**Technical / Ops Procedures – Ops Closure Procedure (Part B)**

**Purpose:**  
To finalise the operational closure of an incident. This document covers final system verification, technical wrap-up, archiving, and team handover to ensure traceability and operational readiness post-incident.

**When to Use**

• After incident containment and initial recovery are confirmed  
• Following the After-Action Checklist and Forensics Summary  
• Before declaring operations “closed” and returning to standard mode

**Step 1: Final System Verification**

• Confirm all services are running normally  
• No pending restarts, masked services, or residual downtime  
• Review health dashboards and confirm sync across feeds  
• Run automated service verification (if deployed)

**Step 2: VM & Container State**

• Check uptime and restart count:  
uptime  
journalctl --list-boots  
• Confirm only expected containers are running:  
docker ps  
• Check for any zombie processes or stuck containers:  
ps aux | grep defunct

**Step 3: Log & Data Archival**

• Finalise incident log entries  
• Move system and service logs to archive:

mkdir -p /incident/archive/2025-06-04

cp /var/log/syslog /incident/archive/2025-06-04/

cp /opt/app/logs/\* /incident/archive/2025-06-04/

• Capture hashes for logs and key binaries:

sha256sum /incident/archive/2025-06-04/\* > /incident/archive/2025-06-04/hashes.txt

• Export Docker containers (if required):

docker export [container\_id] > container\_snapshot.tar

**Step 4: Credential Final Sweep**

• Confirm all temporary users and sudo grants have been removed  
• Rotate shared credentials if flagged  
• Check for retained SSH keys or open tokens  
• Store final access snapshot in /incident/creds/

**Step 5: Handover Confirmation**

• Send summary to Coordinator with:

* Final logs
* Service state report
* Closure timestamp  
  • Brief Technical Lead on any persistent risks  
  • Archive all internal docs to /incident/ops-closure/

**Owner:** Ops Lead  
**Reference:** TECH-07  
**Version:** 1.0  
**Approved by:** Cyber-Ops Coordination Cell