# ZERO TRUST SECURITY ARCHITECTURE

**Summit Digital Solutions, Inc.**

*Document Version: 2.4*

*Effective Date: January 9, 2024*

*Classification: Confidential*

## 1. INTRODUCTION AND SCOPE

1. This Zero Trust Security Architecture document ("Architecture") establishes the framework and requirements for implementing and maintaining Summit Digital Solutions, Inc.'s ("Company") zero trust security model across all technology infrastructure, applications, and services.

2. This Architecture applies to all Company systems, networks, applications, and data, including the Peak Performance Platform and associated enterprise solutions.

## 2. DEFINITIONS

1. "Zero Trust" means a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

2. "Least Privilege Access" means providing users with the minimum levels of access - or permissions - needed to perform their work functions.

3. "Micro-segmentation" means the practice of dividing security perimeters into small zones to maintain separate access for separate parts of the network.

## 3. ARCHITECTURAL PRINCIPLES

1. Core Principles

a) Never trust, always verify

b) Assume breach

c) Verify explicitly

d) Use least privilege access

e) Implement comprehensive security monitoring

2. Design Requirements

a) All resources must be accessed securely regardless of location

b) Access control is on a per-session basis

c) All data flows must be encrypted end-to-end

d) Access is determined by dynamic policy

e) All assets must be monitored and validated continuously

## 4. IMPLEMENTATION REQUIREMENTS

1. Identity and Access Management

a) Multi-factor authentication required for all access

b) Risk-based conditional access policies

c) Just-in-time and just-enough-access provisioning

d) Regular access reviews and certification

2. Network Security

a) Micro-segmentation of all network resources

b) Software-defined perimeter implementation

c) Encrypted communication between all segments

d) Real-time threat detection and response

3. Data Security

a) Data classification and handling requirements

b) Encryption at rest and in transit

c) Data loss prevention controls

d) Regular data access auditing

## 5. COMPLIANCE AND MONITORING

1. Continuous Monitoring

a) Real-time security posture assessment

b) Behavioral analytics and anomaly detection

c) Security event logging and correlation

d) Automated compliance reporting

2. Audit Requirements

a) Quarterly security architecture reviews

b) Annual third-party security assessments

c) Continuous compliance monitoring

d) Regular penetration testing

## 6. INCIDENT RESPONSE AND RECOVERY

1. Security Incident Management

a) Automated threat detection and response

b) Incident classification and escalation procedures

c) Business continuity integration

d) Post-incident analysis and reporting

2. Recovery Procedures

a) Automated system recovery processes

b) Data backup and restoration procedures

c) Business continuity plan activation

d) Stakeholder communication protocols

## 7. GOVERNANCE AND MAINTENANCE

1. The Chief Technology Officer shall be responsible for:

a) Maintaining this Architecture

b) Approving exceptions

c) Ensuring compliance

d) Reporting to executive leadership

2. Review and Updates

a) Annual architecture review

b) Quarterly security controls assessment

c) Continuous improvement process

d) Change management procedures

## 8. LEGAL AND REGULATORY COMPLIANCE

1. This Architecture shall comply with:

a) All applicable federal and state regulations

b) Industry standards and frameworks

c) Contractual obligations

d) Company security policies

## 9. DISCLAIMER AND PROPRIETARY RIGHTS

1. This document contains confidential and proprietary information of Summit Digital Solutions, Inc. All rights reserved. No part of this document may be reproduced, stored, or transmitted without prior written permission.

2. This Architecture is protected under applicable intellectual property laws and trade secret regulations.

## APPROVAL AND EXECUTION

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

APPROVED BY:

Michael Chang

Chief Technology Officer

Date: January 9, 2024

Dr. Alexandra Reeves

Chief Executive Officer

Date: January 9, 2024