HIP Security Policy

- **Edition: 01**
- **Scope: HIP (HIPG and HIPS)**
- **Effective Date: 01 Aug 2022**

Hambantota International Port

Hambantota Sri Lanka

Document Control

Description	Name/Designation	Signature	Date
Prepared by	Senior Manager Security (Shylendra Jeewakarathna)		
Checked by	General Manager – HIPS (Capt. Miyuru Gunasekara)		
Checked by	Head of Human Resources and Administration (Jeevan Premasara)		
Checked by	Senior Manager Legal (Deshani Koralage)		
Approved by	CEO – HIPS/Chief Officer Marine Services and Security - HIPG (Capt. Ravi Jayawickreme)		
Approved by	Chief Financial Officer (Raymond Mu)		
Approved by	Chief Executive Officer – HIPG (Johnson Liu)		

Document Change Log

Rev. No.	Page No.	Description of Amendment	Approved by	Effective Date

Contents

1. Purpose

The purpose of this Security Policy is to provide detailed instructions and guidance on the implementation of the required security measures at Hambantota International Port (HIP)

2. Scope

This Policy applies to all HIP users including investors, tenants, etc. The purpose of introducing a new Security Policy is to set common security standards in compliance with the ISPS code.

3. Responsibility and authority

While the Chief Executive Officers of both the HIPG and HIPS hold ultimate responsibility for the implementation of this policy at all levels of the organization, every HIP employee shall accept individual responsibility to comply with the set security standards and finally to achieve the company objectives.

4. Abbreviations

1.	HIP	Hambantota International Port
2.	HIPG	Hambantota International Port Group
3.	HIPS	Hambantota International Port Services Company
4.	ISPS Code	International Ships and Port Facility Security Code
5.	IMO	International Maritime Organization
6.	SOLAS	Safety of Life at Sea
7.	SOC	Security Oversight Committee
8.	PSC	Port Security Committee
9.	DA	Designated Authority
10.	CA	Competent Authority
11.	PFSO	Port Facility Security Officer
12.	PFSP	Port Facility Security Plan
13.	SLN	Sri Lanka Navy
14.	FOC	Free of Charge
15.	SOP	Standard Operating Procedure
16.	CEO	Chief Executive Officer
17.	GM	General Manager
18.	PSO	Port Security Officer

5. Development of ISPS Code and its relevance to HIP

5.1 Since the terrorist attacks in the USA in 2001 the threat to maritime transport systems worldwide has changed, this has been acknowledged both nationally and internationally and has prompted the development of new and improved security regimes across the transport systems.

5.2 The International Maritime Organization (IMO) responded to the attacks of September 2001 by developing new security requirements for ships and port facilities to counter the threat of acts of terrorism. These requirements entered into force under SOLAS chapter XI-2 to the Convention on the Safety of Life at Sea 1974 (SOLAS) and a new International Ship and Port Facility Security Code has been developed (ISPS Code). The SOLAS amendments and ISPS Code were formally adopted in December 2002.

5.3 Similar to any other International Port in the world, the HIP must also adhere to and should comply with the ISPS Code to ensure that adequate and proportionate maritime security measures are in place on board ships and in the port under an international framework that fosters cooperation between Contracting Governments, Government agencies, local administrations, and the shipping and port industries,

6. Security Sectors and Zones of HIP

6.1 For operational convenience and easy reference, the entire HIP area (11.2 Km^2) has been divided into two sectors and 3 Zones as shown in below maps:

Map - Security sectors of HIP

Map: Security Zones of HIP

7. Security structure

7.1 Security Oversight Committee (SOC)

7.1.1 Under the patronage of the Ministry of Ports and Shipping, the Oversight Committee for HIP security has been formed and convened by the Sri Lanka Ports authority consisting of representatives of the Sri Lanka Navy, Sri Lanka Police, and the Secretary of the Ministry of Defense or his authorized representative for managing the security within and outside the Port Property and the Lease Area. The national security of the Port Property is controlled by such Oversight Committee.

7.1.2 However, the HIPS is responsible for the all internal security within the Port Property, to enable the proper conduct of its business, the safety of the cargo, vessels, and the personnel, including but not limited to manning of the entry/exit gates, in compliance with the ISPS Code and any Applicable Laws. HIPS works are carried out in close coordination with the said Oversight Committee and monitored and guided as necessary.

7.1.3 SOC meets quarterly to examine the security situation and to make necessary changes as deemed appropriate.

7.2 Designated Authority (DA), Competent Authority (CA) and Port Facility Security Officer (PFSO)

7.2.1 Sri Lanka Navy is the Designated Authority (DA) in Sri Lanka and has the oversight responsibility for overall port Security and advice the HIP on security-related matters. Director General Shipping of Sri Lanka has the responsibility for ship security consistent with the mandate for port State control.

7.2.2 Commander Southern Naval Area (the Competent Authority) and Port Facility Security Officer (PFSO) of the HIP are committed to implementing Port Facility Security Plan (PSFP) to detect and deter the terrorist and criminal activities within the port premises and react timely and swiftly to counter such acts

7.3 Port Security Committee (PSC)

7.3.1 PSC is considered an essential part of any security regime, allowing all relevant stakeholders the opportunity to discuss security issues thus ensuring a consistent approach. This is particularly important when a port consists of number of different facilities. Hence, all port facilities at the HIP are part of the PSC, which is required to meet no less than four (4) times a year and more often if necessary. PFSO stands as the head of the PSC.

7.3.2 The role of the PSC will include, but will not be limited to:

.1 Coordinating implementation of the security measures required by the PFSP

.2 Ensuring consistency and compatibility of approach within the port

.3 Providing feedback on implementation, exercises, testing, training and updating of the PFSA and PFSP.

7.3.3 Membership of the PSC is open to all representatives with a security responsibility within the HIP and other interested parties as appropriate. The membership includes following:

.1 Representatives of SLN/Military as nominated by the PFSO

.2 Head of Security, HIP

.3 Sri Lanka Customs representative

.4 Sri Lanka Emigration and Immigration representative

.5 OIC Harbour Police station

.6 SIS representative

.7 Deputy Harbour Master or his representative

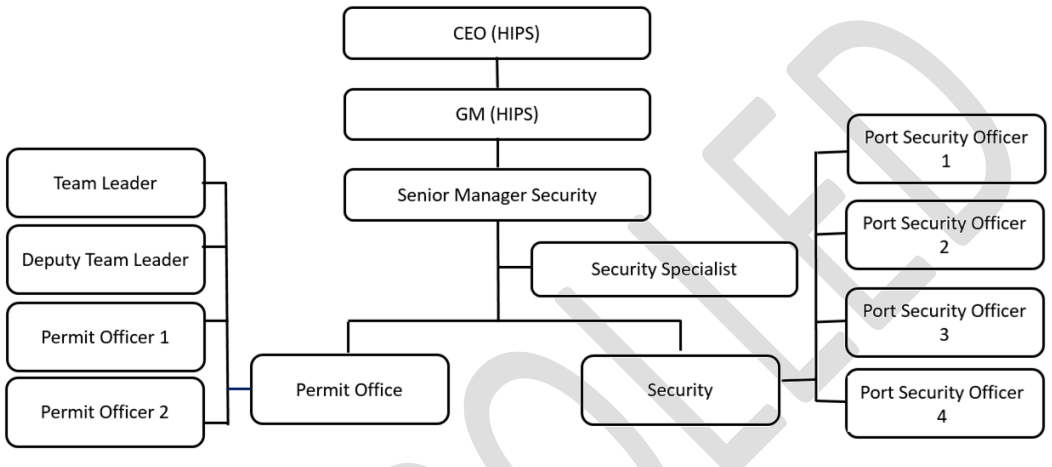
.8 Operations department representative

.9 ENS representative

.10 Terminal/security managers of other facilities/stake Holders

.11 Representatives of outsourced companies

7.4 HIP security organization



7.5 Outsourced security personnel

7.5.1 Outsourced security service provider/s is/are performing security duties at the HIP under the supervision and guidance of the Head of Security HIPS. All outsourced security personnel performing security duties or responsibilities must have sufficient knowledge and ability to perform them and it is the responsibility of the respective security company to train and prepare employees to meet the security standards.

7.5.2 The Head of Security of HIPS ensures that the performance measures are in place to confirm the effectiveness of security staff. The security personnel with specific security duties include;

.1 Port Security Officers

.2 Search teams

.3 Mobile/foot patrol

.4 Static guards

.5 CCTV operators

7.5.3 In addition, all security personnel with security responsibilities are to be subjected to employment checks prior to recruitment. Such checks include consideration of at least two references, a police criminal record check, and a medical checkup.

8. Security levels

8.1.1 The ISPS Code introduces an international system of three Security Levels:

.1 Security Level 1: Normal

.2 Security Level 2: Heightened risk

.3 Security Level 3: Exceptional/imminent risk

8.1.2 These Security Levels reflect the likelihood that a security incident will occur; the higher the Security Level the greater the likelihood of a security incident. The Security Level above 2 will be set by the Minister with responsibility for National Security in conjunction with the Minister of ports and shipping. It will be communicated through the DA to HIP.

8.1.3 At Security Level 1, port facilities will be required to have baseline security measures in place. Security Level 2 represents a heightened level of threat, and port facilities will be required to increase their levels of protective security. Security Level 3 represents an imminent and specific threat, and port facilities will be required to increase their security provisions still further and respond to instructions from the DA and National Security control authorities.

8.2 Changes to security level

8.2.1 The DA would advise HIP of changes to Security Levels. PFSO must ensure that they can be contacted on a 24/7 basis. Port facilities are required to ensure that procedures are in place for advising relevant stakeholders of changes to Security Levels. Port facilities must ensure that revised measures are in place immediately upon notification of a change in Security Level.

9. Perceived risks and threats

9.1 For planning, implementation, and management of security at the HIP, the following risks will be considered typical, and security measures should be based on this selection.

9.1.1 Risks

- Underperformance by outsourced security staff
- Fire
- Natural disasters

9.1.2 Likely threats

- Kidnapping/attacks on employees
- Hijacking ships
- Protests
- Cyber attacks
- Pilfering and theft
- Terrorist Attacks
  - ✓ Standoff attacks
  - ✓ Explosions (IED/shaped charges)
  - ✓ Seaborne attacks
  - ✓ Drone attacks
  - ✓ Sabotage (intentionally damage or destroy property to prevent the success of a plan or action)
  - ✓ Arson (criminal act of deliberately setting fire to property)

10. General security

10.1 Access to port premises

10.1.1 HIPG and HIPS employees are permitted to access the premises of their workspace during working hours as their role demands and as appropriate. Entrance at any other time or to any other area of the port is governed by internal rules. Further, a vehicle pass should be in possession if entering the port using own vehicle. To obtain a vehicle pass, a written request (email would suffice) is to be submitted to the Head of Security through the line manager. A scanned copy of the driving license, insurance, and revenue license is to be attached to the request.

10.1.2 All port users including HMC office spaces leased lands, and industrial park projects are required to obtain a valid pass from the Pass Office well in advance prior entering to the port. A guide to the port entry pass issuing procedure is available at HIPG web (http://www.hipg.lk/our-services/security).

10.1.3 Personnel applying for monthly/annual passes shall submit a Police clearance certificate along with other required documents (specified in the port pass applying procedure) and weekly passes for an individual, will only be issued for four consecutive requests and to obtain passes for a further period, a valid Police clearance certificate is to be considered essential.

10.1.4 Official and business visitors are entertained only when accompanied by an attendant. The respective line department is required to submit following details well in advance to the security department to avoid unpleasant/embracing situations. Entertaining VIPs/VVIPs will be handled case by case basis/on EXCO instructions.

.1 Personal details of visitors (name, company/organization, designation, etc)
.2 Time period
.3 NIC/PP Nos
.4 Purpose of the port visit
.5 Vehicle details including drivers
.6 Intended area of visit
.7 Names of accompanied attendant/conducting officials (HIPG/HIPS)
.8 Health declarations as appropriate.

10.1.5 Port visitors will only be allowed to access the view point area near service berth. However, required to obtained prior approval.

10.1.6 Outsourced company personnel are allowed to access permitted areas/zones/gates only. Entering into unauthorized areas are strictly prohibited. Further, authorization will be accorded upon completing QHSE induction/obtaining work permit, ISPS Office no objection and fulfilling other requirements deemed necessary for port entry. Port entry pass procedure applicable.

10.1.7 Visitors to the tank farm area should obtain prior approval (no objection) form ENS authority.

10.1.8 Participants of Meetings, seminars and other events where any other parties are involved should take place only in meeting rooms with prior notification. HIP visitors SOP to comply when holding such events.

10.1.9 Tenants occupying the HMC should possess an entry pass when entering the building and the passes will be issued free of charge. Additionally, all tenants are required to submit a nominal list of those personnel utilizing the facility through the PIS department as per the format given. The security

department should be kept informed if the facility is used after working hours. Security department will only consider approved list when issuing passes on FOC.

10.1.10 Visitors intend to go onboard the vessels must comply with relevant Government SOP and obtain approval as required therein.

11.1.11 All inter-departmental vehicles transporting/transferring goods equipment/material/ items/etc in and out of the HIP premises should possess a HIP Gate Pass (format attached) authorized by a responsible officer. Further, when items are transported/returned in and out of the port, custom approval shall be obtained as deemed necessary.

12.1.12 All port users and their vehicles are subject to security check/inspection at all access control points where identity is to be revealed and should submit a valid port pass and the NIC to security for identification. In the case of loss of NIC, the port user may submit a certified photograph (by Grama Niladari/Justice of peace) along with the Police entry copy. Support of all customers are expected as it is directly relevant in ensuring a safe and secure environment in the port area. Any inconvenience by security personnel could be directly reported to the Head of Security or Security Specialist via pso@hips.lk

10.2 Workplace security

10.2.1 It is recommended that all workplaces comply with the principle of an empty table, i.e. when leaving the room after work, remove all the documents and media from table and from other visible locations, and recommend to lock computer screens always.

10.2.2 Important documents and media and small but valued physical assets must be kept in a locked cabinet or drawer.

10.2.3 All doors and windows of HMC and PSB building needs to be kept under lock and key after working hours.

10.2.4 Users of cell phones, laptop computers and other valuable items are responsible for their security.

10.2.5 All responsible employees are to ensure other work places and vital installations are kept under lock and key when not in use.

10.3 Security of leased lands/industrial park projects

10.3.1 HIP security department is responsible for controlling the access to port facilities and monitoring restricted areas to ensure that only authorized personnel have access. The overall security of leased lands/industrial park projects is the responsibility of relevant investor/owner/operator. However, all such facilities may have their own Facility Security Plan in accordance with ISPS Code. Further, it should be compatible with the HIP Facility Security Plan.

10.3.2 All such facilities are subjected to a quarterly ISPS audit conducted by the Sri Lanka Navy (SLN).

11. Personnel security

11.1 Staff selection

11.1.1 Whilst selecting staff, each candidate's background must be checked from a security risk perspective (security clearance).

11.1.2 On appointing to the job, new staff must be encouraged to read following documents and confirm their knowledge with their signature:

.1 HIP security policy

.2 Security guide lines/SOPs

.3 Internal security rules and procedures

11.2 Dismissal of an employee

11.2.1 If an employee is dismissed, by the end of the last working day, the dismissed worker must handover the Port Pass to the Pass Office

11.2.2 Respective department Head shall take away all means of access (keys) and other credentials (change the passwords, remove from access control lists).

12. Protective security measures

12.1.1 The aim of protective security measures are to reduce the risk to each facility within the port to an acceptable level, thereby reducing the overall risk to the port operations. Therefore, those

facilities where the risk is assessed to be greater will be required to implement more stringent security measures than those where the risk is lower. e.g Laugfs terminal is more vulnerable and pose a high risk than the Xinji project site.

12.1.2 It is important to note that the standards set by the Designated Authority (DA) are minimum standards and facilities/terminals are free to implement higher standards and additional measure as the situation demands.

12.2 Vetting of port facility personnel

12.2.1 All regular port users must undergo a criminal record check and provide valid Police clearance to be eligible to obtain permanent port entry pass.

12.3 Security monitoring

12.3.1 Random security checks

12.3.1.1 HIPS Security department may conduct random security checks/inspections as and when required. i.e in addition to the ISPS audits/security audits.

12.4 Penalties

12.4.1 In case of breach of security requirements/accidents due to negligence, the offender will be imposed with penalties ranging from black listing to incurring charges (HIP must make the offender compensate for physical damage caused).

12.5 Security information sharing

12.5.1 Notifications regarding the latest Security developments and changes will be conveyed to relevant stakeholders via electronic & social media platforms such as WhatsApp/ding talk/WeChat app groups formed or through emails. The following events will be shared:

.1 Latest security incidents

.2 Security environment changes

.3 Recruitment and dismissal

.4 Changes and additions to the internal network security system

.5 VVIP/delegation visits (need-to-know basis only)

12.6 Reporting security incidents

12.6.1 All real and alleged security incidents/breaches must be reported immediately to HIP Security Control Room (**0771078999**/**0472277861**/**7861**). Subsequently, PSO will contact/interact with relevant authorities as appropriate and initiate actions as per the security SOPs.

End of the Document