NETWORK SECURITY ARCHITECTURE DOCUMENT

Summit Digital Solutions, Inc.

Document Version: 2.4

Last Updated: January 9, 2024

Classification: CONFIDENTIAL

1. INTRODUCTION

1. This Network Security Architecture Document ("Architecture Document") sets forth the comprehensive network security infrastructure and protocols implemented by Summit Digital Solutions, Inc. ("Company") in connection with its Peak Performance Platform and related digital transformation services.

2. This document is considered confidential and proprietary information of the Company and is subject to the terms of any applicable Non-Disclosure Agreement.

2. NETWORK ARCHITECTURE OVERVIEW

1. **Core Infrastructure**

- Multi-layered network architecture utilizing redundant Cisco Nexus 9000 Series switches
- Segmented network zones with dedicated firewalls for Production, Development, and Management
- Geographic distribution across three primary data centers (US-East, US-West, EU-Central)
- Software-defined networking (SDN) implementation using Cisco ACI

2. **Security Zones**

- DMZ for external-facing services
- Restricted zone for client data processing
- Highly restricted zone for AI/ML operations
- Management zone for administrative access
- Development zone for R&D activities

3. SECURITY CONTROLS AND PROTOCOLS

1. **Access Control**

- Multi-factor authentication (MFA) required for all network access
- Role-based access control (RBAC) implemented through Microsoft Active Directory
- Privileged Access Management (PAM) system for administrative credentials
- Regular access reviews conducted quarterly

2. **Network Security**

- Next-generation firewalls with IPS/IDS capabilities
- Network segmentation using VLANs and microsegmentation
- Encrypted VPN access for remote connectivity
- DDoS protection through Cloudflare Enterprise

3. **Data Protection**

- End-to-end encryption for data in transit (TLS 1.3)
- At-rest encryption using AES-256
- Data classification and handling procedures
- Regular backup and disaster recovery testing

4. COMPLIANCE AND MONITORING

1. **Security Monitoring**

- 24/7 Security Operations Center (SOC)
- SIEM implementation using Splunk Enterprise
- Network behavior analytics
- Automated threat detection and response

2. **Compliance Framework**

- ISO 27001:2013 certified
- SOC 2 Type II compliant
- GDPR and CCPA compliant
- Regular third-party security assessments

5. INCIDENT RESPONSE AND RECOVERY

1. **Incident Response Plan**

- Documented procedures for security incidents
- Defined escalation paths and response teams
- Regular incident response drills
- Post-incident analysis and reporting

2. **Business Continuity**

- Recovery Time Objective (RTO): 4 hours
- Recovery Point Objective (RPO): 15 minutes
- Redundant systems and failover capabilities
- Regular disaster recovery testing

6. MAINTENANCE AND UPDATES

1. **Patch Management**

- Automated patch deployment system
- Critical security updates within 24 hours
- Regular vulnerability scanning
- Change management procedures

2. **Architecture Review**

- Quarterly security architecture reviews
- Annual third-party security assessments
- Continuous improvement program
- Technology refresh cycle: 3 years

7. PROPRIETARY SYSTEMS

1. **Peak Performance Platform Security**

- Dedicated security infrastructure for AI/ML operations
- Proprietary encryption for client data processing
- Secure API gateway implementation
- Custom security controls for IoT device integration

8. DISCLAIMERS AND LIMITATIONS

1. This Architecture Document represents the current security infrastructure as of the date specified above. The Company reserves the right to modify any aspect of the security architecture without notice as required to maintain security effectiveness.

2. This document does not guarantee complete security or freedom from breaches but represents the Company's best efforts to implement industry-standard security measures.

9. DOCUMENT CONTROL

1. This document is maintained by the Chief Information Security Officer and reviewed quarterly by the Security Architecture Review Board.

2. Distribution of this document is restricted to authorized personnel only and subject to appropriate non-disclosure agreements.

EXECUTION

IN WITNESS WHEREOF, the undersigned acknowledges the accuracy and completeness of this Network Security Architecture Document 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