CRITICAL INCIDENT MANAGEMENT PLAN

Summit Digital Solutions, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

1. PURPOSE AND SCOPE

1 This Critical Incident Management Plan ("Plan") establishes the framework and procedures for Summit Digital Solutions, Inc. ("Company") to respond to, manage, and recover from critical incidents affecting its operations, clients, or technology infrastructure.

2 This Plan applies to all Company employees, contractors, and third-party service providers involved in the delivery of digital transformation services, AI/ML implementations, IoT systems integration, and related professional services.

2. DEFINITIONS

1 "Critical Incident" means any unplanned event or situation that:

a) Significantly disrupts client service delivery

b) Threatens the security or integrity of the Peak Performance Platform

c) Poses material risk to Company operations

d) May result in substantial financial or reputational damage

e) Creates potential legal or regulatory exposure

2 "Incident Response Team" or "IRT" means the cross-functional team designated to manage critical incidents, comprising representatives from Executive Leadership, Technology, Operations, Legal, and Communications departments.

3. INCIDENT CLASSIFICATION AND ESCALATION

1 Severity Levels:

- Level 1 (Critical): Complete system failure, data breach, or service interruption affecting multiple enterprise clients
- Level 2 (High): Significant disruption to single major client or critical system component
- Level 3 (Medium): Limited service degradation with workaround available

- Level 4 (Low): Minor issue with minimal operational impact

2 Escalation Protocol:

a) Initial incident reporter notifies immediate supervisor

b) Supervisor assesses severity and notifies IRT Lead within 15 minutes for Level 1/2 incidents

c) IRT Lead activates appropriate response team members

d) CEO notification required for all Level 1 incidents within 30 minutes

4. RESPONSE PROCEDURES

1 Initial Response:

a) IRT Lead establishes incident command center

b) Technical team initiates diagnostic procedures

c) Client Services implements communication protocols

d) Legal assesses compliance and liability implications

e) Operations evaluates business continuity measures

2 Documentation Requirements:

a) Incident timeline and response actions

b) System/service impact assessment

c) Client communication records

d) Resource allocation and deployment

e) Recovery measures implemented

5. COMMUNICATION PROTOCOLS

1 Internal Communications:

a) Dedicated incident management Slack channel

b) Hourly status updates during active incidents

c) Daily briefings until resolution

d) Post-incident analysis reports

2 External Communications:

a) Client notification within SLA parameters

b) Regulatory reporting as required

c) Media response protocols

d) Stakeholder updates

6. RECOVERY AND CONTINUITY

1 System Recovery:

a) Implementation of redundancy protocols

b) Activation of backup systems

c) Data restoration procedures

d) Service level normalization

2 Business Continuity:

a) Alternative service delivery methods

b) Resource reallocation

c) Client service contingencies

d) Operational workarounds

7. POST-INCIDENT PROCEDURES

1 Analysis Requirements:

a) Root cause investigation

b) Impact assessment

c) Response effectiveness evaluation

d) Preventive measure identification

2 Documentation and Reporting:

a) Detailed incident report

b) Corrective action plan

c) Policy/procedure updates

d) Training recommendations

8. MAINTENANCE AND TESTING

1 Plan Review:

a) Quarterly review by IRT

b) Annual comprehensive update

c) Post-incident revision as needed

2 Testing Schedule:

a) Monthly tabletop exercises

b) Quarterly technical drills

c) Annual full-scale simulation

9. COMPLIANCE AND GOVERNANCE

1 This Plan shall comply with:

a) ISO 27001 requirements

b) SOC 2 Type II controls

c) Client contractual obligations

d) Applicable regulatory requirements

2 The Chief Digital Officer shall serve as Plan Owner, responsible for maintenance and enforcement.

10. AUTHORIZATION

This Critical Incident Management Plan is approved and adopted by:

Dr. Alexandra Reeves

Chief Executive Officer

Summit Digital Solutions, Inc.

James Henderson

Chief Digital Officer

Summit Digital Solutions, Inc.

Date: January 15, 2024