**Technical / Ops Procedures – Signal Anomaly Response**

**Purpose:**  
To guide technical teams through the identification, investigation, and response process when signal-based anomalies (e.g. GPS spoofing, AIS manipulation, phantom traffic) are detected within maritime operational environments.

**When to Use**

* Unexpected or conflicting signal data is detected (location, vessel ID, or timing mismatch)
* Reports from on-site Ops or dashboards show movement discrepancies
* Logs or monitoring tools show anomalies in feed sources (e.g. spoofed coordinates, missing timestamps)

**Signal Architecture Context**

* AIS and GPS data are ingested via:
  + Serial or USB interfaces (e.g. /dev/ttyUSB0)
  + Network streams (UDP port 10110 or 2947)
* Signal processing is performed in:
  + AIS Collector container or service
  + GPSD daemon running on the Comms VM
* Reference data and known vessel IDs stored in /opt/reference/gps-clean.nmea and /opt/reference/ais-index.json

**Immediate Detection Actions**

* Validate real-time signal input:
* cat /dev/ttyUSB0 | tee /tmp/raw-nmea.log
* netstat -anu | grep 10110
* Cross-reference feeds:
  + AIS: /opt/ais/logs/ais-feed.log
  + GPS: /var/gps/raw-feed.nmea
* grep -i lat /opt/ais/logs/ais-feed.log | tail -n 20
* tail -n 50 /var/gps/raw-feed.nmea
* diff /var/gps/raw-feed.nmea /opt/reference/gps-clean.nmea
* Check for ghost or duplicate MMSI entries:
* grep "MMSI" /opt/ais/logs/ais-feed.log | sort | uniq -c | sort -nr

**Feed Validation Techniques**

* Use gpsdecode or gpspipe (if installed):
* gpspipe -r | tee /tmp/gpspipe.log
* gpsdecode < /tmp/gpspipe.log
* Inspect NTP time sync drift:
* timedatectl status
* Confirm AIS format consistency:
* grep -v '^!' /opt/ais/logs/ais-feed.log

**Network Traffic Inspection**

* Monitor incoming signal traffic:
* tcpdump -i any port 10110 -n -c 100
* netstat -tunap | grep 10110
* Use nc (netcat) to test signal port:
* nc -vu localhost 10110
* Capture entire session for later review:
* tcpdump -i any port 10110 -w /var/log/evidence/ais-signal.pcap

**Anomaly Classification & Evidence Collection**

* Classify:
  + Position drift beyond expected margins
  + Ghost signals (phantom vessels)
  + Duplicate or malformed NMEA sentences
  + Out-of-order signal bursts
* Preserve evidence:
* cp /var/gps/raw-feed.nmea /var/log/evidence/gps-anomaly-$(date +%F-%H%M).nmea
* sha256sum /var/log/evidence/\*.nmea
* docker export ais\_collector > /var/log/evidence/ais\_collector\_snapshot.tar

**Red Flags & Escalation**

Immediately escalate to Incident Lead and Legal if:

* Feeds originate from unknown internal IPs
* AIS data contains duplicate MMSI with divergent paths
* Timestamped feeds do not match system or NTP time
* Container or script found manipulating NMEA before logging

**Owner:** Technical Lead  
**Reference:** TECH-02  
**Version:** 1.1  
**Approved by:** Cyber-Ops Coordination Cell