CHANGE MANAGEMENT PROTOCOL v2.1

Summit Digital Solutions, Inc.

Effective Date: January 15, 2024

Document Control #: CMP-2024-001

1. PURPOSE AND SCOPE

1. This Change Management Protocol ("Protocol") establishes the mandatory procedures and controls governing all changes to Summit Digital Solutions, Inc.'s ("Company") technology infrastructure, software systems, and client-facing solutions, including but not limited to the Peak Performance Platform and associated components.

2. This Protocol applies to all employees, contractors, consultants, and third-party vendors who participate in or affect change management activities within the Company's operational environment.

2. DEFINITIONS

1. "Change" means any addition, modification, or removal of systems, software, hardware, networks, applications, environments, or processes that could affect Company or client operations.

2. "Emergency Change" means any change required to resolve a Critical Incident that poses immediate risk to business operations, security, or regulatory compliance.

3. "Change Advisory Board" or "CAB" means the designated group of technical and business stakeholders responsible for change review and approval.

3. CHANGE CLASSIFICATION

1. Standard Changes

- Level 1: Minor changes with minimal risk and impact
- Level 2: Moderate changes affecting multiple systems or users
- Level 3: Major changes with significant business impact

2. Emergency Changes

- Critical: Requiring immediate implementation
- Urgent: Requiring expedited review within 4 hours

4. CHANGE MANAGEMENT PROCEDURES

1. Change Request Submission

a) All changes must be submitted through the Company's designated Change Management System

b) Requests must include:

- Detailed description of proposed change
- Technical implementation plan
- Risk assessment and mitigation strategy
- Rollback procedures
- Testing requirements
- Business justification

2. Review and Approval Process

a) Level 1 Changes: Require technical lead approval

b) Level 2 Changes: Require CAB review and approval

c) Level 3 Changes: Require CAB and Executive Leadership approval

d) Emergency Changes: Require CTO or designated deputy approval

5. IMPLEMENTATION REQUIREMENTS

1. Pre-Implementation

a) Documented test results in non-production environment

b) Stakeholder sign-off on test results

c) Backup of affected systems

d) Communication to affected users

2. Implementation Window

a) Standard changes must be implemented during approved maintenance windows

b) Changes affecting Peak Performance Platform must be scheduled minimum 72 hours in advance

c) Client notification requirements per service level agreements

3. Post-Implementation

a) Verification of successful implementation

b) Documentation of actual vs. planned outcomes

c) Incident reporting for any issues

d) Lessons learned documentation

6. EMERGENCY CHANGE PROCEDURES

1. Emergency changes require:

a) Immediate notification to CTO and Security Team

b) Abbreviated documentation requirements

c) Post-implementation review within 24 hours

d) Root cause analysis within 72 hours

7. COMPLIANCE AND AUDIT

1. All changes must be logged and documented in accordance with:

a) SOC 2 Type II requirements

b) ISO 27001 standards

c) Client contractual obligations

d) Regulatory requirements

2. Quarterly audit of change management compliance by Internal Audit team

8. ROLES AND RESPONSIBILITIES

1. Change Advisory Board

- Chief Technology Officer (Chair)
- Chief Digital Officer
- Head of Security
- Client Success Director
- Technical Architecture Lead

2. Change Implementers

- Must maintain required certifications
- Must complete annual change management training
- Must adhere to all documentation requirements

9. AMENDMENTS AND REVIEWS

1. This Protocol shall be reviewed annually by the Technology Governance Committee.

2. Amendments require approval from:

- Chief Technology Officer
- Chief Digital Officer
- Chief Innovation Officer

10. ENFORCEMENT

1. Violations of this Protocol may result in disciplinary action up to and including termination of employment or service agreements.

2. Emergency exceptions must be documented and reviewed by the CAB within 5 business days.

Approved by:

Michael Chang
Chief Technology Officer
Date: January 15, 2024

James Henderson
Chief Digital Officer
Date: January 15, 2024

Dr. Robert Martinez
Chief Innovation Officer
Date: January 15, 2024