**Technical / Ops Procedures – Node Isolation Procedure**

**Purpose:**  
To provide step-by-step instructions for isolating compromised or anomalous nodes (VMs or containers) within the Southgate Maritime environment. This procedure ensures threats are contained without triggering unnecessary operational outages.

**When to Use**

* Suspicious activity or compromise is confirmed or strongly suspected on a system
* Persistence mechanisms (e.g. hidden cron jobs, altered binaries) are found
* Lateral movement or unauthorised access between VMs is detected

**Pre-Isolation Checklist**

* Confirm isolation need with Technical Lead or Incident Coordinator
* Identify system owner and assess operational impact
* Capture key logs and evidence before action:
* cp /var/log/syslog /var/log/evidence/syslog-$(date +%F-%H%M).log
* tar -czf /var/log/evidence/service-logs.tar.gz /opt/app/logs/
* sha256sum /var/log/evidence/\*.log
* Alert Coordinator and update team log

**Isolation Techniques**

**1. Container Isolation**

* Stop individual containers:
* docker ps
* docker stop [container\_id]
* docker export [container\_id] > /var/log/evidence/container-[id].tar
* Remove from auto-restart:
* docker update --restart=no [container\_id]

**2. Service-Level Isolation**

* Stop suspicious service:
* systemctl stop [servicename]
* systemctl disable [servicename]
* Prevent restart (masking):
* systemctl mask [servicename]

**3. VM Network Isolation**

* Disconnect VM network interface (requires elevated rights):
* sudo ip link set eth0 down
* # or
* sudo nmcli connection down "Wired connection 1"
* Confirm interface state:
* ip a | grep DOWN
* Optional: block outbound traffic using UFW
* sudo ufw deny out from any to any

**Post-Isolation Actions**

* Log all actions in incident log with timestamps
* Notify relevant stakeholder group (e.g. vendor, legal)
* Continue passive monitoring:
  + Watch syslog, cron, container state
  + Use journalctl -f, docker logs, or auditctl if enabled

**Do Not:**

* Delete any binaries, logs, or user data
* Wipe systems without Legal authorisation
* Restart isolated systems without group consensus

**Owner:** Technical Lead  
**Reference:** TECH-03  
**Version:** 1.0  
**Approved by:** Cyber-Ops Coordination Cell