SHIP SECURITY PLAN (SSP)

Each ship shall carry on-board a SSP having been approved by the Administration or Bureau Veritas acting as a Recognized Security Organization (RSO) on behalf of the Administration.

This SSP shall be developed by the company, or by Bureau Veritas (in that case, the approval of the SSP cannot be carried out by Bureau Veritas), mainly based on the conclusions of the Ship Security Assessment.

It is to be noted that the SSP is generally not subject to inspection by Port State Control (PSC) officers. However, if there are grounds to believe that the ship is not in compliance with the applicable security regulations, limited access to the specific sections of the plan relating to the specific non-compliance raised by the PSC may be carried out with the agreement of the ship's master or of the Flag State.

To ease the preparation of the SSP you will find below a suggested SSP content, which must than be adapted to individual ship. You will find development of the suggested SSP in sections One to Four. Section Five - Ship Security Assessment - will be presented in a separate document. Further sections will only be presented through the table of content.

Note: In Section Two – Plans, procedures and controls, the proposed security measures are examples extracted from the NVIC 10 02 – US Coast Guard.

Suggested standard Ship Security Plan (SSP) content

I) Introduction

I-1) Declaration of the company

I-2) References

I-3) Security guidelines for Ship Plan

I-4) Ship Security Certificate and survey

I-5) Ship information

I-6) Responsibilities
- Company responsibilities
- Company Security Officer (CSO) responsibilities
- Master responsibilities
- Ship Security Officer (SSO) responsibilities
- Crew members responsibilities
- Company crisis management

II) Plans, procedures and controls

II-1) Manning

II-2) Security levels
- Security level 1
- Security level 2
- Security level 3
- Security level matrix

II-3) Access control to the ship
- Access control plan documentation
- Access points to ship
- Gangway log / ID badges
    - -gangway log
    - -visitors log
    - -crew log

II-4) All ships
- Deck Watch Officer (DWO)
- Gangway guards
- Deck roving patrols
- Restricted areas
- Vulnerable points
- Citadel plan
- Security Lighting plan
- Search plan

III) Ship security policy

III-1) Shore leave

III-2) Stores and provisions

III-3) Rubbish / waste material

III-4) Computer security

III-5) Keys

III-6) Monies – Petty cash

III-7) Safe

III-8) Personnel items

III-9) Baggage
- Baggage handling – passenger ships
- Transit / unaccompanied baggage – passenger ships
- Unclaimed baggage

III-10) Lockers

III-11) Drugs

III-12) Alcohol

III-13) Fire watch

IV) Information and Equipment

IV-1) Information
- Passage of information
- Reports

IV-2) Communication
- On board
- External ship to shore communications
- Alarms

IV-3) Technical Equipment
- CCTV
- Intruders alarm

IV-4) Duress words and codes
- Information
- Action

IV-5) Medical

IV-6) Security equipment
- Individual security equipment
- Equipment responsibility

V) Ship Security Assessment (please refer to « Ship Security Assessment » separate document)

V-1) Identification of key shipboard operations

V-2) Identification of existing security measures and procedures

V-3) Identification of potential threats (threat scenarios)

V-4) Performance of an on-scene security survey

V-5) Identification of weakness in both the infrastructure and the process

VI) Ship / Port facilities interface

VI-1) Port facility interface
- CSO
- Contact details
- Master
- SSO
- PFSO

VI-2) Internal security

VI-3) Access control
- Gangway
- Restricted areas
- Controlled zones
- Control measures

VII) Plan documentation and records

VII-1) Lighting plan

VII-2) Access points plan

VII-3) Search parameter plan

VII-4) Crew list

VII-5) Master's quarterly report

VII-6) SSO's security reports, including a record of training and drills and rehearsals

VII-7) SSO's security record

VII-8) Gangway log

VII-9) Ships International Security Certificate

VIII) Training and drills

VIII-1) Security training

VIII-2) Objectives

VIII-3) Security education program

VIII-4) Security training courses and exercises

IX) Contingency plan

IX-1) Threat
- **Criminal**
- **Political**
- **Terrorist**

IX-2) Company firearms policy

IX-3) Use of force

IX-4) Action on receipt of bomb threat
- **Threat analysis**
- **Responsibilities and procedures**
- **Sequence of events**

IX-5) Action on discovery of a bomb or suspect package
- **Policy**
- **Procedures when an unidentified package or bomb is found**

IX-6) Bomb search plan
- **Bomb search guidance**
- **Conduct of search**
- **Bomb state condition response**
- **Evacuation procedure**
- **Reporting procedures**

IX-7) Hijack or armed boarding
- **Action to be taken on receipt of warning**
- **Communications**
- **Military response**
- **Firefight**
- **Press release**

IX-8) Hostage situation
- **Duties and responsibilities**
- **Procedures and rules for hostage situation**
- **Information needed in a hostage situation**

IX-9) Illegal immigrant / Stowaway
- **Security**
- **Procedure**

IX-10) Action on passenger or crewmember failing to return to the ship
- **Procedure**

IX-11) Piracy or potential threat
- **Methods**
- **Security responses**
- **Firearms**
- **Report procedure**

IX-12) Response to MAYDAY / distress signal

IX-13) Small craft attack / suspected ship approach

IX-14) Swimmer attack

I) Introduction

I-1) Declaration of the company

This manual establishes and embodies the company security policy including plans, procedures and guidelines in order to safeguard crew, other employees, visitors, ships and cargoes from activities of terrorist or other criminal organizations. All employees have responsibilities in following the Ship Security Plan.

I-2) References

This Security Manual has been compiled with the following references and these are listed as a guide to assist in further revisions.
These references are held in the Head Office but do not need to be maintained as part of the controlled library (unless stated elsewhere).

I-3) Security guidelines for Ship Plan

The SSP is not subject to inspection by officers appointed by a Contracting Government to carryout control and compliance measures. If officers have clear grounds for non-compliance, verification by reviewing this document may be allowed in exceptional circumstances, but the following areas are considered confidential and cannot be subject to inspection without agreement by the Master through the CSO:

- Identification of the restricted areas
- Procedures for responding to security levels
- Procedures for responding to security instructions Contracting Governments may give at security
  level three
- Duties of shipboard personnel assigned security duties
- Procedures for all security equipment
- Identification and location of the Ship Security Alert System
- Procedures and use of the Ship Security Alert System

I-4) Ship security certificate and survey

The Ship Security Certificate was issued on the………
By……………. and will require to be renewed by…………….

A copy of the Ship Security Certificate is maintained on board the ship.

I-5) Ship information

- COMPANY OPERATOR

Name:
Address:
Tel:
Fax:
E-mail:
Telex:

- DETAILS OF SHIP

Name:
Tel:
Fax:
E-mail:
Telex:
Mobile:
IMO number:

- TYPE OF SHIP

Year built:
Flag:
Length:
Width / Beam:
Drought empty:
Drought loaded:
Deck (Freeboard) height above sea level when loaded:
Gross tonnage:
Deck height above sea level when empty:
Year of registration:
Registry No:
Port of registry:
Number of crew:
Number of cabins / berths:
Radio call sign:

I-6) Responsibilities

- **Company responsibilities**

The company will:

- Observe the International Laws and Regulations regarding maritime security and ensure they are covered in this Security Manual
- Continue to practice good management
- Safeguard employees, visitors, passengers, customer cargo and the ships
- Appoint and empower a suitably senior company officer to have overall responsibility for security on board all company ships, (known as the company Security Officer (CSO) and give support to fulfil his duties and responsibilities)
- Have the security risk assessed taking into account the type of crew, cargo, ship, routes and destinations
- Co-operate with the responsible Authorities and act on their advice
- Promote security awareness among all employees

- Appoint and empower through the Master an officer as Ship Security Officer (SSO) on each ship and support their responsibilities and duties
- Provide guidance and advice, primarily this document, to Masters and crews on the response to the threat and keep such guidance updated
- Establish a security element to the crisis management structure including media and family information plans
- Establish a reporting and recording system for incidents and pass that information to the Authorities
- Recognize that additional security requirements may impose additional burdens on Masters and crews
- Supports the Master in his authority to make independent security decisions and ask for assistance where necessary
- Company will support the CSO, Master and SSO to fulfil their duties and responsibilities

- **Company Security Officer (CSO) responsibilities**

The CSO is responsible for all aspect of security.

The CSO empowered by and acting on behalf of the company is responsible for:

- Ensuring sufficient attention and resources are allocated to security and advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information
- Continuous awareness of and assessment of the security levels
- Effecting the initial Security Assessment and ensure they are carried out
- The development and maintenance of the Ship Security Plan and that each ship reflects accurately the ship specific information
- Modifying the SSP to correct deficiencies and satisfy the security requirements of the individual ship
- Ensuring that any alternate or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained
- Ensuring adequate security training for personnel responsible for the security of the ship
- Promoting security awareness and vigilance
- Co-ordination and implementation of Security Plans with the SSO and relevant Port Facility Security Officers
- Ensuring consistency between security requirements and safety requirements
- Liaison with all the relevant external agencies in the industry, Port Authorities and Law enforcement
- Arranging security inspections and independent annual audits
- Implementation of all aspects of the Security Plan where deficiencies have been identified
- Developing the Security Manual and is the sole authority for changes and updates to develop the manual
- Arranging annual exercises to confirm efficiency of the SSP
- Arranging for initial and subsequent verification of the ship
- Arranging internal audits and reviews security activities
- Implementing his authority to set security level but not less than that set by the Contracting Government
- Complying with security levels set by Port Authorities

The CSO should have in his possession the following documentation for each ship and have a working knowledge of the following:

- Up to date, general layout of each ship
- Location of restricted areas and function of access points to the ship
- Open deck arrangements including freeboard
- Emergency and standby equipment available
- Numerical strength, and duties of ships crew
- Existing security and safety equipment for the protection of passengers and crew
- Existing security measures and procedures in effect to include monitoring, control, inspections, personnel ID, documents and communications, alarms, lighting, and access control
- Relevant international conventions, codes and recommendations
- Dangerous substances
- Security devices and systems available
- Continue updating IMO regulations
- Government legislation and regulations

The CSO will be responsible for evaluating security risks to the ships in his fleet and take relevant steps to ensure the risks are kept to a minimum.

He is responsible for maintaining and issuing a security level and when a higher security alert is implemented, he has pre-planned route changes so that destinations can be altered at short notice.

Any threat received should be treated as 'serious' and he should obtain as much information as possible concerning that threat, especially to the ship or facility concerned.

The CSO should work with the Ship Master and / or the Ship Security Officer (SSO) and implement the necessary security response.

- **Master responsibility**

The Master is responsible for:

- Commanding of his ship at all times and for the safety and security of the crew, other employees, visitors, ship and cargo in accordance with maritime law
- Taking any action within their authority and capability to prevent or minimize the loss or damage of their crew ship / cargo from theft, espionage, sabotage and other criminal activities
- Promoting security awareness in the ship's crew
- Ensuring that the information in the Security Manual is disseminated as necessary and that the crew practice acceptable security standards
- Assisting the SSO in the production and development or update of the Ship Security Plan
- Listening to the advice of the SSO and make adjustments if in agreement
- Retaining authority to change the security levels
- Requesting manpower augmentation at increased alert states
- Ensuring that appropriate members of the crew receive adequate shipboard training and, when required, formal training
- Ensuring that shipboard drills are carried out quarterly
- Including security readiness as a separate item in the Master's assessment report for periodic inspections
- Establishing the level of security complying with the security level set in ports
- Ensuring exercises are carried out as detailed by the Company Security Officer
- Having overriding authority and responsibility to make decisions with respect to the security of the ship and can request assistance where necessary and be aware that safety has priority

- **Ship Security Officer (SSO) responsibilities**

The Master, in writing appoints the SSO.

The SSO is responsible to the Master for all matters affecting the security of the ship. In particular he is responsible for:

- Developing, implementing, maintaining and revising, when necessary, the Ship Security Plan in conjunction with the Master
- Coordinating implementation of the SSP with the CSO and relevant PFSO
- Regular security inspections of the ship
- Advising the Master on all security matters including the threat assessment and proposing modifications to the SSP
- Promoting security awareness and vigilance among the crewmembers
- Reporting all security occurrences or suspected occurrences to the CSO
- Liaison and coordination with Port Facility Security Officers
- Ensuring adequate crew training is carried out with drills and inspections
- Ensuring that all crew members adhere to the security rules and implement the instructed procedures
- Security equipment
- Ensuring that crewmembers observe the company dress code
- Keeping records of all training and inspections
- Conducting the quarterly security survey
- Attending courses of instruction as required
- Coordinating the security aspects of handling ships cargo and stores
- Ensuring that security equipment is properly operated, tested, calibrated and maintained
- Completing declaration of security where required
- Maintaining the Ship Security Record

- **Crew members responsibilities**

Crewmembers are to:

- Practice security awareness at all times
- Carry out their security duties as directed
- Know their position and task as to their security duties
- Have knowledge of the various plans and procedures in the SSP, particularly those regarding access control and search
- Understand their security duties when on guard or patrolling the ship
- Dress appropriately for their duties observing the company dress code
- Have their security equipment to hand
- Understand how to use the security equipment, particularly non-lethal weapons, if carried
- Be clear on the use of force

- **Company crisis management**

The crisis management plan is covered in the shore based contingency manual, which has been amended to cover security as well as other contingencies.

The SSP provides Masters and SSOs with policy and guidance on what actions to take in an emergency.

These are specifically dealt with in the paragraphs concerning:

- Contingencies
- Use of force
- Alert states
- Citadel plan
- Communications
- The relevant annexes covering guidance and reports

II) Plans, procedures and controls

II-1) Manning

It is the policy of the company that crew strength is sufficient for the safe and efficient running of the ship, therefore crew-manning levels are able to cover security level one.

At security level two or three, the Master will decide between continuing commercial operations without security, or closing them down to cover the required security level.
At alert state level three, the Master will have to apply to the CSO for augmentation of the personnel. These personnel will most likely come from local security companies.

The SSO is responsible for maintaining a security bill that makes clear who is assigned to what task. This security bill identifies crew's security responsibilities at all levels.

II-2) Security levels

In line with ISPS Code and for ease of operation, there are three security levels.
These levels relate to a perceived or specific threat as follows:

- **Security level one**

This level is when there is a possibility of a threat against shipping (in general) and this security level should always be maintained during normal working conditions.

- **Security level two**

This is where 'intelligence' from a reliable source has been received indicating that a threat against shipping or ports / terminals has been given to a respective operating area or type of ship although no specific target has been identified.

- **Security level three**

This security level indicates that a specific ship or port / terminal has been identified and that the threat is highly probable.

These are the primary measures to follow:

- Prohibit non-essential access to the ship
- Secure all access points to the ship
- Increase berths screening (e.g. use only known berths)
- Follow Coast Guards and company instructions regarding port entry and operations
- Follow port instructions regarding access to its navigation infrastructure
- If necessary re-route the ship until the threat is eliminated
- Secure all barge batches to prevent unauthorized cargo discharge
- Ensure waterside surveillance for the ship is provided

These security levels will be issued by the CSO from the Head Office of the company.
However Masters, at their own discretion, because of a local change of the threat, may raise the security level.

- **Useful security level matrixes**

You will find several matrixes for a quick survey of the various measures at the different alert states below cover the security measures to be implemented:

2.2.1- Ensuring the performance of all vessel Security duty

Protective Measures	Level 1	Level 2	Level 3
All vessels crewmembers normally review and exercise their security duties and responsibilities through drills and training	**YES** Drills & Exercises conducted at specified intervals		
Provide security information to all crewmembers and any security personnel that includes the security level and any specific threat information	Optional	**YES**	
Vessel Security Officer should normally communicate with the waterfront facility to coordinate protective measures	**YES**	**YES** Coordinate additional protective measures	

Source: NVIC 10 02 - US Coast Guard

2.2.2 - Monitoring restricted areas to ensure that only authorized persons have access

Protective Measures	Level 1	Level 2	Level 3
Locking or securing access to restricted areas (Doors in escape routes must be capable of being opened without keys from the direction for which escape is required)	Optional	**YES**	
Use personnel as security guards or patrols	Optional	**YES** *	**YES** #

* Dedicating personnel to guarding or patrolling restricted areas

\# Posting personnel to continuously patrol restricted areas and areas adjacent to restricted areas

Source: NVIC 10 02 - US Coast Guard

2.2.3 - Measures for controlling access to the vessel

Protective Measures	Level 1	Level 2	Level 3
Access points are normally secured(@)or continuously attended to prevent unauthorized access	YES	**YES** Assign additional personnel at appropriate access point	
Weather-deck access vents, storage lockers, and doors to normally unmanned spaces (such as storerooms,auxiliary machinery rooms, etc) may be looked (@)or precautions taken to prevent unauthorized access	YES		
Limit entry to the level to a minimum number of access points (While not restricting egress from the vessel in the event of an emergency)	Optional	YES	YES*
Coordinate with the waterfront facility to extend access control beyond the immediate area of the vessel	Optional	YES	

@ Doors in escape routes must be capable of being opened without keys from the direction for which escape is required)

* Limit entry to to a single access point

Source: NVIC 10 02 - US Coast Guard

2.2.4 - Monitoring of deck areas and areas surrounding the vessel

Protective Measures	Level 1	Level 2	Level 3
Use security lookout and / or security patrols	Optional	YES	YES*
Perform waterside boat patrols	Optional		YES*
Use divers to inspect the underwater pier structures prior to the vessel's arrival, upon the vessel's arrival, and in other cases deemed necessary (If required by port facility)	Optional		YES

* Increase the number and frequency of :
  - Security patrols to ensure continuous monitoring and
  - Waterside boat patrols to ensure continuous monitoring

Source: NVIC 10 02 - US Coast Guard

2.2.5 - Measures for controlling the embarkation of persons and their effects

Protective Measures	Level 1	Level 2	Level 3
Verify reason personnel are embarking the vessel by using tickets, boarding passes, work orders, or other means	YES		
Positively identify crewmembers, passengers, vendors, visitors, and other personnel prior to each embarkation	YES		
Arriving crew verified as authorized to serve aboard the vessel	YES		
Inspect persons, baggage, carry-on items, and personal gear for prohibited weapons, incendiaries, and explosives	YES 5 to 20 %	YES 25 to 50 %	ALL 100 %
Security briefings provided to all passengers, prior to departing, on any specific threats and the need for vigilance and reporting suspicious persons, objects, or activities	Optional	YES	
Assign personnel to guard designated inspection areas	Optional	YES	
Limit entry to only passengers and crewmembers	Optional		YES
Escort all service providers or other personnel needed aboard to provide essential services to the vessel	Optional		YES

Source: NVIC 10 02 - US Coast Guard

2.2.6 - Supervising the handling of cargo and vessel's stores

Protective Measures	Level 1	Level 2	Level 3
Verify non-containerized cargo against the manifest (Companies are encouraged to participate in the US Customs Service program titled: Custom Trade Partnership Against Terrorism)	YES 25 to 50 %	ALL 100 %	
Verify the container identification numbers of loaded containers against the manifest (Idem as above)	ALL 100 %		
Verify the container identification numbers of empty containers against the manifest (Idem as above)	YES 25 to 50 %	ALL 100 %	
Inspect vessel's store and provisions	YES 25 to 50 %		ALL 100 %

Source: NVIC 10 02 - US Coast Guard

2.2.7 - Ensuring that Port-specific security communication is readily available

Protective Measures	Level 1	Level 2	Level 3
Provide regular communication checks	Optional	YES	
Provide a backup means of communication	Optional	YES	YES*

* Provide a redundant and multiple means of communication

Source: NVIC 10 02 - US Coast Guard

II-3) Access Control to the ship

- **Access control plan documentation**

The SSP has a plan of the ship annotated with:

- All the potential access points to ship
- All restricted areas and vulnerable points
- The citadel plan

- **Access points to ship**

The company policy is that all entrances remain closed unless for operational reasons. Those that are left unsecured must be protected.

A list of each entrance is to be created.

- **Gangway Log / ID Badges**

    - *Gangway log:*

Uncontrolled or unescorted movement must not be permitted; therefore a gangway / visitors log is mandatory at all times.
The company policy is that at all times and all security level, all repairmen and visitors must carry ID and be entered in the gangway visitors log, and maintained at all times for informational and historical purposes.

The format and information is to be documented:

- All entries are to be made in ink
- Mistakes will be corrected by drawing a line through the incorrect entry and initials of corrector placed next to it

The SSO is to maintain the log according to company policy

- *Visitors log*:

- Name of repairman or visitor
- Name of person being visited
- The time in and out
- The allocated badge number

ID badges should be color-coded and issued to escorted or non-escorted repairmen or visitors. They should only be issued on the production of photographic identity documents. At security level three, only pre-cleared visitors should be allowed access to the ship.

Badges will be serialized and color-coded as follows:

- Blue: visitor is on approves access list and escort is not required
- Orange: for personal visits. Sponsor will be required to escort visitor at all times
- Red: for contract / other escort required visitors
- Green: for passengers. With passenger identification, photograph and signature, duration of the pass and issue control

Personnel issued badges will be told:
- How to wear / display the badge
- What to do if badge is lost
- To return badge upon leaving the ship

- *Crew log:*

All crew leaving the ship, away from the immediate berth or facility, must sign in and out of the crew log.

The log should include the following information:

- Name of crewman signed out
- Time out
- Who authorized
- Where going
- What task
- When due back
- Contact number (if available)
- Time in
- Signature

II-4) All ships

- **Deck Watch Officer (DWO)**

The oncoming DWO will be totally familiar with all current standing orders. Additionally, he will be responsible for all orders and / or duties passed on by the Master.

The minimum required duties include the following:

- Ensure gangway and roving patrol watches are relieved properly and are knowledgeable of all standing and special orders
- Ensure you know how to get in touch with the Master and Ship Security Officer in case of an emergency
- Ensure all watches the DWO and how they can get in touch with him
- Ensure all watches are in the proper uniform or coveralls and present a neat and orderly appearance
- Ensure all watches are equipped properly to fulfil their duty
- Ensure standing orders are understood
- Ensure that all visitors are in possession of a valid badge and that they have been entered into the visitors record sheet
- Ensure you are knowledgeable of the current security level and the measures that have been implemented
- Depending on security level, all baggage to be searched prior to boarding.

- **Gangway guards**

Assigned personnel shall be thoroughly briefed on the duties to be performed.
It is the policy of the company that gangways need not be done unless necessary at security level two and should not be down at level three.

Depending on the threat and security level, crew, security guards, law enforcement or armed personnel may be available. In determining personnel to be used to perform guard duties, the Master and SSO should consider the following:

- Threat assessment of the area in which the ship is located
- Current port or terminal situation (security level)
- Most recent messages, intelligence and alert information available
- The ship vulnerability based on this intelligence
- Duties to be performed

Gangway watch duties shall include:

- Stop and identify all persons wanting access. Allow no unauthorized visitors unless approved by Master, SSO or Watch Officer
- Verify individuals' purpose / authority for boarding
- Log all visitors' names, organization represented, purpose of visit, time in / out in visitors record sheet
- Ensure all visitors have departed ship by time stated by Master, SSO or DWO. Report all violations to DWO
- Ensure all visitors receive the appropriate identification badge and are briefed on circulating restrictions and restricted areas. Escort if required
- Check all equipment and cargo leaving and entering the ship for suspected contraband. Report all violations to the Master, SSO or DWO
- Deny entry to all personnel refusing
    - identification
    - satisfactory explanation for reason of visit
    - consent of search of personal belongings
    - consent of search of individual
    - content to conform to ship regulations

- **Deck / roving patrols**

Whether the ship is alongside, at anchor, or in route, it is vulnerable to pirate or terrorist acts.
These conditions or an increased security level warrants roving patrols aboard the ship.
The Master, SQSO or DWO will determine the implementation and degree to which the patrols are used.
The patrol will be thoroughly familiar with the Ship Security Plan and will be briefed by the DWO prior to the patrol commences.

- **Restricted areas**

Three levels of control will designate all restricted areas, which are:

- Exclusion area
Requires the highest level of control. This is the most secured type of restricted area. It contains a security interest, which if lost, stolen, compromised, sabotaged, would cause grave damage to the ship routine.

- Limited area
Second most secured type of restricted area. May be inside a controlled area, but never inside an exclusion area. Contains a security interest, which if lost, stolen, compromised or sabotaged would cause serious damage to the ship routine or current project. Unescorted control could permit access to a security interest or asset.

- Controlled area
Least secured type of restricted area. Contains a security interest, which if lost, damaged, compromised or sabotaged could cause damage to the ship, routine or project. Uncontrolled / unescorted movements may permit access to a security interest or asset.

The restricted areas are:

- The bridge
- The engine room
- The engine control room (ECR)
- Emergency escapes from engine room and ECR
- Rear steering gear
- Bow thruster
- Fire fighting control room
- Emergency generator room
- Communication room (if separate from the bridge)

- **Vulnerable points**

Where possible vulnerable points are to be locked at all times in line with safety and good operations. At security levels two and three, access is as laid under that security level.

- Air conditioning plant and fan rooms
- Battery and accumulators stores
- Electrical stations
- Lift machinery spaces
- Bottled gas stores
- Paint stores

- **Citadel plan**

In line with the principle of access control, the Master and SSO are to draw up a citadel plan for their ship. This will be a plan to physically seal with barriers the essential core of the ship. This must include the wheelhouse/s, the ECR and engine room, and the communications.

This radical form of access control is only to be considered for use at security level three or in the event of one of the contingencies if the situation permits:

- Hijack
- Hostage Situation
- Piracy / Armed attack

- **Security Lighting Plan**

The primary purpose for any security lighting is to provide the means to detect and deter intruders.

Adequate perimeter such as the ships hull or a determinate distance from the ship therefore:

- The perimeter must be lit
- The perimeter must be observed
- Lighting will be such that it will not cause a glare that hinders vision of security personnel or navigability of water traffic
- Light sources should be directed towards likely avenues of approach and / or waterline to a minimum of 100 feet out from the hull
- Light implementation should provide an overlap so not to have any dark spaces and be continuous around the ship
- Security lighting will be activated during all hours of darkness
- Use of spotlight for long ranges if required
-Temporary additional lighting will be established, if any areas are not lit (security level)
- All deficiencies or needed repairs will be logged in and immediately reported to the DWO

- **Search Plan**

To ensure that a thorough and efficient search can be completed in the shortest possible time search plans, specific to each ship, should be prepared in advance.
The plan should be comprehensive and presented logically with details the routes searchers should follow and the areas they should search.
The company policy is that there will be no personnel search unless specified in the security levels.

There are two types of search:

- Searching unlocked / locked spaces
The first response is to search all unlocked spaces followed by locked ones

- Personnel search
This is the best done ashore, most probably at the bottom of the gangplank for ease and control using a hand held detector, but these do not cover explosives, plastic weapons or incendiaries.
Physical searches should be used as the alternative.

And two methods of search:

- Reactive search
Carried out in response to a specific threat or hard intelligence.
To be successful, it must comply the following:

  - Searchers are familiar with the area and can notice the unusual
  - It must be planned and controlled with a central reporting point
  - Searchers must be able to recognize a bomb or explosive device
  - Searchers must have communication with central control
  - Searchers must know what to do if a suspect device is found

- Preventive search
Aimed at anyone smuggling a device on board; this will involve the search of all items before they come aboard the ship. This will include crew, repairmen, facility staff and visitors. It will also cover stores and provisions, gash and rubbish, spares and any other items coming on board.

.

- Procedure for search

The search plan includes a plan of the ship with possibly the access control plan information cards that cover the whole ship designating specific areas to be searched. This will be unlocked areas on stage one, than locked areas on stage two.

Once a search is ordered, the Master or the SSO will brief the crew on any relevant information received and also how the search will be conducted. This brief must include:

- Type of search to be conducted – unlocked or locked or both
- Allocation of areas of responsibility if there are changes from the standard plan
- Priority search areas
- Use and allocation of specialist equipment
- Communications and control

When searching, crewmembers should try to:

- Start from the bottom and work up
- Search for bulkheads to the center of the space
- Avoid conducting random or spot-checking of logical threat areas when conducting a detailed search
- When researching outside areas, thoroughly check trash receptacles, deck drains and storage lockers
- Personnel entirely familiar with the spaces shall do searches of machinery spaces and other specialized spaces. Be alert for small charges placed to rupture the hull, high-pressure piping or electrical cables
- Have the occupants of the space stand by to open lockers, desks and cabinets

III) Ship security policy

III-1) Shore leave

Shore leave will normally be granted during off duty hours unless security conditions or the security level warrants differently. Heightened threat conditions will cause an increase in the number of duty personnel and may cause denial of shore leave or recall of personnel after shore leave has been granted. This is certainly the case at security level three and most probably two.

The decisions and actions required to ensure the control of shore leave and recall are:

- Crewmembers must fill out the crew log
- Master in conjunction with the SSO determine whether leave is granted / denied, or to implement a personnel recall
- All emergency information will be posted at gangway for all crew personnel to read
- If an emergency recall of personnel is required, information will be briefed to all the crew on return
- Upon recall, all crewmembers will immediately report back to ship. If unable to return, personnel should attempt to contact the ship. If contact cannot be made, notify the local Authorities and the company Head Office.

III-2) Store and provisions

All store and provisions offer the opportunity to gain access to the ship by persons or by unlawful objects or substances, therefore the checking of these stores and provisions is the responsibility of the SSO.

III-3) Rubbish and waste material

All rubbish and waste material is classed as a health hazard and fire risk therefore:

- All rubbish to be kept and stored in one enclosed area
- Doors to be kept closed at all times
- When off-loaded, area to be cleaned
- Area to be checked at irregular intervals by the SSO

III-4) Computer security

Basic security measures required are:

- All computers are to be security marked
- All computers are to have password protection to open the software
- Passwords are to be kept in the Master's safe
- Backup files are to be recorded and kept in the master's safe
- No unauthorized personnel will have access to the ship computer system
- All computers to be secured to the desk
- The storage of the disc or computer that holds the SSP in electronic format must be secured at all times

III-5) Keys

All ships are to be provided with key presses and all keys are to be held in the key press unless signed out to ship's officers.

- **Master keys**

Master keys are to be held by the Master.

- **Crew keys**

Crew will have keys for their cabins only and access for those parts of the ship they are authorized to enter.

- **Duplicate keys**

No duplicated keys are authorized.

- **Lost / Replacement keys**

All lost keys that need replacing will be reported to the SSO.

III-6) Monies – Petty cash

All ships are to be provided with safes with all monies and petty cash held by the Master. Any large transactions will be conducted through the shipping agent.

III-7) Safe

All ships have a safe to be placed in a decided place by the company. Keys / combination are held by the Master

III-8) Personnel items

All crew personnel items are to be kept in the individual cabins. If extra storage space required, then permission is required from the SSO.
All crew items that are brought onto the ship are subject to search at the Masters discretion or if security level dictates so.

III-9) Baggage

All baggage is the easiest means by which to take aboard a ship, unlawful substances, illegal objects and firearms, therefore strict access control is mandatory.

- All crewmembers will be liable to search at level two or above
- All visitors, workmen, vendors, … with bags will be searched prior to access

- **Baggage handling - passenger ships**

- All passengers will identify to the "check in" their baggage, which will be clearly labeled with all ship details and the cabin it, will be placed to
- The baggage will then be placed in a secure area and the baggage will be screened and searched by detection devices or with dogs as available
- The owner of this baggage is kept within the area and once the baggage has been cleared, the passenger can board the ship under normal access conditions. The baggage is then marked as "security inspected"
- The baggage is then placed aboard the ship by cleared staff for the cabin stewards to place in the passenger's cabin
- If there is any delay from the secure area to the ship, the area is to be secured
- All disembarking passengers' baggage will be kept separate from embarking passenger's baggage

- **Transit / unaccompanied baggage – passenger ship**

All transit passengers that will have their baggage sent from their original departure point to the ship or from country arrival point to embarkation will be subject to the following security conditions:

- The baggage will only be accepted if a member of the ship company has checked it through or by recognized handling agent
- Baggage will be security wrapped and a security label will be placed on the baggage, stating it has been "security inspected"
- Once at the embarkation point, it will be placed in a separate secure area until the passenger identifies the baggage. This baggage is then subject to the normal screening process

- **Unclaimed baggage**

Check for any identification and inform passenger to collect baggage.
If not, baggage to be thoroughly screened by x-ray machine / hand held detector, and if possible dog and sniffer test.
If clear, open case and try and identify owner.
Baggage to be secured by the company, until claimed.

If, at any stage, a positive reading is carried out, the baggage is to be placed in an isolated secure area and the Authorities are to be informed.

III-10) Lockers

All lockers will be security protected (dependant on the security level) by either of the following:

- Padlock / lock
- Security inspected labels
- Tamper-proof security seals

Those on deck will be secured at all times when not in use.

III-11) Drugs

The company policy states that no drugs apart from those held within the "Medical Room" will be allowed aboard the ship.
Any person found with a banned substance on his possession will be reported to the Master and asked to leave the ship at the next port (if safe to do so).
A report will be sent to Head Office for further proceedings to take place.

Precautions when in port:

- Strict access control
- Restriction of movement
- Enforce "out of bound" areas
- Main deck watch
- Raise gantry when not in use
- Monitor activities around ship
- Conduct ship search prior to departure
- Inform customs of find (at port or next port of call)

If drugs are found:

- Never taste, eat or drink the suspected substance
- Do not handle the substance without gloves or facemask
- Do not inhale fumes, powders or vapors
- Do not smoke near the substance or expose to heat or flame
- Ensure adequate ventilation
- Wash hands and brush clothing free from any contamination
- Do secure the area and take photographic evidence if possible
- Secure substance under lock and key
- Make full report including witness report

Crew as well as passengers can smuggle banned substances aboard the ship for trafficking or personal use. The following is a guideline in what symptoms / behavior patters to look for to indicate drug abuse:

- Nervousness
- Possession of large amounts of cash
- Frequent purchasing of expensive articles
- Possession of lists containing names, quantities and prices
- Meetings with persons not usually associated with this person
- Unusual clothing not associated with season (long sleeves to hide puncture marks, sunglasses to hide dilated pupils…)
- Persons found in part of ship not associated with their duty
- Persons avoiding contact with other members aboard the ship or in a "trance" like state
- Persons taking particular interest in specific cargo
- Possession of tools not relating to their duty

III-12) Alcohol

Company policy states that no crewmembers will consume alcohol aboard any of their ship. Personnel found to be under the influence of alcohol will be reported to the Master for disciplinary action to be taken

III-13) Fire watch

A fire watch will be maintained by the SSO over a 24-hour period.
A record of patrols will be kept and checked by the SSO/DWO.

IV) Information and Equipment

IV-1) Information

- **Passage of information**

The passage of information in a crisis is essential.

All ships are well provided with communications and therefore there are the means.
More particularly over security matters, it is important to have good information flows between the crew and ship officers, and between the officers and the shore side staff.

A list of the relevant publications is held in the library at Head Office for references.
The minimum the ship must hold is:

- A copy of the SSP
-The International Ship Security Certificate of the ship
- Standard available information

To assist in response to a crisis and assist in crisis management, basic ship information is to be held at the company Head Office.
This information is the responsibility of the SSO, who will ensure that is updated.
The ship file should have as a minimum:

- A large-scale plan of the ship layout at all levels
- A copy of the Ship Security Assessment
- A copy of the Ship Security Plan
- The crew list
- A record of all means of communication
- The route, destination and cargo – from the daily operational sheet

- **Reports**

The following is the consolidated list of reports that should be held by the SSO:

- The Master's quarterly report
- The ship security record
- The gangway log
- Visitors log

Reports are to be kept by the ship for the CSO.
A copy (if possible) should be typed onto a computer disc for future references.
SSOs shall maintain a ship security record. This record shall, at a minimum, include the following:

- Names and ratings of the crew
- Dates and specifics of quarterly drills
- Breaches of security and any security incidents
- Communications concerning direct threat to security of ship
- Changes in security level (including those at ports visited)
- Surveys and inspections
- International audits and reviews of security activities
- Reviews of SSA and SSP implementations
- Security measures in effect and their reason
- Security training and drills shall be recorded as well, to include a roster of those in attendance
- DOS Record (minimum 10 ports)

The Master should report all unlawful acts directly to the CSO.

The SSO will keep all written security reports until advised by the CSO.

IV-2) Communications

The ship has the following communication equipment:
List of equipment available onboard the ship.

- **On board**

All security crewmembers are to carry hand radios when on duty. The Master is to ensure that all radio have a common security frequency and a spare channel for emergencies.
All other crewmembers away from immediate ship duties are to monitor this frequency.

Security Level guideline are as follows:

Security level one
- Establish routines for ship position reporting
CSO to consider creating a covert communications capability that might be needed at higher security levels (e.g.; use of code words to communicate, panic / emergency button on BOATRACS, GMDSS, AIS equipment)

Security level two
- Increase frequency of routine ship reporting
- Establish an engine room-wheelhouse communications process for use during a security emergency

Security level three
- Establish a positive fail-safe ship position reporting system (e.g. if a ship fails to report at the specified time, the company will contact the ship in addition to the AIS system)

- **External Ship to Shore Communications**

Masters are to ensure that the ship maintains the ship to shore communications routine laid down in the security level guidelines. This provides security measures as follows:

Security level one
- Establish a plan for ship communications to Head Office in the event of a security incident (e.g. a means of contacting the national response center, company officials, local and federal authorities, lock operators, vendors and other as needed)
- Provide ship crew redundant communications equipment (e.g. radio, cellular phones,…)
- Make any required CG Notice of Arrival (NOA) reports
- Make all appropriate notifications to lock operators

Security level two
No change

Security level three
- Establish local emergency contacts (based on information provided in government-issued threat notices) and increase communications between ship and CSO.

- **Alarms**

The established standard signal is:
The ship shall sound four short rings on the general alarm bell, and four short blasts on the ship's whistle, in addition to hailing the alert to a security situation or drill over the loudhailer / PA system.

IV-3) Technical Equipment

- **CCTV**

The ship has the following CCTV cameras

LOCATION	OBSERVATION	RECORDED	NOTES
MAIN ENTRANCE	GANGWAY	24HR	
PORT AFT	AFT OF SHIP / 50 MTRS	RANDOM	

- **Intruder Alarms**

Ship Security Alert System
Ship Security Alarm System activation are located in three areas

All crewmembers not familiar with this system will report to the SSO for guidance.

IV-4) Duress Words and Codes

Persons on watch are subject to hostile actions at any time, due to the fact that they are most likely to first encounter hostile visitors or intruders.
Although overtly spreading the alarm will be the most rapid means of calling for assistance, there may be times (hostage situation,…) where a more covert means will be a better action.

- **Information**

As a matter of routine, this ship will implement and use a duress word / code system to quietly announce a person is distress. This duress word / code will be implemented in the following ways:

- A duress word may be passed from a person in any way (i.e. the general announcing system, hand-held radio, in person, …). All hands must know the active duress word / code and know what actions to take should they hear this word.

- The duress word will be changed whenever the word has been compromised or deemed appropriate. Occasionally, it may be necessary to alter with a code, or to include a code with a word. A code will be some sort of physical action that can be determined in distance (i.e. Gangway Watch not wearing his ball cap, …)

THE DURESS WORD / CODE WILL NOT BE WRITTEN DOWN.

- **Action**

The SSO will:

- Ensure that all personnel are familiar with the active duress word / code
- Conduct periodic training and drills in reaction to the covert duress procedures
- Change the Word or Code as required

IV-5) Medical

- Medical facilities aboard ship
    - Location
- Medical trained personnel
    - Qualifications
    - Refresher
- MEDIVAC / CASEVAC
- Telephone numbers

IV-6) Security Equipment

The following equipment is held aboard the ship (example):

- X-ray machine
- Hand held metal detectors
- Gas detectors
- Sniffer equipment
- Scenes of crime bag
- Blast blanket
- Handcuffs, plasticuffs
- Batons

- **Individual security equipment**

- Hand held radio
- Torch
- Whistle
- Pepper spray (TBC)
- Bull Horn (if required)

- **Equipment responsibilities**

The SSO is responsible for ensuring that:

- All equipment is signed out
- Individual crewmembers hold the correct equipment
- The ship holds the correct issue of collective security equipment
- All equipment on board, both personal and collective, is in a workable state
- The repair, service and maintenance of equipment
- Trail reports on equipment when called for
- Will ensure security equipment is tested, calibrated and maintained on board, visited at recognized ports, or if not applicable, on return

The crewmember is responsible for:

- Ensuring that he has his personal security equipment about him
- Maintaining that equipment in good working order
- Reporting losses or breakage for replacement

V) Ship Security Assessment

Please refer to « Ship Security Assessment » document.