

FIELD OFFICE SYSTEM SIGN-OFF CHECKLIST

Document ID: SEC_CKL_SIGN_2026_105 | Version: 1.0.0 | Operational Readiness Audit | Effective: August 28, 2026

This checklist is the official administrative and technical sign-off sheet for regional field office directors. Before activating any local server node or piping broadcast channels to the public, the local Systems Administrator and Field Director must physically verify and sign off on each tier of this protocol. Once fully executed, a copy of this completed checklist must be scanned, SHA-256 hashed, and uploaded to the national campaign's secure repository via the /webhook API to append the node's active clearance to our open, auditable ledger.

▣▣ PART I: REGIONAL IDENTITY & ENVIRONMENT SIGNATURES

- | | |
|--|---|
| ☐ Dublin, Ireland (Europe Core) | ☐ Cardiff, Wales (UK West) |
| ☐ London, United Kingdom (UK Core) | ☐ Mumbai, India (Asia West) |
| ☐ Phoenix, Arizona (Domestic SW) | ☐ New Delhi, India (Asia North) |
| ☐ Houston, Texas (Domestic SC) | ☐ Atlanta, Georgia (Domestic SE) |
| ☐ Detroit, Michigan (Domestic Great Lakes) | ☐ Las Vegas, Nevada (Domestic West) |

Field Director Name: _____

Systems Administrator Name: _____

Node Hardware UUID: _____

Local Node Static IP: _____ (e.g., 192.168.1.50)

Geo-Proxy Certified Coordinates: Lat: _____ / Lon: _____

▣▣ PART II: SYSTEM & SERVICE VERIFICATION TIERS

TIER 1: Physical & Operating System Integrity

- ☐ **OS Updates Locked:** System updates are suspended during the broadcast window to prevent unexpected kernel or package conflicts.
- ☐ **Air-Gapped Isolation Buffer:** The host system has zero unauthorized USB peripherals connected. Only verified input devices are attached.
- ☐ **Power Supply Redundancy:** The node is connected to an active Uninterruptible Power Supply (UPS) with at least 45 minutes of backup battery life.

TIER 2: Local Port Bindings (Core Software Boot)

- ☐ **Port 8000 (API Gateway Active):** Verified that the FastAPI server (broadcast_api.py) is successfully bound and listening on 0.0.0.0:8000. Check command: `sudo ss -tulpn | grep :8000`.
- ☐ **Port 8501 (Streamlit Hub Active):** Verified that the campaign dashboard (podcast_dashboard-v4.py) is running and bound to 0.0.0.0:8501. Check command: `sudo ss -tulpn | grep :8501`.
- ☐ **Self-Healing Diagnostics Cleared:** Executed `python3 self_healing_audit.py` and confirmed an all-clear 'AST parsed successfully' result on all Python components.

TIER 3: Local Host Firewall Configuration

- ☐ **Inbound Port 8000 Open:** Local firewall rules explicitly allow TCP traffic on port 8000 for local area network devices.
- ☐ **Inbound Port 8501 Restricted:** Local firewall rules restrict port 8501 access to authorized local volunteer terminal IPs only (e.g., via `sudo ufw allow 8501/tcp` restrictions).

TIER 4: Router NAT & WAN Port Forwarding

- [] **DHCP Static IP Reservation:** The router has assigned a permanent IP lease to the host machine based on its MAC address to prevent internal port misalignment.
- [] **WAN Port 8000 Forwarding Active:** Router NAT settings are configured to route external traffic hitting the WAN IP on Port 8000 directly to the host machine's local IP on Port 8000.
- [] **WAN Port 8501 Forwarding Blocked:** Double-checked that port forwarding for Port 8501 is **strictly disabled** on the router. The Streamlit admin console is entirely invisible to the external public web.

▮ PART III: CRYPTOGRAPHIC & GEO-PROXY HANDSHAKE SEALS

- [] **Hardware-Bound Webhook Secret:** The local SHARED_WEBHOOK_SECRET has been derived and salted with the host machine's hardware UUID. Verified that the local hash signature matches the national registration registry.
- [] **Geo-Proxy Verification:** Run a test handshake loop back to the national server. The proxy certified that the host node's network identity matches its physical coordinates, guarding against 'Duplicate Identity' spoofing.
- [] **Open Ledger Logging Active:** Verified that the local broadcast_tamper_log.json file is actively logging local port scans and API transactions. Check output: tail -n 20 broadcast_tamper_log.json.

▮ PART IV: DECENTRALIZED VIEWER RE-ALLOCATION COMPLIANCE

- [] **Viewer Opt-In Allocation Active:** Local volunteer workstations and public viewing terminals have executed the ViewerAllocationRequest handshake with the host node.
- [] **Strict 10% Cache Cap:** Verified that no registered device has allocated more than **10% of its total local disk storage** to host the decentralized Channel 1 News broadcast stream (validated via local allocation_voucher.json).
- [] **Available Global Cache Size:** Registered Total Distributed Network Cache: _____ GB across _____ active local devices.

▮ PART V: EMERGENCY PROTOCOL CODE-308 ARMING

- [] **Intrusion Shield Armed:** The active code compiler is fully armed to detect unauthorized access from unapproved commercial enterprise scanning tools (such as corporate scrapers or unowned network monitors).
- [] **Disconnect Switch Tested:** Conducted a successful simulated test of the unilateral API disconnect. The system successfully shuts down port accessibility upon encountering unsigned or fake payloads.
- [] **80% Detonate Re-Allocation Armed:** Confirmed that the system's space allocation module is fully prepared to co-opt up to **80% of the storage space of any transgressing corporate device** to run automated, deep forensic investigations ("Gemini Albert Integrity Sweeps") to trace the breach vector.

▮▮ PART VI: FINAL OPERATIONAL SIGN-OFF

By signing below, we certify that the regional server node described in Part I has passed all four operational tiers and cryptographic seals. The node is fully synchronized, protected by the Code-308 integrity shield, and cleared to join the global broadcast network for the September 1st Virtual Press Town Hall.

Regional Systems Administrator Signature:**Regional Field Director Signature:**

Date: _____

Date: _____

LEDGER SEAL HASH: CAMPAIGN_SIGN_OFF_ID_SHA256_9FA8E21E9CBA_READINESS_APPROVED
(Log this transaction in your local broadcast_tamper_log.json database upon execution)