SECURITY OPERATIONS PROCEDURES

Summit Digital Solutions, Inc.

Effective Date: January 1, 2024

Document Version: 3.2

Last Updated: December 15, 2023

1. PURPOSE AND SCOPE

1. These Security Operations Procedures ("Procedures") establish the mandatory security protocols and operational safeguards for Summit Digital Solutions, Inc. ("Company") in relation to its Peak Performance Platform and associated digital transformation services.

2. These Procedures apply to all employees, contractors, consultants, temporary workers, and other personnel ("Personnel") who access Company systems, data, or facilities.

2. DEFINITIONS

1. "Critical Infrastructure" means the Company's core technology systems, including the Peak Performance Platform, IoT integration networks, and machine learning environments.

2. "Secure Areas" refers to designated locations containing Critical Infrastructure components, data centers, or sensitive client information.

3. "Security Event" means any observed or suspected security breach, unauthorized access, or compromise of Company systems or data.

3. PHYSICAL SECURITY PROTOCOLS

1. Access Control

- All Personnel must display Company-issued identification badges while on premises
- Biometric authentication required for entry to Secure Areas
- Visitor access limited to escorted guests with approved temporary credentials
- Quarterly audit of access permissions and credentials

2. Facility Security

- 24/7 video surveillance of all entry points and Secure Areas

- Environmental monitoring systems for temperature, humidity, and fire detection
- Redundant power systems with automated failover
- Monthly testing of all physical security systems

4. NETWORK SECURITY REQUIREMENTS

1. Infrastructure Protection

- Minimum AES-256 encryption for all data in transit
- Multi-factor authentication for all system access
- Segmented network architecture with defined security zones
- Real-time threat monitoring and intrusion detection

2. Remote Access Security

- VPN with split-tunnel configuration required for remote access
- Automatic session termination after 30 minutes of inactivity
- Prohibited use of public Wi-Fi for Company systems access
- Quarterly security assessment of remote access protocols

5. DATA PROTECTION AND HANDLING

1. Client Data Security

- Encryption of all client data at rest using industry-standard protocols
- Segregated storage environments for each client engagement
- Automated data classification and handling controls
- Regular backup verification and recovery testing

2. Internal Data Controls

- Role-based access control (RBAC) for all systems
- Automated logging of all data access and modifications
- Retention policies aligned with legal and contractual requirements
- Quarterly data access audits and permission reviews

6. INCIDENT RESPONSE PROCEDURES

1. Security Event Reporting

- Immediate notification to Security Operations Center for suspected events
- Mandatory incident documentation within 1 hour of discovery
- Escalation protocols based on severity classification
- Client notification procedures per contractual requirements

2. Investigation and Resolution

- Dedicated incident response team activation
- Evidence preservation and chain of custody documentation
- Root cause analysis requirements
- Post-incident review and procedure updates

7. COMPLIANCE AND AUDIT

1. Internal Compliance

- Monthly security compliance assessments
- Quarterly penetration testing of Critical Infrastructure
- Annual comprehensive security audit
- Continuous monitoring of security controls

2. External Requirements

- SOC 2 Type II compliance maintenance
- ISO 27001 certification requirements
- Industry-specific regulatory compliance
- Client-specific security requirements

8. TRAINING AND AWARENESS

1. Required Training

- Annual security awareness training for all Personnel
- Quarterly security updates and briefings
- Role-specific security training for technical staff
- Incident response simulation exercises

9. ENFORCEMENT

1. These Procedures are mandatory for all Personnel. Violations may result in disciplinary action up to and including termination of employment or service relationship.

2. The Chief Information Security Officer shall have primary responsibility for enforcement of these Procedures.

10. AMENDMENTS

1. These Procedures may be amended by the Company's Security Committee with approval from executive leadership.

2. All amendments shall be documented and communicated to Personnel within 5 business days of approval.

Approved by:

Dr. Alexandra Reeves
Chief Executive Officer

Michael Chang
Chief Technology Officer

James Henderson
Chief Digital Officer

Date: December 15, 2023