CLOUD INFRASTRUCTURE SECURITY PLAYBOOK

Summit Digital Solutions, Inc.

Version 2.4 - Last Updated: January 9, 2024

Document Classification: CONFIDENTIAL

1. INTRODUCTION AND SCOPE

1. This Cloud Infrastructure Security Playbook ("Playbook") establishes mandatory security protocols and compliance requirements for all cloud infrastructure deployments supporting Summit Digital Solutions, Inc.'s ("Company") Peak Performance Platform and related digital transformation services.

2. This Playbook applies to all employees, contractors, and third-party vendors who access, manage, or maintain Company cloud infrastructure resources.

2. DEFINITIONS

1. "Cloud Infrastructure" means all Company-operated or controlled computing resources hosted on AWS, Microsoft Azure, or Google Cloud Platform, including virtual machines, containers, storage systems, and networking components.

2. "Critical Systems" refers to components of the Peak Performance Platform that process client data or support production workloads.

3. "Security Event" means any detected or suspected unauthorized access, data breach, or security incident affecting Company cloud infrastructure.

3. SECURITY ARCHITECTURE REQUIREMENTS

1. Network Segmentation

- Production environments must maintain complete logical separation from development/testing
- Implementation of virtual private clouds (VPCs) with distinct security groups
- Mandatory use of private subnets for all data processing components
- Public-facing services limited to load balancers and API gateways

2. Access Control

- Multi-factor authentication required for all administrative access
- Role-based access control (RBAC) implementing principle of least privilege
- Regular access review and certification every 90 days
- Automated deprovisioning integrated with HR systems

3. Encryption Standards

- AES-256 encryption required for all data at rest
- TLS 1.3 mandatory for all data in transit
- Key management through cloud provider native services
- Customer-managed keys required for regulated workloads

4. OPERATIONAL SECURITY CONTROLS

1. Monitoring and Logging

- Centralized log aggregation with 12-month retention
- Real-time security event monitoring and alerting
- Weekly security metrics reporting to CISO
- Automated compliance scanning and reporting

2. Change Management

- Infrastructure as Code (IaC) required for all deployments
- Peer review mandatory for all infrastructure changes
- Change freeze periods during peak business hours
- Automated rollback capabilities for failed deployments

3. Incident Response

- 15-minute SLA for Critical Security Event response
- Documented escalation procedures and contact lists
- Quarterly incident response testing and simulation
- Post-incident analysis and lessons learned documentation

5. COMPLIANCE AND AUDIT

1. Regulatory Requirements

- Annual SOC 2 Type II certification
- Quarterly penetration testing by approved vendors
- Monthly vulnerability assessments
- Compliance with GDPR, CCPA, and HIPAA as applicable

2. Documentation Requirements

- Current network architecture diagrams
- Updated asset inventory and classification
- Security controls mapping to compliance frameworks
- Vendor security assessment documentation

6. VENDOR MANAGEMENT

1. Third-party vendors must:

- Maintain equivalent security controls
- Provide security attestation documentation
- Submit to annual security assessments
- Report security incidents within 24 hours

7. ENFORCEMENT AND UPDATES

1. Compliance with this Playbook is mandatory. Violations may result in disciplinary action up to and including termination of employment or service agreements.

2. This Playbook shall be reviewed and updated annually or upon significant changes to Company infrastructure or regulatory requirements.

8. APPROVAL AND GOVERNANCE

1. The Chief Information Security Officer (CISO) is responsible for maintaining and enforcing this Playbook.

2. Material changes require approval from:

- Chief Technology Officer
- Chief Information Security Officer
- Chief Compliance Officer

- General Counsel

DOCUMENT CONTROL

Document Owner: Office of Information Security

Last Review Date: January 9, 2024

Next Review Date: January 9, 2025

Version: 2.4

APPROVED BY:

Michael Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

[NAME]

Chief Information Security Officer

Summit Digital Solutions, Inc.

Date: _