CONTROLPOINT HEALTH
DSM-MEMBER-SRV CHANGE MANAGEMENT & POLICY ENFORCEMENT SIGN-OFF

Document Version: 1.0
Author: Joseph Knight
Date: 2025-12-30
Environment: DSM-MEMBER-SRV, Windows Server 2025
Classification: Confidential – Internal Use Only

This document defines the change management and policy enforcement processes for DSM-MEMBER-SRV, including the use of the master PowerShell script **DSM-MEMBER-SRV_MasterCompliance.ps1**. The script handles OS hardening, STIG enforcement, drift detection, reporting, and incident response actions.

---

1. Purpose

The purpose of this document is to establish formal procedures for change management and policy enforcement on DSM-MEMBER-SRV. It ensures STIG compliance, baseline security enforcement, automated drift detection and remediation, incident response, and clear accountability for all stakeholders.

---

2. Scope

This document applies to Windows Server 2025 member servers holding sensitive client PII/PHI. All STIG-aligned hardening, baseline configurations, automated scripts, daily monitoring, drift detection, and incident response actions are included.

---

3. Stakeholders and Responsibilities

Joseph Knight – Security Administrator – DSM-MEMBER-SRV
Responsible for implementing STIG controls, developing and enforcing **DSM-MEMBER-SRV_MasterCompliance.ps1**, monitoring drift, and validating compliance.

Jose Guerrero – System Administrator – INDY-AD-DC
Supports baseline security, creates remediation scripts, and monitors KQL alerts.

David Chen – Vulnerability Management Lead
Oversees Tenable Nessus scans, prioritizes remediation based on risk, and reviews vulnerability trends.

Samantha Lee – Director of Risk & Compliance
Establishes HIPAA-aligned compliance policies, reviews STIG applicability, approves exceptions, and validates audit readiness.

Alex Patel – Director of Cybersecurity Operations
Defines endpoint and identity strategy, manages EDR deployment, reviews alerts, and approves security automation.

Maria Thompson – CISO
Owns overall security posture, approves hybrid models, and is the final authority on risk acceptance.

---

4. Policy Objectives

- Maintain consistent STIG compliance on DSM-MEMBER-SRV.
- Enforce baseline security policies and encrypt sensitive data.
- Automate drift detection, remediation, and reporting using **DSM-MEMBER-SRV_MasterCompliance.ps1** and KQL scripts.
- Ensure incident response actions are executed, logged, and auditable.
- Provide documented, verifiable evidence of compliance for audit purposes.

---

5. Change Management & Enforcement Process

- OS Hardening – Firewall enabled, unnecessary services disabled, Windows Updates scheduled.
- STIG Enforcement – Password policies, account lockout policies, and auditing enabled.
- Drift Detection – Daily checks for weak passwords, disabled auditing, or unapproved admin accounts.
- Reporting – Generate compliance reports and IR logs to a centralized, secured location.
- Incident Response – Quarantine suspicious files, remove unauthorized users, notify SOC, and log all actions.
- Review and Approval – All scripts and changes must be reviewed by Alex Patel and Samantha Lee before production deployment. Critical changes require CISO sign-off.

---

6. Sign-Off

By signing below, stakeholders acknowledge and approve the change management and policy enforcement processes described above, and confirm that **DSM-MEMBER-SRV_MasterCompliance.ps1** will be used to enforce and monitor compliance.

Joseph Knight – Security Administrator
Signature: _____ Date: _____

Jose Guerrero – System Administrator
Signature: _____ Date: _____

David Chen – Vulnerability Management Lead
Signature: _____ Date: _____

Samantha Lee – Director of Risk & Compliance
Signature: _____ Date: _____

Alex Patel – Director of Cybersecurity Operations
Signature: _____ Date: _____

Maria Thompson – CISO
Signature: _____ Date: _____