CODE REVIEW STANDARDS

Summit Digital Solutions, Inc.

Effective Date: January 1, 2024

Document Version: 2.0

Last Updated: December 15, 2023

1. PURPOSE AND SCOPE

1. This Code Review Standards document ("Standards") establishes mandatory procedures and requirements for all software code review processes at Summit Digital Solutions, Inc. ("Company"), including its Peak Performance Platform and associated software products.

2. These Standards apply to all employees, contractors, and third-party developers ("Development Personnel") engaged in software development activities for the Company.

2. DEFINITIONS

1. "Code Review" means the systematic examination of source code intended to be deployed in any Company software product or system.

2. "Critical Code" means any code that affects core platform functionality, security features, or client data handling within the Peak Performance Platform.

3. "Pull Request" means a formal submission of code changes for review prior to integration into the main codebase.

3. MANDATORY REVIEW REQUIREMENTS

1. All code changes must undergo review before deployment to any production environment.

2. Critical Code requires review by at least two (2) senior developers, one of whom must be a designated Technical Lead or above.

3. Non-critical code changes require review by at least one (1) developer of equal or higher level than the submitter.

4. Emergency hotfixes must receive post-deployment review within 24 hours of implementation.

4. REVIEW PROCESS

1. Pre-Review Requirements

- Complete static code analysis using approved tools
- Pass all automated tests
- Include updated documentation
- Conform to Company coding standards
- Include appropriate test coverage

2. Review Procedures

a) Submitter must create Pull Request with:

- Detailed description of changes
- Link to relevant ticket/issue
- Test results
- Impact assessment

b) Reviewer(s) must evaluate:

- Code functionality
- Security implications
- Performance impact
- Architecture alignment
- Documentation adequacy

3. Approval Criteria

- All critical issues resolved
- Test coverage meets minimum thresholds
- Documentation complete and accurate
- Compliance with security standards verified
- Architecture review completed for significant changes

5. SECURITY AND COMPLIANCE

1. All code reviews must verify compliance with:

- Company Security Policy

- OWASP Security Guidelines
- Relevant regulatory requirements
- Client-specific security requirements

2. Security-sensitive code requires additional review by the Security Team.

6. DOCUMENTATION REQUIREMENTS

1. All code changes must include:

- Updated API documentation
- Change log entries
- Configuration updates
- Deployment instructions
- Rollback procedures

2. Technical documentation must be maintained in the approved repository.

7. QUALITY METRICS

1. Code Review Performance Metrics

- Review completion time
- Defect detection rate
- Review thoroughness
- Post-deployment issue rate

2. Quarterly review of metrics by Engineering Leadership.

8. ENFORCEMENT AND EXCEPTIONS

1. Compliance with these Standards is mandatory for all Development Personnel.

2. Exceptions require written approval from:

- Chief Technology Officer
- Chief Security Officer
- VP of Engineering

9. AMENDMENTS AND UPDATES

1. These Standards shall be reviewed annually by Engineering Leadership.

2. Updates require approval from:

- Chief Technology Officer
- Chief Digital Officer
- Legal Department

10. LEGAL COMPLIANCE

1. These Standards form part of the Company's compliance framework and are subject to all applicable laws and regulations.

2. Violation may result in disciplinary action up to and including termination.

ACKNOWLEDGMENT

The undersigned acknowledges receipt and understanding of these Code Review Standards:

Name:

Title:

Date:

Signature:

APPROVED BY:

_

Michael Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

_

James Henderson

Chief Digital Officer

Summit Digital Solutions, Inc.

Date: January 1, 2024