

2. All Platform components must maintain SOC 2 Type II compliance and adhere to ISO 27001 standards.

4. Access Control Requirements

1. Authentication Standards

a) Multi-factor authentication required for all user access

b) Minimum password length of 12 characters

c) Password complexity requirements enforced

d) Maximum password age of 90 days

e) Password history of 24 previous passwords

2. Authorization Controls

a) Role-based access control (RBAC) implementation

b) Principle of least privilege enforcement

c) Separation of duties for administrative functions

d) Regular access review and certification

e) Automated access termination processes

5. Security Monitoring and Incident Response

1. Continuous Monitoring

a) 24/7 security operations center

b) Real-time threat detection

c) Automated alert generation

d) Security information and event management (SIEM)

e) Behavioral analytics

2. Incident Response Procedures

a) Defined incident classification matrix

b) Escalation procedures

c) Communication protocols

d) Investigation requirements

e) Documentation standards

6. Compliance and Audit

1. Regular security assessments including:

a) Quarterly vulnerability scanning

b) Annual penetration testing

c) Third-party security audits

d) Compliance validation

e) Control effectiveness testing

2. Documentation Requirements

a) Security policies and procedures

b) System configuration standards

c) Change management records

d) Incident response plans

e) Audit trails and logs

7. Data Protection

1. Data Classification

a) Confidential

b) Internal Use Only

c) Public

2. Data Security Controls

a) Encryption requirements

b) Access restrictions

c) Data retention periods

d) Secure disposal procedures

e) Data loss prevention

8. Maintenance and Review

1. This Framework shall be reviewed and updated annually or upon significant Platform changes.

2. All updates require approval from:

a) Chief Technology Officer

b) Chief Information Security Officer

c) Chief Digital Officer

d) Legal Department

9. Legal Compliance

1. This Framework is designed to ensure compliance with applicable laws and regulations including:

a) GDPR

b) CCPA

c) HIPAA (where applicable)

d) Industry-specific regulations

10. Disclaimer and Proprietary Rights

1. This Framework contains confidential and proprietary information of Summit Digital Solutions, Inc. and is protected under applicable intellectual property laws.

2. No part of this Framework may be reproduced, transmitted, or distributed without prior written authorization from Summit Digital Solutions, Inc.

Execution

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

Michael Chang

Chief Technology Officer

Date: January 15, 2024

James Henderson

Chief Digital Officer

Date: January 15, 2024