LVHN eKVM Remote Update – Implementation Plan

Configuration Custody Notice
Ionic Health engineering exclusively manages all eKVM configuration, firmware, and software changes, including patching operations executed via the jumper server. LVHN operations is solely responsible for provisioning, hardening, and maintaining the Windows jumper server environment. Cross-domain activities require written approval from both teams.

Network Visibility Scope
Planning tasks reference only the LVHN-managed jumper server boundary and its outbound route to Ionic eKVM devices. Ionic Health does not require visibility into other LVHN network segments.

Overview

This implementation plan outlines phased activities, responsible parties, and indicative time frames needed to operationalize the LVHN jumper server pathway for Ionic Health eKVM updates. Durations are estimates expressed in weeks to leave room for joint scheduling adjustments.

Phase Structure

Phase	Objective	Estimated Duration
0	Kick-off & alignment	~1 week
1	Jumper server readiness	~2–3 weeks
2	Questionnaire validation & pre-checks	~1 week
3	Controlled rehearsal	~2 weeks
4	Pilot maintenance windows	~2–4 weeks
5	Broad rollout	~4–6 weeks
6	Closure & transition	~1 week

Phase Details

Phase 0 – Kick-off & Alignment (~1 week)

- Confirm scope boundaries: LVHN owns jumper server infrastructure; Ionic owns eKVM patch execution.
- Share documentation portal link and distribute the LVHN Jumper Server Readiness Questionnaire.
- Establish communication channels, project cadence, and escalation contacts.

Phase 1 – Jumper Server Readiness (~2–3 weeks)

- LVHN provisions Windows Server 2019/2022 with CIS/SCT hardening baseline.
- Configure SSL VPN access, MFA, and Just-in-Time AD accounts for Ionic operators.
- Implement firewall/ACL entries for outbound TCP 3389, 5985, 5986, and 443 during maintenance windows.
- Validate connectivity from jumper server to representative Ionic eKVM public IPs (Test-NetConnection scripts).

Phase 2 – Questionnaire Validation & Pre-checks (~1 week)

- LVHN completes the readiness questionnaire; Ionic reviews responses to ensure minimum operational requirements.
- Close gaps such as pending firewall requests, account creation lead times, or evidence retention expectations.
- Confirm change management tooling (ticket formats, approval workflow, evidence submission path).

Phase 3 – Controlled Rehearsal (~2 weeks)

- Execute Method of Procedure steps against a limited test device or lab eKVM.
- Verify SHA-256 hash checks, WinRM automation scripts, and logging flow to LVHN SIEM.
- Capture findings, refine runbooks, and document troubleshooting steps.

Phase 4 – Pilot Maintenance Windows (~2–4 weeks)

- Run one or more production maintenance windows targeting a small set of eKVMs (2–3 units per window).
- Collect audit evidence (transcripts, logs, hash outputs) and review with LVHN Compliance.
- Monitor latency, bandwidth, and operator workflow feedback to adjust scheduling or tooling.

Phase 5 – Broad Rollout (~4–6 weeks)

- Plan batches of up to 10 eKVMs per maintenance window, respecting LVHN change freeze periods.
- Automate repetitive tasks where approved (hash verification, evidence packaging, SIEM queries).
- Track completion status, incidents, and remediation actions across all devices.

Phase 6 – Closure & Transition (~1 week)

- Consolidate final reports, evidence bundles, and lessons learned.
- Update documentation (MOP, user manual, functional design) with improvements from rollout.
- Define ongoing maintenance cadence and support contacts for steady-state operations.

Workstream Responsibilities

Workstream	LVHN Role	Ionic Role
Infrastructure	Provision jumper server, manage VPN/MFA, enforce ACLs	Request windows, validate connectivity, report issues
Identity & Access	Create JIT accounts, enforce expirations	Use named accounts, follow change tickets, report anomalies
Security & Logging	Ensure SIEM ingestion, monitor alerts	Supply evidence, run validation queries
Change Management	Approve windows, coordinate blackout schedules	Prepare MOP, submit change tickets, close with evidence

Risk & Mitigation Snapshot

Risk	Likelihood	Impact	Mitigation
Firewall rule delays	Medium	High	Submit requests during Phase 1 with clear ports and schedule
VPN/MFA provisioning lag	Medium	Medium	Align on JIT lead time during Phase 0; pre-stage accounts
WinRM throttling or script blocks	Low	Medium	Validate antivirus exclusions; rehearse in Phase 3
Evidence gaps for compliance	Low	High	Use standardized transcript templates and SIEM queries

Change Control Considerations

- All maintenance windows must reference approved change tickets with defined start/end times.
- Evidence packages (hash logs, PowerShell transcripts, SIEM snapshots) should be attached within 24 hours of window closure.
- Emergency maintenance follows LVHN emergency change protocol and requires LVHN leadership approval.

Documentation Linkage

- `docs/procedures/MOP-eKVM-Update.md`
- `docs/procedures/User-Manual.md`
- `docs/solution/Functional-Solution-Design.md`
- `docs/proposal/LVHN-Infrastructure-Questionnaire.md`
- `specs/Technology-Stack-Specification.md`