

# Configuration Management Database Guide

**Summit Digital Solutions, Inc.**

*Version 2.4 - Last Updated: January 9, 2024*

*Document Classification: Confidential*

## 1. Purpose and Scope

1. This Configuration Management Database ("CMDB") Guide establishes the governing framework for maintaining and operating Summit Digital Solutions, Inc.'s ("Company") enterprise-wide configuration management system, including the Peak Performance Platform and associated technology infrastructure.

2. This Guide applies to all employees, contractors, and authorized third parties who access, modify, or manage configuration items within the Company's CMDB environment.

## 2. Definitions

1. "Configuration Item" (CI): Any component requiring management control as part of the service delivery infrastructure.

2. "CMDB": The authorized system of record for all configuration items, their attributes, and relationships.

3. "Peak Performance Platform": The Company's proprietary digital transformation platform, including all associated subsystems and components.

## 3. CMDB Architecture and Components

### 1. Core Database Structure

- Primary PostgreSQL database cluster
- Redundant backup instances
- Real-time synchronization framework
- API gateway interfaces

### 2. Mandatory CI Attributes

- Unique identifier

- Classification category
- Ownership assignment
- Lifecycle status
- Security classification
- Dependencies mapping
- Version control reference

#### **4. Access Control and Security**

##### **1. Authentication Requirements**

- Multi-factor authentication mandatory for all users
- Role-based access control (RBAC) implementation
- Segregation of duties enforcement
- Audit logging of all access events

##### **2. Security Classifications**

- Level 1: Public Reference
- Level 2: Internal Use
- Level 3: Confidential
- Level 4: Restricted

#### **5. Change Management Integration**

##### **1. All modifications to Configuration Items must:**

- Follow established change management procedures
- Receive appropriate approval based on risk assessment
- Include rollback procedures
- Maintain version control integrity
- Document impact analysis

##### **2. Emergency Change Procedures**

- Defined escalation paths
- Post-implementation review requirements
- Executive notification thresholds

- Compliance documentation requirements

## **6. Data Quality and Integrity**

### **1. Mandatory Quality Controls**

- Automated validation checks
- Regular data accuracy audits
- Duplicate detection protocols
- Relationship integrity verification
- Orphaned record identification

### **2. Maintenance Requirements**

- Weekly integrity checks
- Monthly completeness audits
- Quarterly relationship validation
- Annual comprehensive review

## **7. Disaster Recovery and Business Continuity**

### **1. Backup Requirements**

- Real-time transaction logging
- Daily incremental backups
- Weekly full backups
- Monthly archive creation
- Quarterly recovery testing

### **2. Recovery Time Objectives**

- Tier 1 CIs: 4 hours
- Tier 2 CIs: 8 hours
- Tier 3 CIs: 24 hours

## **8. Compliance and Audit**

### **1. Regulatory Requirements**

- SOX compliance documentation

- GDPR data mapping
- ISO 27001 controls
- Industry-specific regulations

## 2. Audit Procedures

- Quarterly internal audits
- Annual external audit
- Continuous compliance monitoring
- Exception tracking and resolution

## 9. Training and Documentation

### 1. Required Training

- Initial CMDB certification
- Annual refresher course
- Role-specific advanced training
- Security awareness education

### 2. Documentation Standards

- Standard operating procedures
- Technical reference guides
- Process flow diagrams
- Training materials maintenance

## 10. Legal Disclaimers

1. This document contains confidential and proprietary information of Summit Digital Solutions, Inc. Unauthorized disclosure, reproduction, or use is strictly prohibited.

2. The Company reserves the right to modify this Guide at any time. All users are responsible for compliance with the most current version.

## 11. Document Control

Document Owner: Chief Technology Officer

Review Frequency: Annual

Last Review Date: January 9, 2024

Next Review Date: January 9, 2025

APPROVED BY:

Michael Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

Sarah Blackwell

Chief Operating Officer

Summit Digital Solutions, Inc.

**Date:** \_