DISASTER RECOVERY PROTOCOL

Summit Digital Solutions, Inc.

Effective Date: January 15, 2024

Document Version: 2.0

Last Updated: January 9, 2024

1. PURPOSE AND SCOPE

1. This Disaster Recovery Protocol ("Protocol") establishes the policies, procedures, and responsibilities for the recovery and continuation of Summit Digital Solutions, Inc.'s ("Company") critical technology infrastructure and business operations following a disaster or major disruption.

2. This Protocol applies to all Company facilities, employees, contractors, and technology systems, with particular emphasis on the Peak Performance Platform and associated client-facing services.

2. DEFINITIONS

1. "Disaster" means any event that causes significant disruption to normal business operations, including but not limited to:

a) Natural disasters

b) Cyber attacks

c) Infrastructure failures

d) Public health emergencies

e) Acts of terrorism

2. "Recovery Time Objective" or "RTO" means the targeted duration of time within which a business process must be restored after a disaster.

3. "Recovery Point Objective" or "RPO" means the maximum targeted period in which data might be lost due to a disaster.

3. DISASTER RECOVERY TEAM

1. The Disaster Recovery Team shall consist of:

a) Chief Technology Officer (Team Leader)

b) Chief Operating Officer

c) Chief Information Security Officer

d) Infrastructure Manager

e) Client Services Director

f) Legal Counsel

2. Team Responsibilities:

- Initial disaster assessment

- Protocol activation

- Communication coordination

- Recovery operations management

- Client impact mitigation

- Compliance monitoring

4. CRITICAL SYSTEMS AND PRIORITIES

1. Priority 1 Systems (RTO: 4 hours)

- Peak Performance Platform core infrastructure

- Client data repositories

- Authentication systems

- Emergency communication systems

2. Priority 2 Systems (RTO: 12 hours)

- IoT integration networks

- Analytics processing systems

- Client reporting interfaces

- Internal collaboration tools

3. Priority 3 Systems (RTO: 24 hours)

- Non-critical business applications

- Development environments

- Training systems

- Administrative systems

5. RECOVERY PROCEDURES

1. Initial Response

a) Disaster Recovery Team activation

b) Situation assessment and classification

c) Communication protocol initiation

d) Resource mobilization

2. Data Recovery

a) Activation of redundant systems

b) Data restoration from secure backups

c) Integrity verification

d) Client data prioritization

3. System Restoration

a) Infrastructure recovery

b) Application restoration

c) Network connectivity

d) Security controls verification

6. COMMUNICATION PROTOCOLS

1. Internal Communications

- Emergency notification system activation

- Employee communication channels

- Status reporting procedures

- Team coordination protocols

2. External Communications

- Client notification procedures

- Regulatory reporting requirements

- Media relations protocol

- Stakeholder updates

7. TESTING AND MAINTENANCE

1. Testing Requirements

- Quarterly tabletop exercises

- Semi-annual technical recovery tests

- Annual full-scale disaster simulation

- Regular backup verification

2. Documentation Requirements

- Test results documentation

- Protocol update procedures

- Improvement recommendations

- Compliance verification

8. COMPLIANCE AND REPORTING

1. The Company shall maintain compliance with:

- SOC 2 Type II requirements

- ISO 27001 standards

- Client contractual obligations

- Industry regulations

2. Documentation Requirements

- Incident logs

- Recovery metrics

- Compliance reports

- After-action reviews

9. LEGAL AND LIABILITY

1. This Protocol does not constitute a guarantee of service levels or recovery timeframes.

2. The Company maintains appropriate insurance coverage for business interruption and cyber incidents.

10. PROTOCOL UPDATES

1. This Protocol shall be reviewed and updated:

- Annually at minimum

- Following major incidents

- Upon significant system changes

- As required by regulatory changes

AUTHORIZATION

This Protocol is authorized and approved by:

Dr. Alexandra Reeves

Chief Executive Officer

Summit Digital Solutions, Inc.

Michael Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

Date: January 15, 2024

End of Document