DevOps Pipeline Configuration Guide

Summit Digital Solutions, Inc.

Document Version: 1.2

Last Updated: January 9, 2024

Classification: Confidential & Proprietary

1. Purpose and Scope

1. This DevOps Pipeline Configuration Guide ("Guide") establishes the mandatory requirements and procedures for configuring, maintaining, and securing continuous integration and continuous deployment (CI/CD) pipelines within Summit Digital Solutions, Inc. ("Company") development environments.

2. This Guide applies to all employees, contractors, and third-party vendors involved in the development, deployment, or maintenance of Company software applications, including but not limited to the Peak Performance Platform(TM).

2. Definitions

1. "Pipeline" refers to the automated sequence of processes for building, testing, and deploying software applications.

2. "Production Environment" means the live environment where Company applications are made available to clients.

3. "Artifact" means any compiled code, container image, or deployable package produced by the pipeline.

3. Pipeline Configuration Requirements

1. **Authentication and Access Control**

- All pipeline configurations must utilize Company-approved SSH keys
- Access credentials must be stored in the approved secure vault system
- Multi-factor authentication is mandatory for all pipeline administrative access

2. **Source Control Integration**

- All pipelines must integrate with Company's approved Git repositories
- Branch protection rules must be enforced as per Section 4
- Commit signing with approved keys is mandatory

3. **Build Requirements**
- All builds must be reproducible and version-controlled
- Dependencies must be pulled from approved internal repositories
- Build artifacts must be digitally signed and verified

4. Security Controls

1. **Code Scanning**
- Static Application Security Testing (SAST) must be integrated
- Software Composition Analysis (SCA) for dependency verification
- Container image scanning for vulnerabilities

2. **Environment Segregation**
- Strict separation between development, staging, and production environments
- Network isolation between pipeline stages
- Separate credential sets for each environment

5. Compliance Requirements

1. **Audit Logging**
- All pipeline activities must be logged to Company's centralized logging system
- Logs must be retained for minimum 180 days
- Pipeline configuration changes require documented approval

2. **Regulatory Compliance**
- SOC 2 Type II controls must be maintained
- GDPR requirements for EU client data handling
- HIPAA compliance measures where applicable

6. Deployment Procedures

1. **Release Authorization**

- All production deployments require documented approval
- Emergency changes must follow incident management procedures
- Rollback procedures must be tested and documented

2. **Deployment Windows**

- Standard deployments restricted to approved maintenance windows
- Geographic region-specific deployment scheduling
- Client notification requirements per service level agreements

7. Monitoring and Maintenance

1. **Performance Monitoring**

- Pipeline execution metrics must be collected and analyzed
- Resource utilization thresholds established and monitored
- Automated alerts for pipeline failures or delays

2. **Regular Maintenance**

- Quarterly security review of pipeline configurations
- Monthly dependency updates and vulnerability scanning
- Annual disaster recovery testing

8. Intellectual Property Protection

1. All pipeline configurations, scripts, and custom tools developed under this Guide are the exclusive property of Summit Digital Solutions, Inc.

2. Confidentiality of client-specific pipeline configurations must be maintained in accordance with applicable NDAs.

9. Amendments and Updates

1. This Guide shall be reviewed and updated annually or as required by material changes in Company technology or compliance requirements.

2. Updates to this Guide must be approved by the Chief Technology Officer and Chief Information Security Officer.

10. Enforcement

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

2. Exceptions to this Guide must be documented and approved by both the CTO and CISO.

APPROVED AND ADOPTED:

Summit Digital Solutions, Inc.

By:

Michael Chang

Chief Technology Officer

Date: _

By:

James Henderson

Chief Digital Officer

Date: _