CONTENTS

SECURITY

1. SHIP SECURITY PROCEDURES

1.1. Scope

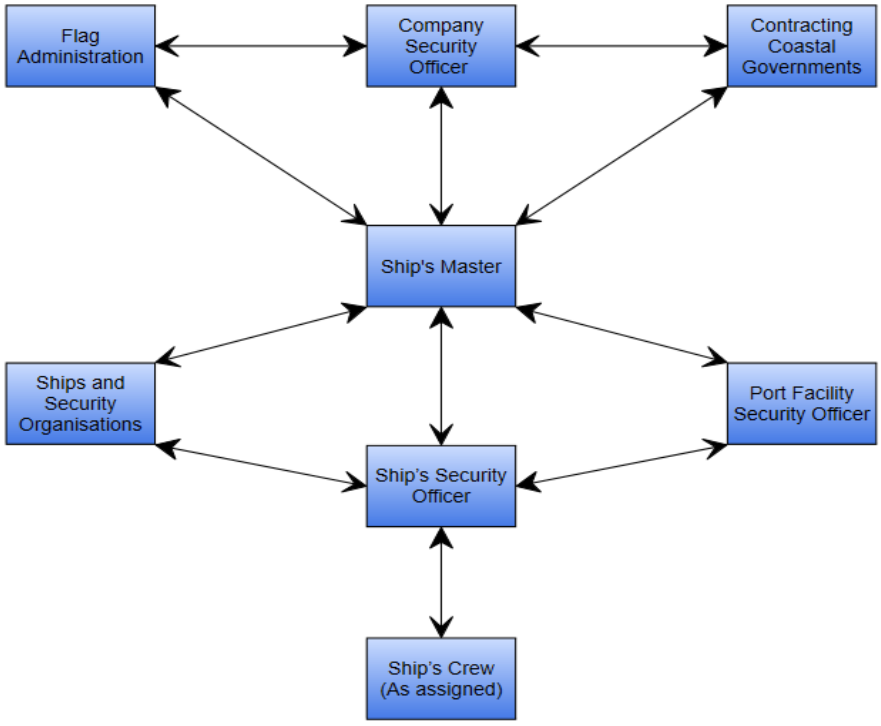
The scope is to establish responsibilities and guidelines for the security procedures[1] on board the Company's Fleet of vessels. The Company Security and Anti-Piracy Policy statement can be found in the Policy Manual Section 1.5.

1.2. Code

ISM
ISPS

2. COMPANY SECURITY ORGANISATION

2.1. Security Responsibilities Organigram



[1] W 18 / 2019

2.2. Masters Overriding Authority

The Master has the overriding authority and responsibility to make decisions regarding the security of the ship and to request the assistance of the Company or of any Contracting Government or any other party as may be necessary.

2.3. Identity Cards

The Company will issue each crewmember with an identity card, which must be presented when joining or boarding the vessel. Due to the relatively small size of the ship's complement existing crewmembers are known to each other and therefore are not required to present their identity card.

Company personnel are provided with Company Identity Cards which must be presented when joining or boarding a vessel.

3. COMPANY SECURITY OFFICER (CSO)

3.1. Company Security Officer's Duties

Refer to Officer Procedures Manual section 4.5.

3.2. Appointment of the CSO

The Company Security Officer has the responsibility and authority delegated by the company for ensuring that security requirements are implemented and maintained within the Company, pertaining to the Fleet.[2]

The company shall appoint an alternative person within senior management to assume the role of Acting CSO if necessary.

3.3. Qualifications

The CSO is required to have attended a course approved by the Administration.

4. SHIP SECURITY OFFICER (SSO)

4.1. Ship Security Officer's Duties

Refer to SSP.

[2] W 09 / 2024

4.2. Appointment of the SSO

Chief Officer is appointed as a Ship Security Officer (SSO) on company vessels, who shall be suitably qualified for performing the duties of SSO.

4.3. Qualifications

The Chief Officer & Master is required to have attended an SSO course approved by the Administration. If for whatever reason Chief Officer on board has not attended an approved course, the Company may appoint the Master as Ships Security Officer if he has attended the course.

5. SHIP SECURITY PLAN IMPLEMENTATION

5.1. Introduction

It is the responsibility of the Company Security Officer (CSO) to ensure that a Ship Security Plan (SSP), unique to each ship, has been prepared and placed on board. The plan is developed based on guidance provided by the International Maritime Organisation (IMO) through the ISPS Code, Recognized Security Organization and the administration. Amendments to the SSP are carried out by the CSO.

The Administration must approve the plan and any subsequent changes that are made to the plan. A Ship Security Plan is not generally subject to inspection by officers authorised by Contracting Government. However, if there are grounds for believing the ship is in violation of the requirements, access to the plan is authorised for the purpose of verifying that ship security requirements have been met and, if necessary, to require appropriate corrective actions.

In preparation of the SSP, a Ship Security Assessment (SSA) is conducted, which examines existing physical security measures, procedures, and operations. A vulnerability assessment is completed to determine potential gaps or weaknesses in security. Details are contained in the SSA which is a confidential document separately maintained in a locked cabinet.

The point of contact for the Ship Security Plan on board the ship is the Master or Ship Security Officer, and for the Company is the Company Security Officer.

5.2. Establishing and Setting Security Levels

The ISPS Code makes provision for three Security Levels, which reflect the likelihood that a security incident will occur; the higher the Security Level the greater the likelihood of a security incident, namely:

a. **Security Level 1** - The level for which minimum appropriate protective security measures shall be maintained at all times;

b. **Security Level 2** - The level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident; and

c. **Security Level 3** - The level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

The Company will keep the Master advised of Security Level changes made by the administration. Whenever level 2 or 3 is set by the administration, the ship must acknowledge receipt of the instruction on change of the Security Level to the CSO. A ship must comply with and operate at the Security Level set by Flag State at all times, unless the port state is operating at a higher security level. If a port's Security Level is higher than the Security Level set by Flag State, the Flag State[3] / CSO and company safety email[4] must be informed and the ship must increase its Security Level to match that of the port for the duration of its call.

Singapore flag – notify the change of security level at MPA's emails: marine@mpa.gov.sg and isps@mpa.gov.sg

Hong Kong flag – notify the change of security level at email: mms@mardep.gov.hk [5]

Liberia flag - notify the change of security level at email: security@liscr.com [6]

Malta flag - notify the change of security level at email: comms.isps@transport.gov.mt [7]

Marshall Island flag doesn't require notification from the ship on the change of security level by Master, but issues Ship Security Advisory recommending raising the security level II or III in certain countries depending upon the threat level for which relevant Ship Security Advisory from the flag should be referred.[8]

All ships are required to raise the security level II in ports as required by relevant USCG Port Security Advisory and comply with the actions when visiting these countries provided in it. Failure to properly implement the actions listed in the Advisory may result in delay or denial of entry into the United States.[9]

[3] W 18 / 2019
[4] W 09 / 2024
[5] W 09 / 2024
[6] W 09 / 2024
[7] W 09 / 2024
[8] W 24 / 2022
[9] W 24 / 2022

When potential increased security threats are identified the Master in liaison with the SSO may at his discretion enhance existing security measures or raise the Security Level appropriately. The CSO must be informed.

Ships must ensure revised measures as may be required by an ordered security level change are fully implemented within 12 hours. Security level 3 (probable or imminent and specific threat) will likely involve a government response and revised measures may have to be in place in less than 12 hours if the ship is to continue operating.

It is important that Security Levels be clearly defined for all personnel. Training should be conducted at all readiness conditions to ensure rapid response to changing threats.

5.3. Document Retention

Records of security activities referred to in the ISPS Code, Part A, Section 10 shall be kept on board by the SSO for a period of 3 years.

These records are regarded as “restricted” and should be kept in the direct custody of the SSO or Master on board, and by the CSO ashore, to prevent unauthorised access or disclosure. Restricted records must be available for inspection when requested by the Flag State.

Officers of contracting governments (Port State, USCG etc) can only request to see parts of the plan if the officer of a contracting government has clear grounds to believe the ship is not in compliance with the ISPS code.

Reviews of the SSP are confidential and should be retained on board (but not filed with the SSP) and ashore for a period of three years. The reviews are to be accorded the same level of security and protection against unauthorised access and disclosure as the actual SSP itself.

6. OPERATIONS IN HIGH RISK AREAS

6.1. High Risk Areas

6.1.1. In specific areas the threat of acts of piracy, armed robbery and other violent crimes involving violence against vessels is significantly increased, including:

a. West coast of Africa in the region of the Gulf of Guinea, the area off the coasts of Ghana, Nigeria, Togo, Cameroon, and Benin;

b. South-east Asia and the South China Sea, particularly in the vicinity of the Malacca Strait;

c. East coast of Africa from the Red Sea to the northern Mozambique Channel, particularly in the Horn of Africa region incorporating the Gulf of Aden and the coast of Somalia.

d. The Celebes Sea / Sulu Sea / Off Sibutu Island, Tawi Tawi, Philippines[10]

6.1.2. Vessels operating in such areas must exercise additional security precautions and extra vigilance in accordance with recommendations from the administration and other relevant organisations. The Company Security Officer (CSO) is responsible for updating ships within the fleet on the situation in high risk areas after reviewing the information from various sources i.e. MSCHOA, NATO Shipping Centre, flag states, regional and local etc and for advising them of the necessary countermeasures to be taken.

6.2. Crew Briefing

Crew is to be briefed by Master and SSO prior entering piracy Voluntary Reporting Area (VRA) / High Risk area (HRA) with specific reference to:

a. The increased security and hardening measures

b. Security drill for pirate attack

c. Accommodation, steering gear, machinery space and stores securing procedure and escape in case of emergency set out and practiced.

d. Familiarity with ships alarms in case of pirate attack; the piracy alarm shall be distinctive to avoid confusion with Emergency Alarm Signal

e. Safe muster point designated within the steering gear room or accommodation space in case of pirate attack

f. Personnel's responsibilities and duties;

g. Reference the Ship's Security Plan;

h. Security exercise to ensure lock down and personnel retreat to safe location as designated (steering gear room, strong room or citadel if constructed)

i. Delegate an officer to maintain discipline and calm;

j. Ensure mechanical integrity of ME to ensure MCR can be maintained throughout;

k. Reminding crew of the dangers of posting voyage related information on social media.[11]

6.3. Additional Security Measures in Port

6.3.1. Minimise access points to a single controlled gangway or accommodation ladder.

6.3.2. Keep emergency ladders clear of the water; raise and stow pilot ladders immediately after use.

[10] W 24 / 2022
[11] W 24 / 2022

6.3.3. Search all deliveries when possible; conduct frequent, random, and overt searches if all materials cannot be examined.

6.3.4. Increased frequency of search of visitors.

6.3.5. Keep small craft in the vicinity under constant surveillance.

6.3.6. Carefully control documents containing information about the cargo or ship's itinerary.

6.3.7. Restrict access to the accommodation to a single access on the main / A / first poop deck.

6.3.8. Conduct a search of the ship before sailing.

6.4. Ship Protection Measures at Sea

6.4.1. When approaching or sailing through high-risk areas:

a. Test SSAS & communication equipment prior entering **piracy** VRA / HRA. Inform office for SSAS test.

b. Plan route to avoid the area if possible; if entering HRA, screen shot of ECDIS passage plan to be sent to company for approval clearly indicating distance from land (as per insurance requirements)[12]

c. Do not anchor or drift in or near ports where attacks are known to have taken place. Rather announce the vessels arrival with Port Authorities and remain underway well-off shore or adjust the vessels speed and ETA to avoid anchoring;

d. Augment bridge watches and lookouts, use of night vision optics;

e. Keep a lookout and radar watch for small craft;

f. When monitoring nearby ships, give additional attention to small craft that match the speed of own ship or travelling parallel to the ship;

g. Maintain radio communications with appropriate shore and naval authorities;

h. Controlled access to accommodation, machinery spaces and store rooms should be set out and practiced. Limit access to the accommodation in daylight hours through one door which to be locked during dark. Access to the accommodation limited to one unlocked wheelhouse door during dark;

i. All doors and hatches providing access to the bridge, accommodation, steering gear and machinery spaces should be properly secured to prevent

[12] W 46 / 2018

them being opened by pirates ensuring these openings can be easily opened by crew in case of emergency escape is required;

j. Rigging the physical barrier razor wires and or spikes around vessel; send photo of the rigged barriers to company.[13]

k. Confirm vessels fire pump are on line and available

l. Hoses are to be securely rigged at the ship's side rails from the mid ship area aft such that they can be operated remotely. The hose stream should be on or close to jet and pointing overboard, alongside and downwards to impede small craft coming alongside (usually amidships) and transferring personnel;

m. Where possible no maintenance should be carried out on the vessel's sea water systems whilst on passage in the High Risk Area. Note that in order to utilise all pumps additional power may be required and therefore these systems should also be ready for immediate use.

n. Dummies should be lashed to prominent points to provide extra deterrent by creating the appearance of crew manning the rails

o. Blocking or lifting external ladders on the accommodation block to prevent their use, and to restrict external access to the bridge.

p. Tools and equipment that may be of use to the pirates should be stored in a secure location.

q. Pre-planned response messages should be available at the GMDSS station for easy reference and rapid transmission

r. Monitor Navtex and Inmarsat- C navigational warnings

s. Pirates detect and target vessels by sight and by the use of AIS. Therefore, limit the use of lighting at night and reduce the power or turn off AIS. Unfortunately, this has a major drawback in that it may reduce the likelihood of an intervention by "friendly forces" if attacked. Consequently, AIS must be switched on immediately if the ship is boarded.

t. Make regular use of the search lights fitted to the bridge wings to sweep the area adjacent to the ship

u. Useful contact details Annex A of BMP5 along with company emergency contact details are posted on bridge, ECR and steering gear room for transit of Somalia Piracy area.

Similarly, MDAT-GoG Contact details as provided in Annex A of BMP West Africa[14] along with company emergency contact details are posted on Bridge, ECR and Steering Gear Room for transit of Gulf of Guinea / West Coast Africa VRA[15].

[13] W 46 / 2018
[14] W 24 / 2022
[15] W 24 / 2022

v. Keep the following in steering gear compartment or strong room/citadel if constructed prior transiting HRA:[16]

- 3 days rations (items like Biscuits, dry provisions etc which do not perish and can be returned back to store after 3 days)
- Sufficient blankets
- Torches
- Drinking Water
- At least 2 walkie talkies with battery charger to alert nearby ships

6.5. Piracy Attack

6.5.1. If a suspicious ship or small craft at sea approaches in a threatening manner:

a. Increase speed and alter course if safe to do so;

b. Do not allow the ship or small craft to come alongside; do not respond to messages by radio, light, or hailing;

c. Initiate the ship's pre-prepared emergency procedures;

d. At night, switch off the weather deck lighting; direct searchlights at the approaching ship / small craft;

e. Start fire pump and direct water jets over the sides;

f. Sound the emergency alarm and make a 'Pirate Attack' announcement in accordance with the Ship's Emergency Plan.

g. In Somalia piracy area, report the attack immediately to UKMTO (+44 2392 222060[17]). UKMTO is the primary point of contact during an attack but MSCHOA acts as a back-up contact point.

h. In West Coast Africa/Gulf of Guinea, report the attack immediately to MDAT-GoG by telephone **+33 298 228888** and email **watchkeepers@mdat-gog.org**[18]

i. Activate the Ship Security Alert System (SSAS). Make a 'Mayday' call on VHF Ch. 16

j. Send a distress message via the Digital Selective Calling system (DSC) and Inmarsat-C

k. Ensure that the Automatic Identification System (AIS) is switched ON.

l. Activate water spray and other appropriate self-defensive measures

[16] W 46 / 2018
[17] W 46 / 2018
[18] W 24 / 2022

m. Ensure that all external doors and, where possible, internal public rooms and cabins, are fully secured.

n. All crew, except those required on the bridge or in the engine room, should muster at the Safe Muster Point or Strong room / Citadel if constructed.

o. Check Vessel Data Recorder (VDR) is recording and the data saved.[19]

6.5.2. In addition to the emergency alarms and announcements for the benefit of the vessel's crew sound the ship's whistle/foghorn continuously to demonstrate to any potential attacker that the ship is aware of the attack and is reacting to it.

6.6. Attack Stage

Reconfirm that all ship's personnel are in a position of safety.

Report the attack immediately to UKMTO or MDAT-GoG as applicable.[20]

As the pirates close in on the vessel, Masters should commence small alterations of helm whilst maintaining speed to deter skiffs from lying alongside the vessel in preparation for a boarding attempt. These manoeuvres will create additional wash to impede the operation of the skiffs.

Substantial amounts of helm are not recommended, as these are likely to significantly reduce a vessel's speed.

6.7. If Pirates Take Control

6.7.1. Try to remain calm.

6.7.2. All crew evacuate to strong room or citadel if constructed

6.7.3. Before the pirates gain access to the bridge, inform UKMTO or MDAT-GoG as applicable. Ensure that the SSAS has been activated, and ensure that the AIS is switched on.

6.7.4. Offer no resistance to the pirates once they reach the bridge. Once on the bridge the pirates are likely to be aggressive, highly agitated, and possibly under the influence of drugs.

6.7.5. If the bridge/engine room is to be evacuated the main engine should be stopped and all way taken off the vessel if possible (and if navigationally safe to do so). All remaining crew members should proceed to the designated Safe Muster Point (if no citadel) with their hands visible.

[19] W 24 / 2022
[20] W 24 / 2022

6.8. Sources of information

6.8.1. Information, recommendations and updates on piracy and armed robbery, and countermeasures, can be obtained from the following organisations:

a. United Kingdom Maritime Traffic Operation (UKMTO) (**www.ukmto.org**)[21]

b. Maritime Safety Corridor Horn of Africa (MSC-HOA) (**www.mschoa.org**)[22]

c. International Maritime Bureau (IMB)

d. Regional Cooperation Agreement Against Piracy in South-east Asia (RECAAP)

e. NATO Shipping Centre

f. The Maritime Domain Awareness for Trade-Gulf of Guinea (MDAT-GoG) (https://gog-mdat.org/home)[23]

6.8.2. The Company Security Officer is responsible for ensuring that the latest security-related information received in circulars from the Flag State, International Maritime Organization (IMO) and above sources is conveyed to vessels in the fleet.

7. OPERATIONS ON THE SOMALIA HIGH RISK AREA

7.1. Boundaries of the High-Risk Area

7.1.1. Best Management Practices for Protection Against Somalia Based Piracy (BMP5) defines areas as following[24]:

Geographical area[25]

The geography of the region is diverse and ranges from narrow choke points such as the Bab el Mandeb (BAM) Straits and the Strait of Hormuz to the wide-open ocean of the Somali basin. Each area presents different challenges and threats will vary.

Voluntary Reporting Area[26]

The UKMTO Voluntary Reporting Area (VRA) is identified on maritime security charts such as UKHO Q6099. Ships entering and operating within the VRA are encouraged to register with the UKMTO. Registration establishes direct contact between the reporting ship and UKMTO.

[21] W 24 / 2022
[22] W 24 / 2022
[23] W 24 / 2022
[24] W 24 / 2022
[25] W 24 / 2022
[26] W 24 / 2022

A **High-Risk Area (HRA)**[27] is an industry defined area within the VRA where it is considered that a higher risk of attack exists, and additional security requirements may be necessary. The HRA is outlined on maritime security chart Q6099. It is important the latest information on current threats is used when planning routes through the HRA. Ships should be prepared to deviate from their planned route at short notice to avoid threats highlighted by navigation warnings or by military forces.

7.1.2. .

7.1.3. Many attacks have taken place beyond the extremities of the High-Risk Area and the Company Security Officer (CSO) should liaise with the administration and relevant organisations to ensure that the latest information concerning the threat of pirate attack is made available to the Master and Ship Security Officer (SSO) of any ship operating in or near this region.

7.1.4. Within the Gulf of Aden region, ships should make use of the Maritime Safety Corridor provided by international naval forces for monitoring and escort.

7.2. Route Planning

Vessel route planning is to be conducted while transiting the HRA. Planning will take into account latest piracy attacks and information, sea and wind condition, armed security guards on board, considering that South West monsoon considerably reduces the chances of piracy in Arabian Sea. CSO will provide latest piracy information to master obtained from MSCHOA, NATO websites and other sources. Chart Q6099 Anti-Piracy Planning Chart – Red Sea, Gulf of Aden and Arabian Sea is to be maintained on board. The Maritime Security Transit Corridor (MSTC) which consists of following is to be used for transiting the Gulf of Aden and a small area of Red Sea:[28]

- The Internationally Recommended Transit Corridor (IRTC), an established transit corridor in the Gulf of Aden where naval forces focus their counter piracy patrols. [29]
- The BAM TSS and the TSS West of the Hanish Islands.[30]
- A two-way route directly connecting the IRTC and the BAM TSS.[31]

7.3. Risk Assessment

The risk assessment specific to ship and voyage shall be carried out prior transiting the HRA to assess the likely hood and consequences of the piracy attack based on the latest piracy

[27] W 24 / 2022
[28] W 46 / 2018
[29] W 46 / 2018
[30] W 46 / 2018
[31] W 46 / 2018

information. The CSO and Master shall have the combined responsibility to produce a voyage risk assessment.[32]

The risk assessment shall include:[33]

- Highlighting areas of increased threat to the vessel (HRA)
- Identifying methods often used by pirates in these areas and vulnerable areas where pirates could board
- The ships characteristics including handling and general arrangement
- Military or official organisation cooperation and reporting requirements
- Existing guidelines and information sources
- Ship and Company procedures, communication and chain of command.

Some of the factors to be considered are freeboard, speed of vessel, state of sea, armed security guards and presence of naval ships in the area while safety of crew is prime. Risk Assessment shall identify measures for prevention, mitigation and recovery. Ship hardening measures shall be implemented in accordance with the result of risk assessment. Risk Assessment shall be reviewed regularly during the transit of HRA.

The Company shall implement appropriate measures to meet the threat of piracy by adopting IMO and other industry recommended practices suitable for the circumstances of the voyage and ship type.[34]

7.4. Ship Security Measures

7.4.1. In addition to the usual security measures for high risk areas, as stated in Section 6.4 additional counter-piracy measures will include:

a. Use of armed security personnel;

b. Travelling in convoy with other vessels, preferably under naval escort depending upon the prevalent piracy situation at the time of transit;

c. Increasing speed to maximum and changing course frequently;

d. Blacking out all external lighting at night, provided it is considered safe to do so;

7.4.2. Further recommendations are given in the latest version of Best Management Practices for Protection Against Somalia Based Piracy (BMP5).

7.5. Reporting Procedure for Transiting the Somalia Piracy area (VRA/HRA)

[32] W 22 / 2023
[33] W 22 / 2023
[34] W 22 / 2023

In line with BMP5 and Flag States requirement, company requires Master to report to Naval/Military forces of their transit in Somalia HRA & VRA. In order Naval/Military forces are aware of vessel's route and may respond in emergency (it may not be possible at some areas due to large distances involved in Somalia Piracy Area), Master is required to notify UKMTO prior entering UKMTO Voluntary Reporting Area – an area bounded by Suez to the North, 10°S and 78°E includes Arabian Gulf, refer Chart Q6099 for boundary[35].

Master is required to register the vessel with MSCHOA using website www.mschoa.org or by sending the updated Vessel Movement Registration form at email: postmaster@mschoa.org prior entering the area bounded by the Strait of Hormuz and Suez to the North, 10S and 78E. MSCHOA confirms the receipt of the vessel's registration.

Following position reports as per format provided in BMP5, Annex D[36] are required to be sent to UKMTO at email: watchkeepers@ukmto.org[37]. All reporting messages are to be copied at company's common email: technical@grindrodshipman.com[38]

a. Initial Report (upon entering the VRA or departure port)
b. Daily Reports,
c. Final Report (upon departure from the VRA or arrival in port).

8. PROTECTION AGAINST PIRACY IN THE GULF OF GUINEA/WEST AFRICA[39]

Best Management Practices to Deter Piracy and Enhance Maritime Security off the Coast of West Africa including the Gulf of Guinea (BMP West Africa)'' aims to help ships plan their voyage and to detect, avoid, deter, delay and report attacks. BMP West Africa is[40] provided in Regs4ships under Anti-Piracy Measures section.

8.1. Introduction

The Gulf of Guinea the pirate business model falls into three categories; cargo theft, armed robbery and kidnapping. For the cargo theft which is applicable for tankers, part a ship loaded with the cargo of Gasoil or Gasoline is hijacked from the STS transfer area for few days and cargo is transferred to a smaller ship. The armed robbery normally occurs while the vessel is approaching, drifting or anchored off ports to take valuables from safe, IT equipment and personal effects. Crew members are kidnapped and taken ashore for ransom.

8.2. Piracy Area coverage

[35] W 09 / 2024
[36] W 24 / 2022
[37] W 24 / 2022
[38] W 24 / 2022
[39] W 24 / 2022
[40] W 24 / 2022

The recommended practices and procedures for vessels operating in the Voluntary Reporting Area is depicted on UKHO Chart Q6114. Attacks on ships and seafarers have taken place throughout the region but most predominantly in the eastern part of the Gulf of Guinea. Threats are dynamic, the latest information should be sought before entering in the region.

The MDAT-GoG Voluntary Reporting Area (VRA) is identified on maritime security chart **UKHO Q6114.** Ships entering and operating within the VRA are required to register with the MDAT-GoG as registration establishes direct contact between the reporting ship and MDAT-GoG. [41]

8.3. Risk Assessment

Voyage and ship specific Risk Assessment is required to be conducted prior entering the Voluntary Reporting Area (VRA) to identify suitable measures of preventing and mitigation of the piracy including recovery procedures in case of piracy. Risk assessment will take into account prevailing piracy threat, ship characteristics, vulnerability and capability to withstand the threat. Shipboard preparation to counter threat by installing hardening measures around vessel, ship board preparedness measure to counter the attack, drills, additional watches, decision making process and reporting vessel's movement to MDAT-GoG.

8.4. Ship Movement Reporting

Marine Domain Awareness for Trade – Gulf of Guinea (MDAT-GoG) is a service operated by the French and UK navies from centers in Brest, France, and in Portsmouth, England and aims to develop, maintain and share details of the maritime domain picture of the waters off Africa's western seaboard. The MDAT-GoG administers a Voluntary Reporting Area (VRA) scheme under which merchant vessels are encouraged to report position information while operating in the VRA. The VRA as shown on Admiralty Chart Q6114 which is to be carried on board the vessel.

While vessel operating in VRA, following vessel movement is to be reported to MDATGoG at email: watchkeepers@mdat-gog.org using MDAT-GoG Reporting Forms/Format provided in BMP West Africa[42].

Initial Report: On entering the VRA
Daily Position Report: Daily ship's position, course and speed[43]
Final Report: On departing the VRA
Reports of suspicious/irregular activity: when necessary[44]

8.5. Ship Protection Measures

[41] W 24 / 2022
[42] W 24 / 2022
[43] W 24 / 2022
[44] W 24 / 2022

In additional to ship protection measures as indicated in section 6.4, Company will arrange armed/unarmed security guards as and when permitted and feasible.

Where possible Master to avoid waiting and slow steaming in HRA. If drifting or waiting is required, do so more than 250NM from the coast

Where possible minimize use of VHF, use email or phone instead

Anti-piracy watches are to be maintained while vessel is at anchor or drifting. Hawse pipe cover in place and no ladder hanging over side.

8.6. Piracy or Armed Robbery Attacks[45]

In the event of a suspicious approach, or if in any doubt, call MDAT-GoG without delay. Report the attack immediately to MDAT-GoG by telephone **+33 298 228888** and email watchkeepers@mdat-gog.org

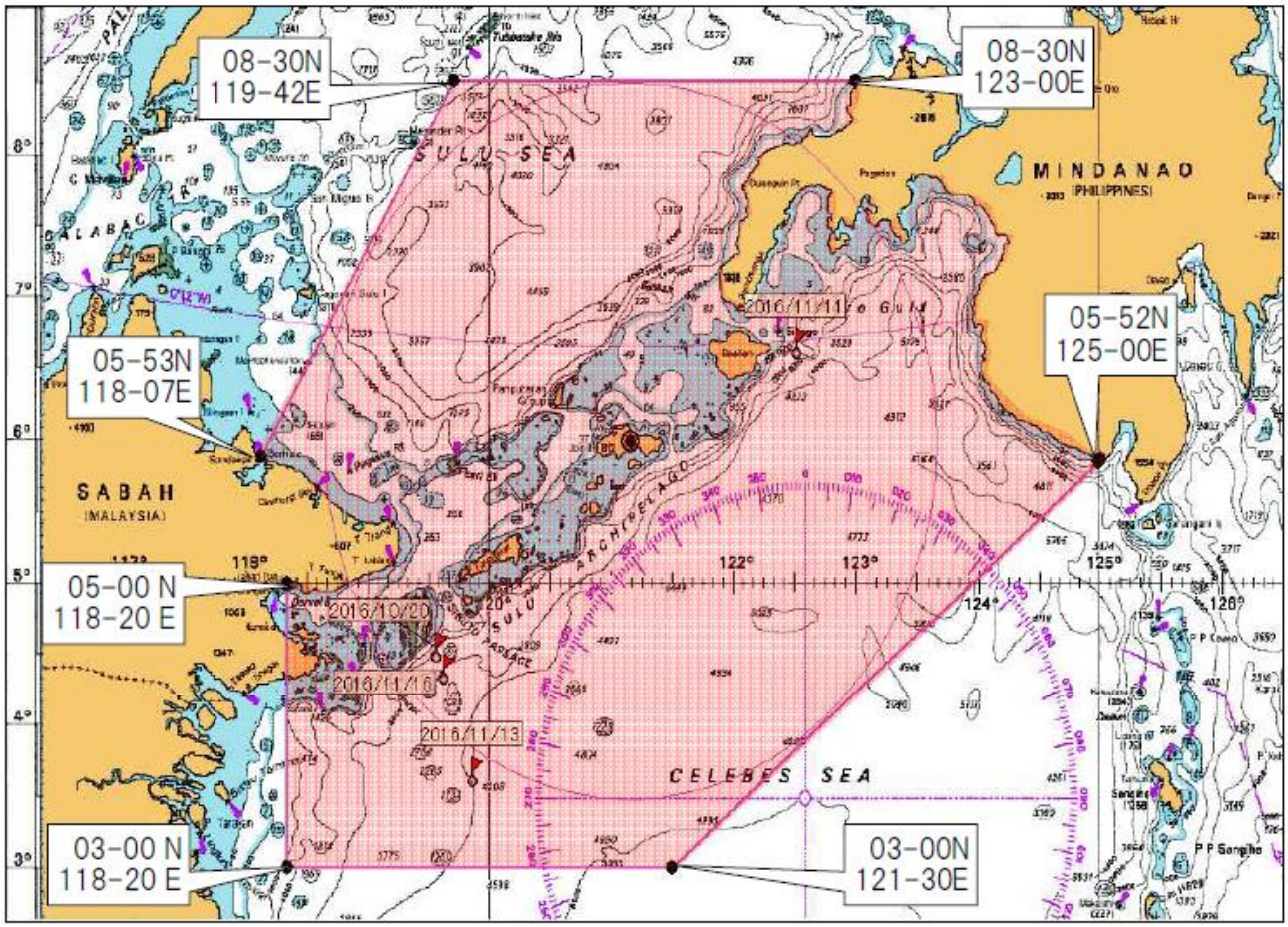
Follow the steps provided in section 6.5 Piracy attack.

[45] W 24 / 2022

9. HIGH RISH AREA - THE CELEBES SEA / SULU SEA / OFF SIBUTU ISLAND, TAWI TAWI, PHILIPPINES (REFERENCE: MALAYSIA NOTICE T MARINERS NTM 14 OF 2017)

9.1. MAP – High risk area – Celebes Sea and Sulu Sea

High-risk area
(Celebes Sea and Sulu Sea)



9.2. Areas that have a High Potential for Piracy Attacks in the High Risk Area

Each area has been designated based on locations where piracy incidents have been reported recently.

a. South of a straight line between latitude 05-53N, longitude 118-07E and latitude 08-30N, longitude 119-42E and latitude 08-30N, longitude 123-00E.

b. North of a straight line between latitude 05-00N, longitude 118-20E and latitude 03-00N, longitude 118-20E and latitude 03-00N, longitude 121-30E and latitude 05-52N, longitude 125-00E.

9.3. Routing

Routes in high-risk areas need to be selected with caution. The master should assess the risks and manage the risk by considering the latest piracy incidents and proper routing. Transit corridors / sea lanes, bound within following coordinates were set by three countries for easy monitoring and patrol. All ships are requested to navigate along with this transit corridor as far as practical.

Point ID	Lattitude	Longitude
15	04 – 23 16.0N	119 – 35 00.0E
23	05 – 04 35.0N	119 – 35 02.0E
24	05 – 04 35.0N	119 – 42 00.0E
18	05 – 19 00.0N	119 – 28 37.0E
19	05 – 25 04.0N	119 – 28 37.0E
20	05 – 52 36.0N	118 – 49 51.9E
21	05 – 52 36.0N	119 – 47 06.0E
22	05 – 07 45.0N	119 – 35 02.0E
25	05 – 56 30.0N	119 – 56 00.0E
26	06 – 05 08.0N	120 – 05 38.5E

Point ID	Lattitude	Longitude
1	06 – 09 15.8N	119 – 59 46.0E
2	05 – 59 36.0N	119 – 48 59.0E
3	05 – 59 36.0N	118 – 27 08.3E
4	05 – 21 00.0N	119 – 21 30.0E
5	04 – 44 59.0N	118 – 56 30.0E
6	04 – 03 30.0N	118 – 56 30.0E
9	03 – 56 30.0N	118 – 56 30.0E
16	03 – 59 14.0N	119 – 00 30.0E
17	04 – 39 43.0N	119 – 00 30.0E
7	04 – 03 00.0N	118 – 27 21.5E
8	03 – 56 00.0N	118 – 22 30.0E
10	03 – 44 12.5N	118 – 38 46.8E
11	03 – 39 48.6N	118 – 44 51.1E
12	04 – 52 45.7N	120 – 30 00.0E
13	05 – 01 16.7N	120 – 30 00.0E
14	04 – 28 08.0N	119 – 42 00.0E

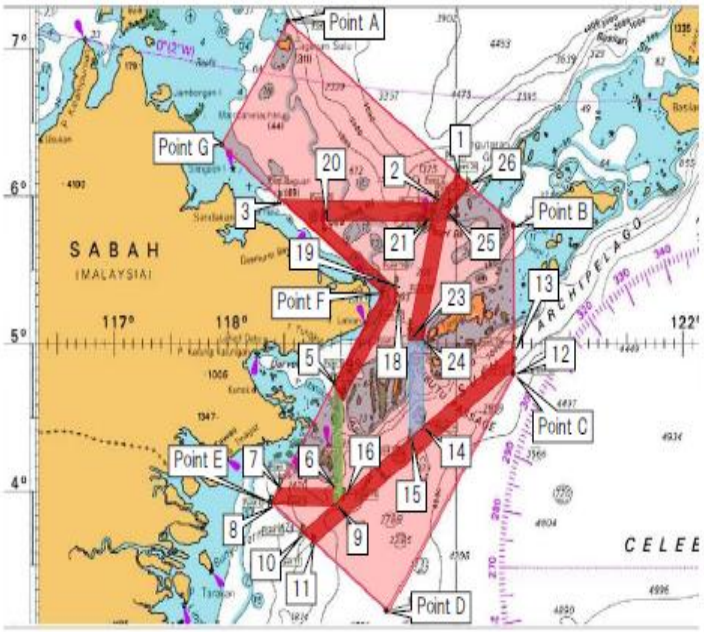
9.4. DMA and Reporting

9.4.1. Designated Maritime Area (DMA)

POINT	LATITUDE	LONGITUDE
A	07 – 11 00N	118 – 32 00E
B	05 – 48 00E	120 – 30 00E
C	04 – 48 00N	120 – 30 00E
D	03 – 11 33N	119 – 23 52E
E	03 – 56 00N	118 – 22 30E
F	05 – 21 00N	119 – 21 30E
G	06 – 21 00N	117 – 57 00E

DMA & Transit Corridors for Commercial Shipping

(Refer to MALAYSIA Notice to Mariners NTM 14 OF 2017)



【LEGEND】

: Designated Maritime Area

: Transit Corridors for Commercial Shipping

: Sibutu Passage

: Alice Channel

9.4.2. Contact Details of Patrol Agency

All vessels are required to render report to below agencies at least 24 hours before arrival at the designated maritime areas with complete ships routing information.

Vessel to send message to 9 agencies (12 email address).

AGENCY	EMAIL	PHONE
National Coast Watch Center (NCWC)	ncwatchcenter@gmail.com	+63(2)2413104
Naval Operation Center (NOC), Philippine Navy	noc@nav.ph hpn.noc@navy.mil.ph	+63(917)8512708 +63(2)5244981
Coast Guard Action Center (CGAC), Philippine Coast Guard	cgac@coastguard.gov.ph	+63(917)7243682 +63(2)5273877
Naval Force Western Mindanao Operation Center	nfwm.nfoc@navy.mil.ph nfoc.wm@gmail.com	+63(917)6860681
Maritime Research Information Center (MRIC)	mric@nav.ph	+63(917)7085248 +63(2)8431833

AGENCY	EMAIL	PHONE
Maritime Command Center (MCC), Tawau MALAYSIA	mcctawau2@gmail.com	+6089 775600 +6089 779777 +6089 982623 (1700-0800)
Eastern Sabah Security Command (ESSCOM) Malaysia	bilikqerakan_esscom@jpm.gov.my	+6089 863181
Marine Department Malaysia, Sabah Region	aisjlsbh@marine.gov.my	+6088 401111
Maritime Command Center (MCC), Tarakan INDONESIA	mcctarakan2@gmail.com mcc_tarakan@tnial.mid.id	+625513806288 +625513806289

9.4.3. Reporting

All vessels passing the Designated Maritime Area (DMA) are required to render reports to Philippines, Malaysia and Indonesia Patrol Agencies as per below.

- Registration

  At least 24 hours before entering the DMA.

- Initial Report

  Vessel should report initial report upon entering the DMA.

- Position Report

  Vessel should report position report at least every 24 hours in the DMA.

- Final Report

- Vessel should report final report after clearing the DMA.

9.4.4. Reporting Items

Vessel Name, Vessel Flag, Call Sign, Position with Time (UTC), Course, Speed, Name of sea lane, Status (I.E. Underway / All is well / under attack or in Distress etc)

9.5. Countermeasures prior entering the Celebes sea and Sulu sea HRA

- Company to be informed
- Measures as per BMP5 (AS APPLICABLE) shall be complied with.
- Razor wires/ barbed wires/ spikes shall be rigged.
- Passage Plan shall include entry and exit date / time and position in DMA
- SSAS shall be tested prior entry in DMA.
- All communications shall be tested (SATC / VSAT / FBB – Phone as well as email.)
- Don't anchor or drift in the area.

10. SECURITY INCIDENTS

10.1. Investigating and Reporting Security Incidents

10.1.1. A breach in security or a threat to security should be investigated on-board as soon as practically possible to determine how security measures were circumvented or nearly circumvented and possible target/objectives.

10.1.2. Preventive action measures should be identified and implement as practical to prevent any further occurrence. This must be promptly reported in detail to the Company Security Officer.

10.1.3. The CSO will review all Security Incident Reports and will conduct further investigation if this is deemed necessary. The CSO will close-out the reports when any necessary action has been taken.

10.2. Internal Reporting

10.2.1. Security incidents involving a breach in security or threat in security should be reported to the CSO using the "Security Incident Report" form. A serious breach of security resulting in death, lost time injury or serious damage to the ship should be reported to the Company within 24 hours.

10.2.2. Reports must be limited to a factual and objective account of the incident or threat and opinions must not be expressed.

10.2.3. If the shore facility security has been inadequate and contributed to the breach in security the Master must report it to the Port Facility Security Officer (PFSO) and to the CSO, who will in turn report to the Port Authorities, Coastal State Authorities and Flag State as appropriate regarding the problems encountered.

10.3. Reporting to the Flag Administration

10.3.1. The Administration is responsible for the monitoring of security incidents and occurrences that could adversely affect maritime security and has an interest in the investigation of the circumstances surrounding the incident and the remedial activity required.

10.3.2. Any incident where it is suspected that the intended purpose was to endanger the ship's crew or the vessel, and that further action should be initiated, must be reported to the CSO and Administration immediately. In all other cases such occurrences need only be recorded and reported to the CSO.

10.3.3. The types of incident that must be reported to the Administration include:

a. Media aware incidents

b. Bomb warnings

c. Discovery of firearms and ammunition

d. Discovery of explosives

e. Hijack

f. Discovery of weapons other than firearms, and items that could endanger the security of the port facility, a ship within the port facility, ship and port facility personnel, staff and crew, such as knives, volatile fluids etc.

10.4. Summary of Reporting Requirements

Any security incident or breach of security shall be immediately reported to CSO/Company. Company will report to flag state as applicable.[46]

10.5. Reporting of piracy-related incidents in the High-Risk Area

Following any piracy attack or suspicious activity, a detailed report of the event should immediately be submitted by the Master to UKMTO and MSCHO, using the form in the annexure to BMP. The report should contain descriptions and distinguishing features of any suspicious vessels that were observed, to assist in establishing a full analysis of trends in piracy activity and to enable assessment of piracy techniques or changes in tactics, in

[46] W 09 / 2024

addition to ensuring that appropriate warnings can be issued to other Merchant shipping in the vicinity.

11. USE OF ARMED GUARDS ON VESSEL

Based on the risk assessment of the HRA transit area, company will engage the services of the armed guards (Privately Contracted Armed Security Personnel, PCASP).[47]

However, armed guards/PCASP presence does not replace existing self-protective measures and procedures as provided in the latest BMP including safe routing and safe speed.[48]

The Master is to advise the DPA/CSO and company with the following information[49]:

i. Port and date of embarkation.

ii. Entry into VRA[50]/HRA.

iii. Exit out of VRA[51]/HRA.

iv. Port and date of disembarkation.

v. Number of crew on board and lifeboat capacity.

This information is required to be submitted by the office to Flag state[52] by the DPA/CSO[53] for obtaining the flag state's approval for carrying arms on board the vessel[54]. Thereafter the Vessel is separately to submit by means of electronic submission the particulars of the Security Personnel.

Ship safety familiarization of the PCASP is to be conducted upon their boarding using Contractor Safety Checklist Form 3.3.2.[55]

The armed guards, who are sailing on board the ship, are to be reported to the flag state as per the requirement of the relevant flag state.[56]

11.1. Relationship Between Master and PMSC/PCASP and PCASP's duties [57]

At all times the Master remains in command and retains the overriding authority on board.

Master shall be involved in all the decision-making process by the PMSC/PCASP.

In the event of any actual or perceived threat of piracy, the Team Leader of the PCASP shall advise the Master or OOW (in the Master's absence) that he intends to invoke the Rules for the Use of Force.

---

[47] W 18 / 2019
[48] W 18 / 2019
[49] W 09 / 2024
[50] W 18 / 2019
[51] W 18 / 2019
[52] W 18 / 2019
[53] W 18 / 2019
[54] W 09 / 2024
[55] W 18 / 2019
[56] W 29 / 2024
[57] W 18 / 2019

Master retains the authority to order the PCASP to cease firing under all circumstances without compromising the PCASP's right of self-defence in accordance with the applicable law.

The owner, the charterer, the company, the PMSC /PCASP or any other person shall not prevent or restrict the master of the ship from taking or executing any decision which, in the master's professional judgment, is necessary for safety of life at sea and protection of the marine environment.

The engagement of the armed guards on board is as one of the primary layer of defence against piracy and to act upon lawful instructions of the Master during the transit.

The duties of the armed guards on board are provided in the contract agreed between company and PMSC. The contract should be referred in this regard.

In general, armed guards shall assist in:

- the implementation of self-protective measures and hardening of the vessel
- carrying out on board security assessment and advise master
- conducting the security drills/training with crew for preparing the vessel for the transit in agreement with master
- maintaining watch for monitoring suspicious vessels or craft during the transit

11.2. Flag state's Laws on the Carriage of Arms[58]

Flag state's laws[59] normally do not prohibit the carriage of arms on board ships. However, this does not exempt a person on board from criminal liability in respect of any offence that he commits on the ship. Even though the crew of a ship, or their hired security personnel, may lawfully bear arms, the ship owner, manager and private maritime security company (PMSC) should be aware that the bearer of the firearms will still be liable under flag state's laws[60] if the firearm is used on board the ship without lawful excuse.

11.3. Carriage of Firearms On-Board Ships Entering Port

PMSC and the PCASP embarked on board the vessel should be aware that the carriage of firearms on board ships is also subject to the laws and regulations of the Coastal/Port State in whose territorial sea and/or ports the ship is sailing in or entering. Some Coastal/Port States may have laws prohibiting the carriage of arms on board ships entering into their territorial sea or ports. The requirements pertaining to the carriage of firearms on board ships

[58] W 09 / 2024
[59] W 09 / 2024
[60] W 09 / 2024

entering port can be found as below in most of the cases. However, port requirement should be obtained from agent before entering in the port.[61]

i. The owner, agent, master or person-in charge of a ship may require the person on board who possesses arms or explosives to deposit or place the arms and explosives in an approved strong-room or safe on board the ship and to keep the arms and explosives there until the ship leaves the port.

ii. The strong-room must be approved by port state[62]

iii. In the event that there is no strong-room or safe on board the ship that meets port requirements, the arms and explosives are to be deposited/stored in the armoury ashore as per the port requirement. The arms and explosives are to be delivered back to the ship before departure.[63]

11.4. Lifesaving Appliances

Carriage of armed security personnel should not exceed the lifesaving appliances capacity, in particular the lifeboat capacity. Crewing department is to be informed in advance if few crew members need to be disembarked prior embarkation of security personnel.

11.5. Rules for the Use of Force[64]

Under no circumstances are the crew of the vessel to handle or discharge the weapons which have been placed onboard the vessel as per the requirement of the PCASP onboard. Crew members found to have handled weapons will be subject to disciplinary action and may be dismissed.

Following guidance is to be observed with regard to use of force.

- The purpose of the Privately Contracted Armed Security Personnel (PCASP) is exclusively for the protection of life of persons on board and the ship from armed pirate attacks.
- Private Maritime Security Company (PMSC) should provide a detailed graduated response plan to the master to a pirate attack as part of their teams' operational procedures.
- Firearms will be used in line with Internationally-recognised Rules for The Use of Force which shall be advised to the Master by the Team Leader prior to or at the start of the Transit or as soon thereafter as is practical

[61] W 09 / 2024
[62] W 09 / 2024
[63] W 09 / 2024
[64] W 18 / 2019

- Master shall review the Rules For The Use of Force with the Team Leader and shall confirm the review and their understanding of the Rules For The Use of Force in writing
- Firearms should only be handled by armed guards and are at no time to be handled or utilised by the master or the vessel's crew
- The intended use of Firearms is for the purpose of non-lethal force in the defending of the vessel and its crew from the threat of attack.
- A warning is to be given by PCASP prior to use of firearms
- The option to discharge any Firearm remains with the master of the vessel at all times and any suggestion to the master to use lethal force would only be considered when all other alternatives have been exhausted and should be used as a last resort.
- While using force, care should be taken to minimize damage and injury and preserve human life.
- Ensure all incidents involving the use of weapons and armed force are reported at the earliest instance to the Flag State and the Company Security Officer (CSO).

11.6. Reporting and Record Keeping for the Use of Firearms[65]

The Master shall maintain a log of every circumstances in which firearms are discharged, whether accidental or deliberate or test firing. Such actions should be fully documented in sufficient detail in order to produce a formal written record of the incident.

In the event, it becomes necessary to use force by the PCASP, the team leader should be advised to photograph (if appropriate), log, report and collate written statements from all persons present at the incident in anticipation of legal proceedings.

11.7. Test Firing of the Firearms[66]

Test firing of the firearms is allowed only at sea after office approval and risk assessment. On tankers, the location selected is to be in gas safe area preferably at bridge wing and hot work permit shall be completed. Shots are to be fired in upward direction towards sea away from the ship's structure and away from the gas hazardous area. PCASP should don proper PPE. The ship staff are well clear from the area designated for test firing.

11.8. Inventory of Firearms[67]

The port authority, customs or regional coast guard authority as applicable in the relevant jurisdiction will require the information of firearms on board.

[65] W 18 / 2019
[66] W 18 / 2019
[67] W 18 / 2019

Security personnel should provide complete inventory of all firearms, ammunition and security equipment available upon arrival aboard the ship (inventory should detail make, model, calibre, serial number and company end-user certificate and proof of purchase of all firearms and accessories; and details of ammunition natures and amount).

The inventory should be reconciled on disembarkation of all firearms and ammunition from the ship.

11.9. Storage of Firearms[68]

The firearms, ammunition and security equipment should be kept locked in the appropriate container except when in use.
The local requirement for the storage should be complied when in port. Some states may require firearms, ammunition and security equipment transferred ashore for depositing in the armoury of the local police or other authority and deliver back upon departure.
Depending upon the local requirement, some states may require firearms, ammunition and security equipment transferred to a separate compartment on board and sealed during port stay.

12. STOWAWAYS[69]

Before arrival in port all non-essential lockers and compartments are to be sealed with company security seals. Crew are to be briefed on reporting any persons acting suspiciously activities aboard, finding of broken seals and stowaway paraphernalia aboard. Any persons not involved in operations noted aboard are to be challenged as to their purpose aboard.

A stowaway search is to be carried out on departure port where stowaways are likely, using the ship specific checklist covering all areas of the vessel assigned to respective crew members. All areas of the vessel are to be included in the checklist. Some of the likely hiding spaces are cargo hold vent trunking, air duct spaces, funnel interiors and funnel exhaust deck, empty drums, garbage receptacles, deck stores, rudder casing and spurling pipe etc. Each crew member is responsible for searching area assigned to him and his cabin. The result of the stowaways' search is to be entered in the deck logbook.

Company will employ shore watchmen to assist crew to prevent stowaways on board in high-risk port. All access points – hawse pipe, mooring ropes, gangway and offshore side are to be monitored.

Refer Ship Security Plan for detailed precautions, preventive measures, response and reporting procedures on discovery of stowaways. Refer contingency plan manual for the action to be taken on discovery of the stowaways.

[68] W 18 / 2019
[69] W 49 / 2022

The immediate action on stowaway discovery is to report to the company and port agents, passing all available information.

The stowaways are to be treated humanely with periodic dated photographs of the stowaways' quarters, and the stowaways themselves as evidence until they are disembarked from the vessel.