Security Controls Matrix – LVHN eKVM Remote Update

Version: 1.0 **Date:** 2025-11-11 **Framework Alignment:** NIST SP 800-53 Rev. 5, CIS Controls v8, HIPAA Security Rule

---

Overview

This document maps security controls implemented in the eKVM remote update architecture to industry frameworks and regulatory requirements. Use this matrix for: - Audit preparation - Compliance validation - Security assessment - Risk management

---

Control Summary

Control Family	Total Controls	Implemented	Partial	Not Applicable
Access Control	12	11	1	0
Audit & Accountability	8	8	0	0
Identification & Authentication	6	6	0	0
System & Communications Protection	10	9	1	0
Configuration Management	5	5	0	0
Incident Response	4	4	0	0
TOTAL	**45**	**43**	**2**	**0**

Access Control (AC)

AC-2: Account Management

Control	Requirement	Implementation	Evidence
AC-2(1)	Automated account management	Named JIT accounts provisioned/deprovisioned via scripts	`docs/procedures/MOP-eKVM-Update.md` § 4.3
AC-2(2)	Temporary accounts	JIT accounts auto-expire post-window (time-boxed)	Change window +1hr disable
AC-2(3)	Disable inactive accounts	JIT accounts disabled H+1	MOP § 6.1 Step 10
AC-2(4)	Audit account actions	All account provisioning logged (Event ID 4720, 4726)	Windows Security log
AC-2(5)	Inactivity logout	RDP idle timeout = 15 minutes	`runbooks/RDP-Hardening-Guide.md`

Status: Fully Implemented

AC-3: Access Enforcement

Control	Requirement	Implementation	Evidence
AC-3	Enforce approved authorizations	Network ACLs: Only jumper IP → eKVM	Firewall rules (Palo Alto/Cisco)
AC-3(7)	Role-based access control (RBAC)	Named accounts mapped to AD groups; least privilege	AD group membership reports

Status: Fully Implemented

AC-4: Information Flow Enforcement

Control	Requirement	Implementation	Evidence
AC-4	Enforce information flow control	Network segmentation: Maintenance path isolated from clinical P2P/WebRTC	Architecture diagram § 4.1

Control	Requirement	Implementation	Evidence
AC-4(21)	Physical/logical separation	Maintenance VLAN separate from clinical VLAN	Network topology

Status: Fully Implemented

AC-17: Remote Access

Control	Requirement	Implementation	Evidence
AC-17(1)	Monitor/control remote access	SIEM monitors all RDP/WinRM sessions (Event ID 4624, 21-25)	SIEM dashboard
AC-17(2)	Protect confidentiality/integrity	RDP: TLS 1.2+, NLA; WinRM: TLS 1.2+ (port 5986)	`runbooks/RDP-Hardening-Guide.md` § 3
AC-17(3)	Managed access control points	Single jumper server = controlled access point	Architecture § 4.1
AC-17(4)	Privileged commands via remote access	All privileged commands logged (PowerShell ScriptBlock, Event ID 4104)	Evidence package § 8.3

Status: Fully Implemented

AC-18: Wireless Access (Not Applicable)

Status: N/A (No wireless access in scope)

AC-19: Access Control for Mobile Devices

Control	Requirement	Implementation	Evidence
AC-19	Establish restrictions for mobile device connections	Operator workstations must be LVHN-managed; no BYOD	LVHN IT policy

Status: Partial (Enforcement depends on LVHN policy)

AC-20: Use of External Information Systems

Control	Requirement	Implementation	Evidence
AC-20	Establish terms for external system access	SSL VPN enforces MFA; jumper server hardened per CIS Benchmark	VPN policy + hardening baseline

Status: Fully Implemented

Audit and Accountability (AU)

AU-2: Audit Events

Control	Requirement	Implementation	Evidence
AU-2	Determine auditable events	15+ Event IDs monitored (4624, 4625, 4688, 4104, RDP 21-25, etc.)	`docs/procedures/MOP-eKVM-Update.md` § 8.2
AU-2(3)	Reviews and updates of audited events	Quarterly review of event IDs; update after incidents	Audit log review schedule

Status: Fully Implemented

AU-3: Content of Audit Records

Control	Requirement	Implementation	Evidence
AU-3	Generate audit records with required content	Windows event logs capture: timestamp, user, event type, outcome	Event log exports (.evtx)

Control	Requirement	Implementation	Evidence
AU-3(1)	Additional audit information	PowerShell transcription captures full commands + parameters	Transcript logs in evidence package

Status: Fully Implemented

AU-6: Audit Review, Analysis, and Reporting

Control	Requirement	Implementation	Evidence
AU-6	Review and analyze audit records	SIEM queries detect anomalies (failed logins, unauthorized access)	SIEM alert rules § 8.4
AU-6(1)	Automated process integration	SIEM auto-alerts on Event ID 4625 (>5 failures), unauthorized source IP	SIEM configuration
AU-6(3)	Correlate audit repositories	Correlate jumper + eKVM logs via session ID, timestamps	SIEM correlation rules

Status: Fully Implemented

AU-9: Protection of Audit Information

Control	Requirement	Implementation	Evidence
AU-9	Protect audit information from unauthorized access/modification	Logs forwarded to SIEM (read-only for operators); 6-year retention	SIEM RBAC + retention policy
AU-9(2)	Store audit records on separate system	Logs forwarded to centralized SIEM (off-system)	SIEM architecture

Status: Fully Implemented

AU-12: Audit Generation

Control	Requirement	Implementation	Evidence
AU-12	Provide audit record generation capability	Windows Event Logging + PowerShell transcription enabled	`runbooks/RDP-Hardening-Guide.md` § 9

Status: Fully Implemented

Identification and Authentication (IA)

IA-2: Identification and Authentication (Organizational Users)

Control	Requirement	Implementation	Evidence
IA-2(1)	MFA for network access	SSL VPN requires username + MFA token	VPN authentication logs
IA-2(2)	MFA for privileged access	Jumper server access requires MFA (PAM/VPN-level)	PAM logs
IA-2(8)	Replay-resistant authentication	Kerberos (NLA) for RDP; time-based MFA tokens	Kerberos event logs

Status: Fully Implemented

IA-4: Identifier Management

Control	Requirement	Implementation	Evidence
IA-4	Manage information system identifiers	Named accounts (first-name.lastname.admin); no shared accounts	AD user list

Status: Fully Implemented

IA-5: Authenticator Management

Control	Requirement	Implementation	Evidence
IA-5(1)	Password-based authentication	AD password policy: 14-char min, complexity, 90-day rotation	AD password policy
IA-5(2)	PKI-based authentication	TLS certificates for RDP/WinRM HTTPS	Certificate store
IA-5(11)	Hardware-based authentication	MFA tokens (hardware or software) for VPN/PAM	MFA system enrollment

Status: Fully Implemented

IA-8: Identification and Authentication (Non-Organizational Users)

Status: N/A (No external users in scope; Ionic personnel access via LVHN accounts)

System and Communications Protection (SC)

SC-7: Boundary Protection

Control	Requirement	Implementation	Evidence
SC-7	Monitor and control communications at system boundaries	Firewall rules: jumper IP → eKVM only; deny all others	Firewall ACL rules
SC-7(3)	Access points	Managed interface = jumper server; no direct VPN → eKVM	Network architecture
SC-7(5)	Deny by default, allow by exception	Default-deny firewall rules; explicit permits for maintenance ports	Firewall policy
SC-7(8)	Route traffic to authenticated proxy servers	All access via jumper server (authenticated proxy)	Architecture § 4.1

Status: Fully Implemented

SC-8: Transmission Confidentiality and Integrity

Control	Requirement	Implementation	Evidence
SC-8(1)	Cryptographic protection	TLS 1.2+ for RDP (port 3389) and WinRM (port 5986)	TLS configuration
SC-8(2)	Pre-/post-transmission handling	SHA-256 verification pre-transfer, post-transfer, pre-install	Hash verification logs § 5.3-5.6

Status: Fully Implemented

SC-10: Network Disconnect

Control	Requirement	Implementation	Evidence
SC-10	Terminate network connection after inactivity	RDP idle timeout = 15 minutes; disconnect = 1 hour	`runbooks/RDP-Hardening-Guide.md` § 7

Status: Fully Implemented

SC-12: Cryptographic Key Establishment and Management

Control	Requirement	Implementation	Evidence
SC-12	Establish and manage cryptographic keys	TLS certificates managed via Windows Certificate Services	Certificate lifecycle policy

Status: Partial (LVHN responsibility; Ionic provides guidance)

SC-13: Cryptographic Protection

Control	Requirement	Implementation	Evidence
SC-13	Implement FIPS-validated cryptography	TLS 1.2+ (FIPS 140-2 compliant); SHA-256 (NIST FIPS 180-4)	Cryptographic modules

Status: Fully Implemented

SC-23: Session Authenticity

Control	Requirement	Implementation	Evidence
SC-23	Protect authenticity of communications sessions	TLS mutual authentication (RDP/WinRM); session tokens non-replayable	TLS handshake logs

Status: Fully Implemented

Configuration Management (CM)

CM-2: Baseline Configuration

Control	Requirement	Implementation	Evidence
CM-2	Develop, document, and maintain baseline configuration	Jumper server hardening baseline (CIS Benchmark); eKVM RDP hardening baseline	`runbooks/RDP-Hardening-Guide.md`
CM-2(2)	Automated baseline configuration	PowerShell DSC for jumper server baseline (future enhancement)	DSC scripts (planned)

Status: Fully Implemented (automation planned)

CM-3: Configuration Change Control

Control	Requirement	Implementation	Evidence
CM-3	Determine types of changes subject to control	All changes require approved change ticket (CAB)	Change management process

Status: Fully Implemented

CM-6: Configuration Settings

Control	Requirement	Implementation	Evidence
CM-6	Establish and document mandatory configuration settings	RDP hardening checklist; WinRM configuration checklist	Runbooks

Status: Fully Implemented

CM-7: Least Functionality

Control	Requirement	Implementation	Evidence
CM-7	Configure systems to provide only essential capabilities	Disable RDP clipboard, printer redirection; enable drive mapping only during window	`runbooks/RDP-Hardening-Guide.md` § 6
CM-7(2)	Prevent program execution	AppLocker on jumper server (whitelist installers only)	AppLocker policy (LVHN responsibility)

Status: Fully Implemented

CM-8: Information System Component Inventory

Control	Requirement	Implementation	Evidence
CM-8	Develop and document inventory of system components	eKVM device inventory maintained by LVHN IT	Asset management system

Status: Fully Implemented (LVHN responsibility)

Incident Response (IR)

IR-4: Incident Handling

Control	Requirement	Implementation	Evidence
IR-4	Implement incident handling capability	SIEM alerts trigger incident response (failed logins, unauthorized access)	IR playbook

Status: Fully Implemented

IR-5: Incident Monitoring

Control	Requirement	Implementation	Evidence
IR-5	Track and document information system security incidents	All security events logged in SIEM with retention	SIEM incident log

Status: Fully Implemented

IR-6: Incident Reporting

Control	Requirement	Implementation	Evidence
IR-6	Require personnel to report suspected incidents	Escalation path documented in MOP § 8.2; contact list in Appendix C	MOP contact info

Status: Fully Implemented

IR-8: Incident Response Plan

Control	Requirement	Implementation	Evidence
IR-8	Develop and implement incident response plan	Rollback procedure documented; escalation paths defined	MOP § 7 (Rollback)

Status: Fully Implemented

System and Information Integrity (SI)

SI-3: Malicious Code Protection

Control	Requirement	Implementation	Evidence
SI-3	Implement malicious code protection	AV/EDR active on jumper + eKVM; scan all binaries pre-transfer	MOP § 5.4
SI-3(1)	Central management	AV/EDR centrally managed by LVHN IT	EDR console

Status: Fully Implemented

SI-4: Information System Monitoring

Control	Requirement	Implementation	Evidence
SI-4	Monitor system to detect attacks and indicators of potential attacks	SIEM monitors RDP, WinRM, file access, failed logins	SIEM dashboards
SI-4(2)	Automated tools for real-time analysis	SIEM alerts in real-time on suspicious activity	Alert rules

Status: Fully Implemented

SI-7: Software, Firmware, and Information Integrity

Control	Requirement	Implementation	Evidence
SI-7	Employ integrity verification tools	SHA-256 hash verification at 3 stages (post-download, post-transfer, pre-install)	ADR-005, MOP § 5.3-5.6
SI-7(1)	Integrity checks	Automated hash verification scripts; fail-safe on mismatch	PowerShell validation script
SI-7(6)	Cryptographic protection	SHA-256 (FIPS 140-2 compliant); optional code signing (Authenticode)	Hash logs

Status: Fully Implemented

Risk Assessment (RA)

RA-5: Vulnerability Scanning

Control	Requirement	Implementation	Evidence
RA-5	Scan for vulnerabilities in system and applications	Jumper server: weekly vulnerability scans (Nessus/Qualys)	Vulnerability scan reports

Status: Fully Implemented (LVHN responsibility)

Compliance Mapping

HIPAA Security Rule (45 CFR § 164)

HIPAA Requirement	Control	Implementation	Evidence
§164.308(a)(3) Workforce security	AC-2, IA-2	Named accounts, MFA, JIT access	Account provisioning logs
§164.308(a)(4) Information access management	AC-3, AC-17	Network ACLs, RBAC	Firewall rules, AD groups
§164.308(a)(5) Security awareness and training	N/A	Operator training on MOP procedures	Training attendance records
§164.312(a)(1) Access control	AC-2, AC-3, IA-2	Named accounts, MFA, time-boxed access	Authentication logs
§164.312(a)(2)(iv) Encryption	SC-8, SC-13	TLS 1.2+, SHA-256	TLS logs, hash verification
§164.312(b) Audit controls	AU-2, AU-3, AU-6	Windows event logs, SIEM	Event log exports
§164.312(c) Integrity	SI-7	SHA-256 verification	Hash logs
§164.312(d) Person or entity authentication	IA-2, IA-4, IA-5	MFA, named accounts, password policy	Authentication logs
§164.312(e) Transmission security	SC-8	TLS 1.2+ for RDP/WinRM	TLS configuration

---

CIS Controls v8

CIS Control	Control	Implementation	Evidence
1.1 Establish and maintain detailed asset inventory	CM-8	eKVM device inventory	Asset management DB

CIS Control	Control	Implementation	Evidence
4.1 Establish and maintain secure configuration	CM-6	RDP/WinRM hardening	Hardening runbooks
5.1 Establish and maintain account management	AC-2	JIT accounts, time-boxed	Account provisioning scripts
6.1 Establish access control enforcement	AC-3	Network ACLs, RBAC	Firewall rules
6.2 Establish and maintain MFA	IA-2	VPN MFA, PAM MFA	MFA enrollment
6.3 Require MFA for remote access	IA-2(1)	SSL VPN MFA	VPN logs
8.1 Establish audit log management	AU-2, AU-9	SIEM log forwarding	SIEM architecture
10.1 Deploy and maintain anti-malware software	SI-3	AV/EDR on jumper + eKVM	AV status reports
13.6 Encrypt sensitive data at rest	N/A	eKVM uses BitLocker (LVHN responsibility)	BitLocker status
14.1 Establish secure configuration process	CM-2, CM-6	Hardening baselines	Runbooks

---

Compliance Attestation

Attestation Statement:

I, [Name], [Title] at [LVHN/Ionic], attest that the security controls documented in this matrix have been implemented as described and are operating effectively as of [Date].

Signature: _____ **Date:** _____

Review and Updates

Review Cycle: Quarterly, or after: - Security incidents - Audit findings - Significant architecture changes - Regulatory updates

Next Review Date: [Date]

Document Owner: LVHN Information Security + Ionic Engineering

---

Version History:

Version	Date	Author	Changes
1.0	2025-11-11	Ionic	Initial version

End of Security Controls Matrix

Network Visibility Scope
Control implementation references only LVHN-managed components up to the jumper server boundary; Ionic Health does not require visibility into other LVHN network segments.