DEPLOYMENT ROLLBACK PROCEDURES

Summit Digital Solutions, Inc.

Effective Date: January 15, 2024

Document Version: 2.4

Classification: Confidential

1. PURPOSE AND SCOPE

1. This document establishes the mandatory procedures and protocols for executing deployment rollbacks within Summit Digital Solutions, Inc.'s ("Company") Peak Performance Platform and associated enterprise systems.

2. These procedures apply to all production deployments, system updates, and code releases affecting client environments or internal production systems.

2. DEFINITIONS

1. "Deployment" means any release of code, configuration changes, or system updates to production environments.

2. "Rollback" refers to the process of reverting a deployment to its previous stable state.

3. "Critical Systems" include the Peak Performance Platform, client-facing applications, and core infrastructure components.

4. "Recovery Point Objective (RPO)" means the maximum targeted period in which data might be lost due to a rollback.

3. ROLLBACK AUTHORIZATION

1. Rollback authority is hereby vested in the following roles:

a) Chief Technology Officer

b) VP of Engineering

c) Senior Platform Architects

d) On-call Engineering Managers

2. Emergency rollbacks may be initiated by the on-call engineer with post-facto approval from an

authorized party within 1 hour of execution.

4. PRE-DEPLOYMENT REQUIREMENTS

1. Prior to any production deployment, the following must be documented:

a) Complete backup of affected systems

b) Detailed rollback plan with specific steps

c) Recovery time estimates

d) Data preservation strategy

e) Client impact assessment

2. Rollback scripts and procedures must be tested in staging environments before deployment approval.

5. ROLLBACK TRIGGERS

1. Mandatory rollback scenarios include:

a) Critical functionality failure affecting >5% of users

b) Data integrity issues

c) Security vulnerabilities (CVSS score >7.0)

d) Performance degradation exceeding 200% baseline

e) Regulatory compliance violations

2. Discretionary rollback scenarios require documented approval from two authorized parties.

6. EXECUTION PROCEDURES

1. Standard Rollback Process:

a) Issue "ROLLBACKINITIATED" alert to stakeholders

b) Freeze all related deployments

c) Execute database restoration procedures

d) Revert code to previous stable version

e) Restore configuration files

f) Verify system integrity

g) Execute automated test suite

h) Perform manual verification

2. Time Requirements:

a) Decision to rollback: 15 minutes

b) Execution completion: 45 minutes

c) System verification: 30 minutes

7. CLIENT COMMUNICATION

1. The Company shall notify affected clients within:

a) 15 minutes for Critical Systems rollbacks

b) 30 minutes for non-critical rollbacks

2. Communications must include:

a) Incident description

b) Expected resolution time

c) Business impact assessment

d) Mitigation steps

e) Post-resolution status

8. DOCUMENTATION AND REPORTING

1. Post-rollback documentation requirements:

a) Incident timeline

b) Technical impact analysis

c) Root cause assessment

d) Client impact report

e) Preventive measures

f) Lessons learned

2. Reports must be submitted to the Technology Steering Committee within 24 hours.

9. COMPLIANCE AND AUDIT

1. All rollback events shall be logged in the Company's compliance management system.

2. Quarterly audits of rollback procedures and execution shall be conducted by the Quality Assurance team.

10. AMENDMENTS AND REVIEWS

1. This document shall be reviewed and updated annually or upon material changes to deployment infrastructure.

2. Amendments require approval from the Technology Steering Committee and Chief Technology Officer.

11. LEGAL DISCLAIMER

1. These procedures are confidential and proprietary to Summit Digital Solutions, Inc.

2. Nothing in this document shall be construed to create any warranties or guarantees regarding system availability or performance.

APPROVAL AND EXECUTION

APPROVED AND ADOPTED this 15th day of January, 2024.

SUMMIT DIGITAL SOLUTIONS, INC.

By:

Michael Chang

Chief Technology Officer

By:

Sarah Blackwell

Chief Operating Officer