

SOUTHGATE TERMINAL

Port Operations Security Documentation

Technical / Ops Procedures – Ops After-Action Checklist

Purpose:

To provide a structured, operations-focused checklist for reviewing system and service recovery post-incident. Ensures all components have returned to expected baseline and that lessons learned are captured for future resilience.

When to Use

- After incident has been contained or resolved
- During the technical and operational debrief phase
- Prior to formal incident closure and report finalisation

Phase 1: System Recovery Confirmation

- Core services restarted and stable (e.g. AIS Aggregator, Planning Engine)
- Confirmed service uptime with:
systemctl status [servicename]
- All containers active and healthy:
docker ps
docker inspect [container_id] | grep -i health
- Cron jobs verified — no unexpected entries:
crontab -l
cat /etc/cron.*/*
- System time/NTP resynchronised:
timedatectl status

Phase 2: Log Review & Residual Tracing

- Final service logs checked for lingering errors:
tail -n 100 /opt/app/logs/*.log
grep -i fail /var/log/syslog
- No evidence of reactivated persistence mechanisms
- Clean shutdown and restart history:
last reboot
journalctl --since "1 hour ago" | grep -i shutdown

- Confirm log rotation and no tampering of evidence logs

Phase 3: Access & Credential Verification

- No new user accounts unexpectedly present:
`cat /etc/passwd | tail`
- SSH key directories clean and known:
`ls -la ~/.ssh/`
- Rotate shared/system credentials if any compromise suspected
- Review privileged access events:
`cat /var/log/auth.log | grep sudo`

Phase 4: Internal Ops Debrief

- Short summary of what worked / failed operationally
- Flag any systems requiring patch or rebuild
- Confirm alignment with Incident Log timeline
- Note any open issues for Coordinator follow-up

Storage & Reporting:

Submit completed checklist with incident closure documentation

Store digital copy in shared /incident/ops-review/ folder

Hash checklist and attach to forensics archive if required

Owner: Ops Lead

Reference: TECH-05

Version: 1.0

Approved by: Cyber-Ops Coordination Cell