**Technical / Ops Procedures – Technical Containment Guide**

**Purpose:**  
To guide technical responders in identifying, isolating, and containing threats or anomalies within a live operational environment. This guide ensures containment actions align with system integrity, legal boundaries, and escalation procedures.

**When to Use**

* Anomalous behaviour is detected (e.g. signal spoofing, log inconsistencies, unexpected cron jobs)
* Security indicators suggest unauthorised access or persistence
* Service degradation appears linked to internal systems or VM-based infrastructure

**General Containment Principles**

* Containment does **not** equal resolution — aim to stop spread or limit damage
* Avoid making permanent changes unless directed by Ops or Legal
* Record all actions taken in a structured log (timestamp + action + system)
* Do not delete files, restart hosts, or isolate systems from the network unless explicitly authorised

**Immediate Actions by VM Type**

**🖥️ Core Infrastructure VMs (e.g. AIS Aggregator, Scheduler, Container Planner)**

* SSH into the machine: ssh admin@[vm-name] (credentials provided separately)
* Check system status:
* top
* journalctl -xe
* df -h
* du -sh /opt/\*
* Review key logs:
* tail -n 100 /var/log/syslog
* grep -i error /opt/app/logs/planner.log
* journalctl -u scheduler.service --since "1 hour ago"
* Stop only affected services:
* systemctl stop planner.service
* kill -9 [pid] # if service is unresponsive
* Collect logs for evidence:
* cp /opt/app/logs/planner.log /var/log/evidence/planner-incident.log
* sha256sum /opt/app/logs/planner.log > /var/log/evidence/planner.log.hash
* Store notes: /var/log/incident/containment-[YYYYMMDD-HHMM].txt

**🌐 Vendor Gateway VM**

* View-only access permitted. Do **not** restart or stop services.
* Logs located at: /var/vendor/logs/gateway.log
* Sample inspection:
* tail -n 50 /var/vendor/logs/gateway.log
* grep -i connect /var/vendor/logs/gateway.log
* stat /usr/bin/gatewayd
* Report any anomalies immediately via Coordinator — do **not** modify files or settings.

**📡 Communications / GPS VM**

* Monitor traffic:
* ss -tunap
* tcpdump -i eth0 port not 22 -c 100
* netstat -tnp
* Check DNS, routing, and external connections:
* cat /etc/resolv.conf
* dig example.com
* route -n
* Isolate network (with authorisation only):
* ifconfig eth0 down

**⚙️ Physical Ops / Sensor Feed VM**

* Identify and stop containers:
* docker ps
* docker stop [container\_id]
* docker inspect [container\_id] > /var/log/dumps/container-[id].json
* Review container logs:
* docker logs [container\_id] | tail -n 100
* Review disk usage and file changes:
* find /opt/sensors/ -type f -mtime -1
* ls -lt /tmp/

**Red Flags Requiring Immediate Escalation**

* Unexpected cron entries:
* crontab -l
* cat /etc/cron.\*/\*
* Suspicious binaries or file changes:
* find / -type f -name "\*sh" -exec stat {} \;
* md5sum /usr/bin/ssh
* Cross-VM traffic or log evidence of lateral movement
* Services running from non-standard paths (e.g. /tmp/, /dev/shm/)

**Communication & Coordination**

* Log all containment actions in the team channel and incident log
* Tag actions with urgency (#containment, #forensics, #approval-needed)
* Validate vendor boundaries: **do not breach service terms** even under pressure
* Escalate prior to deleting or isolating persistent threats

**Owner:** Technical Lead  
**Reference:** TECH-01  
**Version:** 1.1  
**Approved by:** Cyber-Ops Coordination Cell