CONTINUOUS INTEGRATION BEST PRACTICES

Summit Digital Solutions, Inc.

Effective Date: January 9, 2024

Document Version: 2.0

Classification: Confidential

1. PURPOSE AND SCOPE

1. This document establishes the mandatory continuous integration ("CI") practices and procedures for all software development activities conducted by Summit Digital Solutions, Inc. ("Company") in relation to its Peak Performance Platform and associated software products.

2. These practices apply to all employees, contractors, and third-party developers engaged in software development activities for the Company.

2. DEFINITIONS

1. "Continuous Integration" means the practice of automating the integration of code changes from multiple contributors into a single software project.

2. "Build Pipeline" refers to the automated sequence of steps that code changes must successfully pass through before deployment.

3. "Development Environment" means the Company's approved integrated development environment and associated tools.

4. "Production Code" means any code intended for deployment to customer-facing systems or the Peak Performance Platform.

3. MANDATORY CI PRACTICES

1. Version Control Requirements

a) All Production Code must be maintained in the Company's approved Git repository

b) Branch naming must follow the format: feature/[TICKET-ID]-description

c) Commits must reference corresponding JIRA tickets

d) Force pushes to protected branches are prohibited

2. Build Pipeline Requirements

a) All code changes must pass through the following stages:

i. Static code analysis

ii. Unit testing (minimum 85% coverage)

iii. Integration testing

iv. Security scanning

v. Performance testing

b) Failed builds must be addressed within one business day

c) Build artifacts must be versioned according to semantic versioning standards

3. Code Review Standards

a) All code changes require minimum two (2) peer reviews

b) Reviews must be completed within 24 business hours

c) Automated code quality gates must be satisfied

d) Security review required for changes to authentication or authorization systems

4. SECURITY AND COMPLIANCE

1. All CI/CD pipelines must implement:

a) Encrypted secrets management

b) Role-based access control

c) Audit logging of all pipeline activities

d) Automated security scanning

e) Compliance validation for relevant standards (SOC 2, ISO 27001)

2. Security Scanning Requirements

a) SAST (Static Application Security Testing)

b) DAST (Dynamic Application Security Testing)

c) Software composition analysis

d) Container security scanning

e) Infrastructure as Code validation

5. MONITORING AND METRICS

1. Required CI Pipeline Metrics

a) Build success rate

b) Average build duration

c) Code coverage percentage

d) Security findings

e) Technical debt metrics

f) Time to recovery from failed builds

2. Reporting Requirements

a) Weekly CI metrics review

b) Monthly trend analysis

c) Quarterly compliance audit

d) Annual security assessment

6. DISASTER RECOVERY AND BUSINESS CONTINUITY

1. CI System Recovery

a) Maximum recovery time objective: 4 hours

b) Daily backup of CI configurations

c) Documented recovery procedures

d) Quarterly recovery testing

2. Alternative Procedures

a) Manual code review process

b) Temporary build procedures

c) Emergency deployment protocols

7. COMPLIANCE AND ENFORCEMENT

1. Compliance with these practices is mandatory for all software development activities.

2. Violations will be tracked and may result in:

a) Mandatory additional training

b) Revocation of commit privileges

c) Disciplinary action per Company policy

8. AMENDMENTS AND UPDATES

1. This document shall be reviewed and updated annually or as required by:

a) Technology changes

b) Regulatory requirements

c) Business needs

d) Security incidents

APPROVAL AND EXECUTION

IN WITNESS WHEREOF, this document has been approved and executed by the undersigned authorized representatives of Summit Digital Solutions, Inc.

APPROVED BY:

Michael Chang

Chief Technology Officer

Date: January 9, 2024

James Henderson

Chief Digital Officer

Date: January 9, 2024

Dr. Robert Martinez

Chief Innovation Officer

Date: January 9, 2024