
**Ships and marine technology —
Guidelines for Private Maritime
Security Companies (PMSC) providing
privately contracted armed security
personnel (PCASP) on board ships
(and pro forma contract) —**

**Part 1:
General**

*Navires et technologie maritime — Guide destiné aux sociétés privées
de sécurité maritime (PMSC) fournissant des agents de protection
armés embarqués sous contrat privé (PCASP) à bord de navires (et
contrat pro forma) —*

Partie 1: Généralités



Sample Document

get full document from standards.iteh.ai



COPYRIGHT PROTECTED DOCUMENT

© ISO 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Security management system elements for Private Maritime Security Companies (PMSC)	3
4.1 General requirements	3
4.1.1 Understanding the PMSC and its context	3
4.1.2 Understanding the needs and expectations of interested parties	4
4.1.3 Determining the scope of the security management system	4
4.1.4 Security management system	4
4.1.5 Leadership and commitment	4
4.1.6 Competence	5
4.1.7 Organizational roles, responsibilities and authorities	5
4.1.8 Structure of the organization	6
4.1.9 Financial stability of the organization	6
4.1.10 Outsourcing and subcontracting	7
4.1.11 Insurance	7
4.2 Planning	7
4.2.1 Security management policy	7
4.2.2 Actions to address risks and opportunities	8
4.2.3 Security objectives and plans to achieve them	8
4.2.4 Legal, statutory and other regulatory requirements	9
4.2.5 Authorization and licensing of firearms and security related equipment	10
4.3 Resources	11
4.3.1 General	11
4.3.2 Selection, background screening and vetting of security personnel, including PCASP	11
4.3.3 Selection, background screening and vetting of sub-contractors	12
4.4 Training and awareness	12
4.4.1 General	12
4.4.2 Training standards	12
4.4.3 Training procedures and protocols	13
4.4.4 Firearms training	14
4.4.5 Training records	15
4.5 Communication and awareness	15
4.5.1 Awareness	15
4.5.2 Internal and external communication	15
4.6 Documented information and records	16
4.6.1 General	16
4.6.2 Control of documented information	16
5 Operation	17
5.1 Operational planning and control	17
5.2 Command and control of security personnel including security team, size, composition and equipment	18
5.2.1 Command and control	18
5.2.2 Size and composition of security team	18
5.3 Guidance on Rules for the Use of Force (RUF)	19
5.4 Incident management and emergency response	19
5.5 Incident monitoring, reporting and investigation	20
5.6 Scene management and protection of evidence	20
5.7 Casualty management	21

5.8	Health safety environment.....	21
5.9	Client complaints, grievance procedures and whistle blowing.....	21
6	Performance evaluation	22
6.1	Monitoring, measurement analysis and evaluation.....	22
6.2	Internal audit.....	22
6.3	Management review.....	23
6.4	Nonconformity and corrective action.....	23
6.5	Continual improvement.....	23
Bibliography		24

Sample Document

get full document from standards.iteh.ai

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/TC 8, *Ships and marine technology*.

This first edition of ISO 28007-1 cancels and replaces ISO/PAS 28007:2012.

Introduction

ISO 28000 is the certifiable security management system standard for organizations which has been developed along the format of other management system standards (ISO 9001 and ISO 14001) with the same management system requirements.

ISO 28000 was developed in response to demand from industry for a security management standard with the objective to improve the security of supply chains and is certifiable in accordance with the International Accreditation Forum. In effect ISO 28000 is a risk-based quality management system for the security of operations and activities conducted by organizations. Organisations seeking to be certified to this International Standard should respect the human rights of those affected by the organisations operations within the scope of this International Standard, including by conforming with relevant legal and regulatory obligations and the UN Guiding Principles on Business and Human Rights. This part of ISO 28007 sets out the guidance for applying ISO 28000 to Private Maritime Security Companies (PMSC).

Sample Document

get full document from standards.iteh.ai

Ships and marine technology — Guidelines for Private Maritime Security Companies (PMSC) providing privately contracted armed security personnel (PCASP) on board ships (and pro forma contract) —

Part 1: General

1 Scope

This part of ISO 28007 gives guidelines containing additional sector-specific recommendations, which companies (organizations) who comply with ISO 28000 can implement to demonstrate that they provide Privately Contracted Armed Security Personnel (PCASP) on board ships. To claim compliance with these guidelines, all recommendations (“shoulds”) should be complied with.

Compliance with this part of ISO 28007 can be by first, second and third party (certification). Where certification is used, it is recommended the certificate contains the words: “This certification has been prepared using the full guidelines of ISO 28007-1 as a Private Maritime Security Company providing Privately Contracted Armed Security Personnel”.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 28000, *Specification for security management systems for the supply chain*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

Private Maritime Security Company

PMSC

organization which provides security personnel, either armed or unarmed or both, on board for protection against piracy

Note 1 to entry: Henceforth throughout this International Standard, the word “organization” refers to the PMSC.

3.2

Privately Contracted Armed Security Personnel

PCASP

armed employee or subcontractor of the Private Maritime Security Company (PMSC)

3.3

area of high risk of piracy

area identified as having an increased likelihood of piracy

3.4

guidance on the procedures or rules for the use of force (RuF)

clear policy drawn up by the Private Maritime Security Company (PMSC) for each individual transit operation which sets out the circumstances in which force, to include lethal force, in the delivery of maritime security services may be used in taking account of international law and the law of the flag state

3.5

Security Management System

SMS

risk-based security framework

3.6

interested party and stakeholders

person or organization that can affect, be affected by or perceive themselves to be affected by a decision or activity

Note 1 to entry: This denotes but is not limited to clients (ship-owners, charterers), the shipping community including seafarers, THE flag STATE, impacted communities, coastal STATES, international organizations, P and I clubs and insurers, and security training companies, certification bodies.

3.7

maritime security services

services which range from intelligence and threat assessment to ship hardening and the guarding and protection of people and property (whether armed or unarmed) or any activity for which the company personnel may be required to carry or operate a firearm in the performance of their duties

3.8

Guiding Principles on Business and Human Rights

UNGPs

guidance principles to companies on how to respect the human rights of all those affected by their operations, including developing a human rights policy, taking steps to identify, address and mitigate human rights risks and developing effective operational level grievance mechanisms

3.9

personnel

persons working for a Private Maritime Security Company (PMSC) whether as a full-time or part-time employee or under a contract, including its staff, managers and directors

3.10

risk assessment

overall process of risk identification, risk analysis and risk evaluation

[SOURCE: ISO Guide 73, definition 3.4.1]

3.11

firearms

portable barrelled weapon from which projectile(s) can be discharged by an explosion from the confined burning of a propellant and the associated ammunition, related ancillaries, consumables, spare parts and maintenance equipment used by security personnel at sea

3.12

security

process to pre-empt and withstand intentional, unauthorised act(s) designed to cause harm, damage or disruption

3.13

home state

state of nationality of a Private Maritime Security Company (PMSC), i.e. where a PMSC is domiciled, registered or incorporated

3.14**coastal state**

state of nationality of the area of transit within coastal waters

3.15**security management objective**

specific outcome or achievement required of security in order to meet the security management policy

3.16**security management policy**

overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and legal and regulatory requirements

3.17**security related equipment**

protective and communication equipment used by security personnel at sea

3.18**team leader**

designated leader of the personnel contracted to provide security services aboard the ship

3.19**threat assessment**

assessment by the organization, the client and other expert sources on the potential for acts of piracy or other threats to a specific transit or to operations more generally

3.20**top management**

person or group of people who direct and control an organization at the highest level

3.21**incident**

event that has been assessed as having an actual or potentially adverse effect

4 Security management system elements for Private Maritime Security Companies (PMSC)

4.1 General requirements

4.1.1 Understanding the PMSC and its context

The organisation should determine and document relevant external and internal factors. These include the international and national legal and regulatory environment including licensing and export/import requirements, the political, the natural and physical environment, the role, perceptions, needs, expectations and risk tolerance of the client and other interested parties and stakeholders as well as key international developments and trends in the home state, flag and coastal states and areas of operation. The organisation should also evaluate and document elements that might impact on its management of risk including its own organisation and lines of authority for operations, its capabilities in delivering objectives and policies, and the contribution of partners and subcontractors, and any voluntary commitments to which the organisation may subscribe. The evaluation should include the particular circumstances of each operation or transit and the attendant risk factors for the organisation.

The organisation should also identify, document and manage as necessary the significant risks identified by the ship owner which have prompted consideration of the use of security services which may include PCASP. Where PCASP are used, this should cover the legal requirements of the flag state, and of the coastal state where applicable and relevant, and the need for prior approval to deploy PCASP. The organisation should determine how this applies to its planning needs and expectations and that it is