SYSTEM ACCESS CONTROL POLICY

Summit Digital Solutions, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Policy Owner: Information Security Department

1. PURPOSE AND SCOPE

1. This System Access Control Policy ("Policy") establishes the standards and procedures for securing access to Summit Digital Solutions, Inc.'s ("Company") information systems, including the Peak Performance Platform, enterprise applications, development environments, and network infrastructure.

2. This Policy applies to all employees, contractors, consultants, temporary workers, and other personnel ("Users") granted access to Company systems.

2. DEFINITIONS

1. "Access Control" means the selective restriction of access to Company systems through authentication and authorization mechanisms.

2. "Privileged Access" refers to elevated system permissions that provide capabilities beyond standard user access.

3. "Multi-Factor Authentication (MFA)" means authentication using two or more verification factors.

4. "System Administrator" refers to personnel responsible for managing and maintaining Company systems.

3. ACCESS CONTROL PRINCIPLES

1. Least Privilege

- Users shall be granted minimum access rights necessary to perform their job functions
- Access rights shall be reviewed quarterly
- Temporary elevation of privileges requires documented approval

2. Need-to-Know

- Access to sensitive data shall be granted only when required for legitimate business purposes
- All access requests must be documented and approved by appropriate management

3. Segregation of Duties

- Critical system functions shall require multiple Users for execution
- Development and production environments shall maintain strict separation

4. ACCESS AUTHORIZATION PROCEDURES

1. Request Process

- Access requests must be submitted through the Company's ServiceNow platform
- Requests must include business justification and duration
- Approvals required from immediate supervisor and system owner

2. Verification Requirements

- Identity verification required prior to access grant
- Background checks for privileged access
- Annual re-certification of access rights

3. Documentation

- All access grants must be logged in the access management system
- Audit trails maintained for minimum of 3 years
- Quarterly access review reports generated for compliance

5. AUTHENTICATION STANDARDS

1. Password Requirements

- Minimum 12 characters
- Complexity requirements enforced
- Password rotation every 90 days
- Previous 12 passwords cannot be reused

2. Multi-Factor Authentication

- Required for all remote access
- Required for privileged account access

- Hardware tokens for critical systems access

6. MONITORING AND COMPLIANCE

1. System Monitoring

- Access attempts logged and reviewed
- Automated alerts for suspicious activity
- Regular penetration testing of access controls

2. Compliance Reviews

- Quarterly access rights audits
- Annual policy compliance assessment
- Third-party security assessments

7. INCIDENT RESPONSE

1. Unauthorized Access

- Immediate access suspension upon detection
- Incident response team notification
- Investigation and documentation requirements

2. Emergency Access

- Break-glass procedures for emergency access
- Executive approval required
- Post-incident review mandatory

8. ENFORCEMENT

1. Policy violations may result in:

- Immediate access revocation
- Disciplinary action up to termination
- Legal action where applicable

9. POLICY MAINTENANCE

1. Review Schedule

- Annual policy review required
- Updates based on risk assessments
- Change management procedures apply

2. Version Control

- Policy versions maintained in document management system
- Distribution to all Users upon updates
- Acknowledgment tracking required

10. EXCEPTIONS

1. Exception Process

- Written requests required
- CISO approval mandatory
- Maximum 6-month duration
- Documentation in exception register

APPROVAL AND REVISION HISTORY

Approved by: _

James Henderson

Chief Digital Officer

Date: January 15, 2024

Previous Revision: July 1, 2023

Next Review Date: January 15, 2025

Document Control Number: SEC-POL-2024-001