Malachor MSP Standards and Procedures

Compliance Operations Manual

Version: 1.1.0 **Effective Date:** December 30, 2025 **Review Cycle:** Quarterly

---

Table of Contents

Purpose and Scope

This document establishes standard operating procedures for the Malachor MSP Compliance Platform. These procedures apply to all managed client sites and govern the handling of compliance incidents, infrastructure maintenance, and HIPAA-related security controls.

Applicability

- All managed healthcare client sites
- All Malachor MSP technicians and administrators
- Automated compliance agent operations
- Third-party contractors with system access

HIPAA Controls Coverage

Control Category	HIPAA Reference	Description
Access Control	164.312(a)(1)	Unique user identification, automatic logoff
Audit Controls	164.312(b)	Activity logging, review procedures
Integrity Controls	164.312(c)(1)	ePHI alteration/destruction protection
Transmission Security	164.312(e)(1)	Encryption, integrity controls
Contingency Plan	164.308(a)(7)	Backup, disaster recovery
Security Awareness	164.308(a)(5)	Training, incident reporting

---

Incident Response Procedures

Three-Tier Resolution Model

The platform uses an automated three-tier resolution model:

L1: Deterministic Resolution (70-80% of incidents)

- **Response Time:** < 100ms
- **Cost:** $0
- **Actions:** Pre-defined automated fixes
- **Human Intervention:** None required
- **Examples:**
  - Restart stalled Windows services
  - Clear temporary file accumulation
  - Force signature updates

L2: LLM-Assisted Resolution (15-20% of incidents)

- **Response Time:** 2-5 seconds
- **Cost:** ~$0.001 per incident
- **Actions:** AI-generated remediation plans
- **Human Intervention:** Optional review
- **Examples:**
  - Complex service dependency issues
  - Multi-step configuration repairs
  - Novel issue patterns

L3: Human Escalation (5-10% of incidents)

- **Response Time:** Per SLA (typically 4 hours)
- **Cost:** Technician time
- **Actions:** Manual intervention required
- **Human Intervention:** Required
- **Examples:**
  - Hardware failures
  - Security incidents requiring investigation
  - Vendor-specific issues

Incident Classification

Severity	Description	Response Target	Escalation Trigger
Critical	System down, data at risk	15 minutes	Immediate page
High	Major function impaired	1 hour	After 2 L1 failures
Medium	Partial impact	4 hours	After 3 L1 failures
Low	Minor issue, workaround exists	24 hours	End of business day

Incident Response Workflow

1. **Detection**

   - Continuous monitoring via compliance agent
   - Check-in every 60 seconds

    - Drift detection against baseline

2. **Classification**
    - Automatic severity assignment
    - HIPAA control mapping
    - Resolution level determination
3. **Resolution**
    - L1: Execute runbook immediately
    - L2: Generate and execute remediation plan
    - L3: Create ticket, page on-call technician
4. **Verification**
    - Post-remediation health check
    - Drift re-scan within 5 minutes
    - Evidence bundle generation
5. **Documentation**
    - Incident record creation
    - Evidence hash and timestamp
    - Audit trail preservation

Learning Loop System

The Learning Loop is the core mechanism that continuously improves L1 automation by analyzing successful L2 resolutions. This reduces costs and response times over time.

Pattern Detection

When L2 (LLM-assisted) resolutions succeed, the system:

1. **Signature Generation:** Creates a unique pattern signature from:
    - Incident type
    - Runbook executed
    - Match conditions (normalized and sorted)
    - Parameters used
2. **Pattern Aggregation:** Updates pattern statistics:
    - Occurrence count
    - Success/failure counts
    - Success rate calculation
    - First/last seen timestamps

Promotion Criteria

Patterns become eligible for promotion to L1 when ALL conditions are met:

Criterion	Threshold	Rationale
Occurrences	≥ 5	Sufficient sample size

Success Rate	≥ 90%	High confidence in reliability
Status	Pending	Not already promoted or rejected

Promotion Process

1. **Candidate Review:** Security team reviews eligible patterns weekly
2. **Approval:** Pattern marked as "promoted" in database
3. **Rule Creation:** L1 rule created with:
   - Unique rule ID
   - Match conditions from pattern
   - Associated runbook
   - HIPAA control mappings
4. **Distribution:** Rule synced to all agents on next check-in

Agent Rule Synchronization

Parameter	Default	Description
Sync Interval	3600s	How often agents pull rules
Rules Version	MD5 hash	Quick change detection
Batch Size	10	Evidence items per upload

Sync Protocol:

1. Agent calls `/agent/sync` with site ID
2. Server returns rules array with version hash
3. Agent compares hash to cached version
4. If changed, agent updates local rule cache
5. New L1 rules take effect immediately

Monitoring

Metric	Dashboard Location	Alert Threshold
L1 Resolution Rate	Learning Loop tab	< 70% (warning)
Promotion Candidates	Learning Loop tab	> 20 pending review
Pattern Success Rate	Pattern details	< 85% (review needed)
Rule Sync Failures	Fleet Health	> 3 consecutive

Review Procedures

Weekly:

- Review promotion candidates
- Approve or reject pending patterns
- Verify rule distribution success

Monthly:

- Analyze L1/L2/L3 resolution ratios

- Review rejected patterns for improvements
- Update runbooks based on pattern data

Quarterly:

- Full learning loop audit
- Cost savings analysis
- Pattern library cleanup

Patching Standards

Operating System Patches

Platform	Patch Cycle	Maintenance Window	Auto-Reboot
Windows Server	Monthly	Sunday 2-6 AM	Yes, if required
Windows 10/11	Monthly	Sunday 2-6 AM	Yes, if required
NixOS	Weekly	Continuous (atomic)	No

Patch Compliance Thresholds

- **Critical Security Patches:** 72 hours maximum
- **Important Patches:** 14 days maximum
- **Optional Patches:** 30 days maximum
- **Compliance Target:** 95% of devices fully patched

Emergency Patching

For zero-day vulnerabilities with active exploitation:

1. Assess impact to managed fleet
2. Test patch in sandbox environment
3. Deploy to critical systems within 24 hours
4. Document exception for extended timeline

Patch Failure Handling

1. Automatic retry after 1 hour
2. L1 runbook: Clear Windows Update cache
3. L2 escalation: Diagnose specific failure
4. L3 escalation: Manual intervention if unresolved

Backup and Recovery

Backup Schedule

Data Type	Frequency	Retention	Offsite Copy
System State	Daily	30 days	Weekly
User Data	Daily	90 days	Weekly
Database	Hourly	7 days, then daily	Daily

Logs	Real-time	365 days	Monthly

Backup Verification

- **Automated Testing:** Daily integrity checks
- **Recovery Testing:** Monthly full restore test
- **Documentation:** Test results retained 1 year

Recovery Time Objectives (RTO)

System Category	RTO	RPO
Critical (EHR, billing)	4 hours	1 hour
Important (email, file shares)	8 hours	4 hours
Standard (workstations)	24 hours	24 hours

Backup Failure Procedures

1. Alert generated immediately on backup failure
2. L1 runbook: Restart VSS services, retry backup
3. L2 escalation: Diagnose storage/connectivity issues
4. L3 escalation: Manual intervention if 2+ consecutive failures

---

Antivirus and Endpoint Protection

Required Protection

All managed endpoints must have:

- **Real-time scanning:** Enabled at all times
- **Signature updates:** Maximum 24-hour age
- **Behavioral monitoring:** Enabled
- **Firewall:** Enabled with managed policy

Scan Schedule

Scan Type	Frequency	Duration Limit
Quick Scan	Every 4 hours	10 minutes
Full Scan	Weekly	4 hours
Custom Scan	On demand	No limit

Detection Response

1. **Threat Detected:**
    - Automatic quarantine
    - Alert generated
    - Evidence preserved
2. **Quarantine Review:**

    - L1: Known false positives auto-released
    - L2: AI analysis of unknown threats
    - L3: Manual review for high-risk detections

3. **Post-Incident:**

    - Root cause analysis
    - Prevention measures
    - User notification if required

Signature Staleness Handling

- **12 hours:** Warning alert
- **24 hours:** L1 runbook: Force update
- **48 hours:** L2 escalation: Investigate update mechanism
- **72 hours:** L3 escalation: Critical, potential compromise

---

Logging and Monitoring

Required Log Sources

Source	Retention	Format	Integrity
Windows Security	365 days	EVTX/JSON	Hash chain
Application Logs	90 days	Various	Hash chain
Firewall Logs	365 days	Syslog	Hash chain
Backup Logs	365 days	JSON	Hash chain
Access Logs	365 days	JSON	Hash chain

Log Collection

- **Agent Check-in:** Every 60 seconds
- **Log Forwarding:** Every 5 minutes (batch)
- **Compression:** GZIP before transmission
- **Encryption:** TLS 1.3 in transit, AES-256 at rest

Monitoring Thresholds

Metric	Warning	Critical
CPU Usage	> 80% for 5 min	> 95% for 2 min
Memory Usage	> 85%	> 95%
Disk Space	< 15% free	< 5% free
Log Ingestion Delay	> 10 minutes	> 30 minutes

Log Integrity

All logs are protected by:

- Cryptographic hash chaining
- RFC 3161 trusted timestamps
- Tamper-evident storage
- Regular integrity audits

Access Control

User Account Standards

- **Password Complexity:** 12+ characters, mixed case, numbers, symbols
- **Password Expiration:** 90 days (or MFA exemption)
- **Account Lockout:** 5 failed attempts, 30-minute lockout
- **Session Timeout:** 15 minutes idle, 8 hours maximum

Privileged Access

- **Admin Accounts:** Separate from daily-use accounts
- **Just-in-Time Access:** 8-hour maximum elevation
- **MFA Required:** All privileged access
- **Activity Logging:** All privileged actions logged

Access Reviews

Review Type	Frequency	Reviewer
User Access	Quarterly	Client IT contact
Privileged Access	Monthly	Malachor security
Service Accounts	Quarterly	Malachor operations
API Keys	Monthly	Malachor security

Account Deprovisioning

Upon termination notification:

1. Disable account immediately
2. Revoke all active sessions
3. Remove from all groups
4. Archive mailbox (if applicable)
5. Document in audit log

Change Management

Change Categories

Category	Approval	Testing	Rollback Plan
Standard	Pre-approved	Optional	Recommended
Normal	CAB review	Required	Required
Emergency	Manager + tech lead	Post-change	Required

Standard Changes (Pre-Approved)

- Signature updates
- Security patches (non-critical)
- L1 runbook executions
- Backup schedule adjustments

Normal Change Process

1. **Request:** Submit change request with business justification
2. **Assessment:** Impact and risk analysis
3. **Approval:** CAB review (if required)
4. **Testing:** Validate in non-production
5. **Implementation:** During maintenance window
6. **Verification:** Post-change testing
7. **Documentation:** Update CMDB

Emergency Change Process

1. Verbal approval from manager
2. Implement change
3. Document within 24 hours
4. Post-incident review within 7 days

Escalation Procedures

On-Call Rotation

- **Primary:** First responder, 15-minute response
- **Secondary:** Backup if primary unavailable
- **Manager:** Escalation point for major incidents

Escalation Matrix

Condition	Action	Timeline
L1 fails 3 times	Escalate to L2	Immediate
L2 fails 2 times	Escalate to L3	Immediate
Critical severity	Page on-call	Immediate
No response	Escalate to manager	30 minutes
Client-reported issue	Acknowledge	15 minutes

Communication Requirements

- **Initial Response:** Within SLA window
- **Status Updates:** Every 2 hours (critical), 4 hours (high)
- **Resolution Notification:** Immediate upon fix
- **Post-Incident Report:** Within 72 hours

Documentation Requirements

Required Documentation

Document	Update Frequency	Owner
Network Diagram	On change	Client site lead
Asset Inventory	Monthly	Automated
Contact List	Monthly	Account manager
Runbook Library	On change	Engineering
Incident Reports	Per incident	Operations

Evidence Bundle Contents

Each compliance incident generates an evidence bundle containing:

- Incident timestamp and duration
- Affected systems and users
- Drift data (before/after)
- Remediation steps executed
- Verification results
- Cryptographic hash

Retention Periods

Document Type	Retention	Storage
Incident Evidence	6 years	WORM storage
Audit Logs	6 years	WORM storage
Configuration Backups	2 years	Encrypted backup
Reports	3 years	Document management

Appendix A: Contact Information

Escalation Contacts

Role	Contact Method	Response Time
L1 Automation	Automatic	Immediate
L2 AI Assistant	Automatic	2-5 seconds
L3 On-Call Technician	Page/SMS	15 minutes
Account Manager	Email/Phone	4 hours
Security Incident	security@malachor.io	1 hour

Client Portal

- **Dashboard:** http://[server]:3000

- **Documentation:** http://[server]:3000/USER_GUIDE.pdf
- **Support:** support@malachor.io

Appendix B: Compliance Checklist

Daily Checks (Automated)

- □ All agents checking in
- □ Backup jobs completed
- □ AV signatures current
- □ No critical incidents pending

Weekly Checks

- □ Review open incidents
- □ Verify patch compliance
- □ Review backup integrity
- □ Check disk space trends

Monthly Checks

- □ Access review
- □ Backup recovery test
- □ Security scan review
- □ Performance baseline update

Quarterly Checks

- □ Full access audit
- □ Disaster recovery test
- □ Policy review
- □ Training verification

Document Control

Version	Date	Author	Changes
1.0.0	2025-12-30	Malachor Operations	Initial release
1.1.0	2025-12-30	Malachor Operations	Added Learning Loop System section

---

This document is confidential and intended for authorized personnel only. For questions, contact compliance@malachor.io