SECURITY INCIDENT RESPONSE PLAYBOOK

Summit Digital Solutions, Inc.

Last Updated: January 9, 2024

Document Version: 3.2

1. PURPOSE AND SCOPE

1. This Security Incident Response Playbook ("Playbook") establishes the procedures and protocols for responding to security incidents affecting Summit Digital Solutions, Inc. ("Company") systems, networks, data, and operations.

2. This Playbook applies to all employees, contractors, consultants, temporary workers, and other personnel who have access to Company systems or data.

2. DEFINITIONS

1. "Security Incident" means any actual or suspected event that threatens the confidentiality, integrity, or availability of Company information systems, networks, or data, including but not limited to:

a) Unauthorized access to Company systems

b) Data breaches or exfiltration

c) Malware infections

d) Denial of service attacks

e) Physical security breaches

f) Social engineering attempts

2. "Incident Response Team" or "IRT" means the cross-functional team responsible for managing security incidents, comprising representatives from:

- Information Technology
- Information Security
- Legal Department
- Corporate Communications
- Executive Leadership
- Risk Management

3. INCIDENT CLASSIFICATION

1. Level 1 - Minor Incident

- Limited impact
- No sensitive data exposure
- Routine resolution possible
- Response within 24 hours

2. Level 2 - Moderate Incident

- Potential sensitive data exposure
- Limited system disruption
- Response within 4 hours
- IRT notification required

3. Level 3 - Critical Incident

- Confirmed data breach
- Significant system disruption
- Immediate response required
- Full IRT activation
- Executive notification mandatory

4. INCIDENT RESPONSE PROCEDURES

1. Initial Detection and Reporting

a) All personnel must immediately report suspected security incidents to security@summitdigital.com

b) On-call security personnel must acknowledge within 15 minutes

c) Initial assessment must be completed within 1 hour

2. Containment

a) Implement immediate containment measures

b) Isolate affected systems

c) Preserve evidence

d) Document all actions taken

3. Investigation

a) Establish incident timeline

b) Identify affected systems and data

c) Determine root cause

d) Document findings

e) Maintain chain of custody

4. Remediation

a) Develop remediation plan

b) Obtain necessary approvals

c) Execute remediation measures

d) Verify effectiveness

e) Document all actions

5. COMMUNICATION PROTOCOLS

1. Internal Communications

a) IRT communications via encrypted channels only

b) Regular status updates to stakeholders

c) Documentation of all communications

2. External Communications

a) Legal department approval required

b) Coordinate with PR team

c) Follow disclosure requirements

d) Document all external communications

6. REGULATORY COMPLIANCE

1. The Company shall comply with all applicable notification requirements, including:

a) State data breach notification laws

b) GDPR requirements

c) Industry-specific regulations

d) Contractual obligations

2. Legal department shall maintain current notification requirements matrix

7. DOCUMENTATION AND REPORTING

1. Required Documentation

a) Incident timeline

b) Actions taken

c) Evidence collected

d) Communications log

e) Post-incident analysis

2. Retention Requirements

a) Maintain all incident documentation for 7 years

b) Store in encrypted format

c) Restrict access to authorized personnel

8. POST-INCIDENT ACTIVITIES

1. After-Action Review

a) Conduct within 72 hours of incident closure

b) Document lessons learned

c) Update procedures as needed

2. Preventive Measures

a) Implement recommended changes

b) Update training materials

c) Revise security controls

9. TRAINING AND AWARENESS

1. All personnel must complete annual incident response training

2. IRT members must complete quarterly tabletop exercises

3. Documentation of training completion required

10. REVIEW AND UPDATES

1. This Playbook shall be reviewed annually

2. Updates require CISO and General Counsel approval

3. Version control must be maintained

APPROVAL AND EXECUTION

IN WITNESS WHEREOF, this Security Incident Response Playbook has been approved and adopted by the undersigned authorized representatives of Summit Digital Solutions, Inc.

Date: January 9, 2024

Michael Chang

Chief Technology Officer

Sarah Blackwell

Chief Operating Officer

James Henderson

Chief Digital Officer