

MySleepScoring™

**Volume 7 – Incident Response & Risk Management
Manual**

Version 1.0 | Internal Confidential

Table of Contents

1. Incident Response Program
2. Security Event Classification
3. Incident Reporting
4. Incident Response Team
5. Initial Triage
6. Evidence Preservation
7. Cybersecurity Incidents
8. Unauthorized Access
9. Malware & Ransomware
10. Lost or Stolen Devices
11. Privacy Incidents
12. Breach Investigation
13. Root Cause Analysis
14. Corrective & Preventive Actions
15. Risk Register
16. Enterprise Risk Assessment
17. Threat Identification
18. Risk Analysis
19. Risk Treatment
20. Residual Risk Acceptance
21. Client Notification
22. Regulatory Notification
23. Post-Incident Review
24. Annual Testing

Incident Response Program

This section establishes company requirements for incident response program.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Security Event Classification

This section establishes company requirements for security event classification.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Incident Reporting

This section establishes company requirements for incident reporting.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Incident Response Team

This section establishes company requirements for incident response team.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Initial Triage

This section establishes company requirements for initial triage.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Evidence Preservation

This section establishes company requirements for evidence preservation.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Cybersecurity Incidents

This section establishes company requirements for cybersecurity incidents.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Unauthorized Access

This section establishes company requirements for unauthorized access.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Malware & Ransomware

This section establishes company requirements for malware & ransomware.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Lost or Stolen Devices

This section establishes company requirements for lost or stolen devices.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Privacy Incidents

This section establishes company requirements for privacy incidents.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Breach Investigation

This section establishes company requirements for breach investigation.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Root Cause Analysis

This section establishes company requirements for root cause analysis.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Corrective & Preventive Actions

This section establishes company requirements for corrective & preventive actions.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Risk Register

This section establishes company requirements for risk register.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Enterprise Risk Assessment

This section establishes company requirements for enterprise risk assessment.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Threat Identification

This section establishes company requirements for threat identification.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Risk Analysis

This section establishes company requirements for risk analysis.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Risk Treatment

This section establishes company requirements for risk treatment.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Residual Risk Acceptance

This section establishes company requirements for residual risk acceptance.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Client Notification

This section establishes company requirements for client notification.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Regulatory Notification

This section establishes company requirements for regulatory notification.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Post-Incident Review

This section establishes company requirements for post-incident review.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.

Annual Testing

This section establishes company requirements for annual testing.

All suspected incidents shall be reported immediately through established reporting channels.

The Incident Response Team documents actions taken, preserves relevant evidence, and coordinates containment, eradication, recovery, and communication.

Risk decisions are documented, assigned to responsible owners, monitored, and reviewed during management meetings.

Policies are reviewed at least annually and after significant incidents, regulatory changes, or operational updates.