MySleepScoring™

Volume 2 – Security Policies

Version 1.0 | Internal Confidential

Table of Contents

37. Business Continuity Policy
38. Disaster Recovery Policy
39. Vendor Management Policy
40. Business Associate Management Policy

Policy 1: Information Security

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 2: Security Governance

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 3: Risk Management

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 4: Risk Assessment

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 5: Acceptable Use

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 6: Confidentiality

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 7: Access Control

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 8: Identity Management

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 9: Password

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 10: Multi-Factor Authentication

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 11: Privileged Access

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 12: User Provisioning

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 13: User Deprovisioning

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 14: Endpoint Protection

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 15: Laptop Security

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 16: Remote Work

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 17: BYOD

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 18: Mobile Device

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 19: USB Media

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 20: Network Security

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 21: Firewall

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 22: VPN

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 23: Wireless Security

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 24: Encryption

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 25: Data Classification

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 26: Data Retention

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 27: Secure Disposal

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 28: Backup & Recovery

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 29: Secure File Transfer

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 30: Email Security

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 31: Logging & Monitoring

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 32: Patch Management

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 33: Vulnerability Management

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 34: Change Management

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 35: Incident Response

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 36: Breach Notification

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 37: Business Continuity

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 38: Disaster Recovery

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 39: Vendor Management

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually

Policy 40: Business Associate Management

Purpose
Establish minimum security requirements for this operational area.

Policy Statement
All workforce members shall comply with this policy. Exceptions require written approval from executive leadership and the Compliance Officer.

Requirements

• Access shall follow the principle of least privilege.

• Activities shall be documented where applicable.

• Annual review and updates are required.

• Violations may result in corrective action.

• Controls shall support HIPAA obligations and client contractual requirements.

Responsible Owner: Information Security Officer

Review Frequency: Annually