LVHN Jumper Server Readiness Questionnaire

Document Control - **Version:** 1.1 (Lean) - **Date:** 2025-11-11 - **Classification:** Internal – Discovery Document - **Purpose:** Collect only the data required to confirm that the LVHN-managed jumper server can support Ionic Health eKVM patching. - **Return To:** Ionic Health Project Manager (email)

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

Network Visibility Scope
This questionnaire limits discovery to the LVHN-operated jumper server and its outbound connectivity toward Ionic-managed eKVM devices; no additional network details are required.

Instructions

- Please complete only the fields marked **Required**. Optional items help contextualize operations but are not mandatory.
- The questionnaire focuses on the jumper server path; Ionic-owned eKVM devices remain external to LVHN's managed network and are reached via public IP over the maintenance window.
- Return the completed form by email or the agreed secure channel.

---

1. Jumper Server Deployment (Required)

Topic	Response
Hostname / FQDN	
Physical / Virtual Location (e.g., Data Center A)	
Windows Server Version (2019/2022)	
Build Level / Patch Status (latest CU applied?)	
Hardening Baseline Applied (CIS, SCT, other)	
Local Admin Contact (name / email)	
Backup / Snapshot capability available? (Yes/No)	

1.1 Out-of-Band Access (Optional)

Topic	Response
Remote management tool (e.g., ILO, DRAC)	
Emergency console process	

---

2. Connectivity Path (Required)

Topic	Response
How do Ionic operators reach the jumper server? (Select)	

☐ SSL VPN (preferred)

☐ Dedicated network access

☐ Other (describe)

Topic	Response
VPN / Access URL or Gateway	
Authentication Method (AD, SAML, RADIUS)	
MFA Provider (Duo, Microsoft Authenticator, other)	
Can the jumper server reach the public IP of Ionic eKVM devices over the Internet during the maintenance window? (Yes/No)	
Firewall or ACL change needed to allow outbound TCP 3389 / 5985 / 5986 / 443? (Yes/No)	
Contact for scheduling firewall updates (name/email/phone)	

2.1 Connectivity Validation (Optional)

Validation Item	Status
Test-NetConnection from jumper to sample eKVM IP (RDP port)	
Proxy required for outbound HTTPS? (Yes/No + details)	

---

3. Identity & Access (Required)

Topic	Response
Directory Service providing credentials (e.g., LVHN Active Directory domain)	
Process to request Just-In-Time accounts for Ionic (change ticket, portal, email)	
Minimum lead time to create / enable accounts (hours)	
Account expiry policy after window (auto-disable H+1, manual, other)	
PAM in use? (Yes/No – only if credentials must be checked out)	

3.1 Logging & Monitoring (Optional)

Topic	Response
Windows Event logs forwarded to SIEM? (Yes/No)	
SIEM contact (email)	

---

4. Maintenance Window Logistics (Required)

Topic	Response
Change Management System (ServiceNow, Cherwell, other)	
Standard maintenance window days/times	
Minimum notice required to schedule a window (days)	
Primary change approver (name / role / email)	
On-call contact during window (name / phone)	

4.1 Evidence Handling (Optional)

Topic	Response
Preferred method to receive execution evidence (email, ticket attachment, SharePoint)	
Required retention period for evidence (days)	

---

5. Additional Notes (Optional)

Free-text space for any constraints, planned upgrades, or known blackout periods relevant to the jumper server or VPN path.

---

6. Approvals

Role	Name	Signature/Date
LVHN IT Operations		
LVHN Security / Compliance		
Ionic Health Project Manager		