BS EN 16747:2015

BSI Standards Publication

Maritime and port security services

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 16747:2015.

The UK participation in its preparation was entrusted to Technical Committee GW/3, Private Security Management & Services.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 86296 0

ICS 03.080.20; 03.220.40; 13.310

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2015.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16747

September 2015

ICS 03.080.20; 03.220.40; 13.310

English Version

Maritime and port security services

Services de sécurité maritime et portuaire

Sicherheitsdienstleistungen für Seeschifffahrt und Seehäfen

This European Standard was approved by CEN on 17 July 2015.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 16747:2015 E

Contents

Page

European foreword

This document (EN 16747:2015) has been prepared by Technical Committee CEN/TC 417 “Project Committee - Maritime and port security services”, the secretariat of which is held by ASI.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2016, and conflicting national standards shall be withdrawn at the latest by March 2016.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

1 Scope

This European Standard is a service standard that specifies requirements for quality in organization, processes, staff and management of a security services provider and/or its independent branches and establishments under commercial law and trade as a provider with regard to port and maritime security services.

This European Standard applies according to the laws and the regulations applicable in the territory of every national CEN member adopting the standard.

This European Standard does not apply to security services provided by private security companies that are subject to particular rules and conditions and/or related to a specific high-risk situation and/or the use of heavy weapons and/or special training and/or government supervision, such as security services in relation to piracy. In case such particular rules and/or conditions do not exist at national level, this European Standard can apply.

This European Standard lays down quality criteria for the delivery of security services in and to ports and in relation to maritime activities, requested and contracted upon by public and private clients or buyers. This European Standard is therefore suitable for the selection, attribution, awarding and reviewing of the most suitable provider for port and maritime security services.

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.

EN 15602, *Security service providers — Terminology*

EN 15713, *Secure destruction of confidential material — Code of practice*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 15602 and the following apply.

3.1
additional training for maritime and port security
training aimed at acquiring highly specific skills and knowledge to perform maritime and port security tasks that requires skills and/or knowledge not foreseen in basic or specialized training

3.2
basic training for maritime and port security
training aimed at acquiring the basic, common and introductory knowledge and skills to perform maritime and port security tasks

3.3
corporate governance
system of structuring, operating, directing and controlling a provider with a view to achieve long term strategic goals to satisfy shareholders, creditors, employees, customers and suppliers, and complying with the applicable legal and regulatory requirements, as well as meeting environmental and local community needs

Note 1 to entry: Corporate Governance Code indicates an internal system encompassing policies, processes and people, which serves the needs of shareholders and other stakeholders, by directing and controlling management activities with good business savvy, objectivity, accountability and integrity.

3.4
customer
public and/or private client or buyer of security services related to maritime and port security

3.5
incident preparedness and operational continuity management
systematic and coordinated activities and practices through which an organization optimally manages its risks and the associated potential threats and impacts there from

3.6
maritime and port security
combination of measures and human and material resources intended to secure and safeguard international or domestic shipping, ports and maritime environment

3.7
piracy
illegal acts of violence or detention, or any act of depredation, committed for private ends and directed:

— on the high seas, against another ship, or against persons or property on board such ship;

— against a ship in a place outside the jurisdiction of any state;

— any act of voluntary participation in the operation of a ship with knowledge of facts making it a pirate ship

3.8
port
specified area of land and water where port facilities are situated and that contains infrastructure, equipment, storage and other related facilities

3.9
port facility
location where the ship/port interface takes place; this includes areas such as anchorages, awaiting berths and approaches from seaward, as appropriate

3.10
provider
security service company and/or its independent branches and establishments under commercial law and trade offering port and maritime security services and employing licensed security officers/security guards and other security staff, licensed or authorized by national competent authorities, if applicable

3.11
screening
searching
application of technical or other means which are intended to identify and/or detect prohibited articles, illegal goods or persons

3.12
ship/port interface
interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons or goods or the provision of port services to or from the ship

3.13
security officer/security guard for maritime and port security
any person licensed by the appropriate authority who is paid a fee, wage or salary and is trained and screened and performs one or more of the following functions:

— prevention or detection of intrusion, unauthorized entry (access control) or activity, vandalism or trespass on public or private property;

— prevention or detection of theft, loss, embezzlement, misappropriation or concealment of merchandise, money, bonds, stocks, notes or valuable documents or papers;

— protection of individuals from bodily harm;

— environmental protection and management in rural and maritime domains;

— enforcement of (while obeying) established company rules, regulations, policies and practices related to crime reduction;

— reporting and apprehension of violators as defined by national law

3.14
specialized training for maritime and port security
training aimed at acquiring the necessary skills and in-depth knowledge to perform specific maritime and port security tasks in accordance with clients/site/contracts etc. special needs

4 Compliance with applicable national and EU-legislation

The provider should respect all applicable legislation in the field of private security, labour and social related matters and occupational health and safety.

In particular, the provider should respect

— Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security [21], and

— EU Directive 2005/65/EC of 26 October 2005 on enhancing port security [20].

5 Subcontractors

When the provider subcontracts any element of its services, the provider is responsible for the subcontractor meeting all the requirements of this European Standard.

6 Temporary or leased workers

When the provider is using temporary or leased workers, it is the provider's responsibility to guarantee that both the temporary work agency and temporary work agents meet all the requirements of this European Standard.

7 Quality related to the organization of the provider

7.1 General

Where applicable, the provider shall be authorized by the competent authorities to provide maritime and port security services if those are already specified and/or regulated by public authorities.

A provider shall only provide private security services for which the provider has obtained the necessary authorization from the competent authority.

7.2 Organization

7.2.1 Structure and organization

The provider shall demonstrate that he has the necessary capacity in terms of infrastructure, staff and procedures to guarantee the full execution of all terms and clauses of the contract between the service provider and the customer.

The provider shall demonstrate that its owners, board members and management have a clear record regarding previous similar functions in other private security companies.

The provider shall disclose information to the potential customer about its organizational structure, its dedicated responsible management if applicable, the range of services it is authorized to provide and the length of time it has been operating in port and maritime security.

The provider shall:

a) have a management structure showing command control and accountability at each level of operation;

b) have a code of conduct on drugs and alcohol;

c) have a code of conduct about operational procedures (e.g. appearance, attitudes, punctuality);

d) clearly communicate structures and procedures to all operational levels;

e) have certification, if required by national or international regulations;

f) operate a complaints management system in accordance with quality management systems;

g) have secure storage of important and confidential documents related to the contract;

h) operate under confidentiality management of information and data related to the business;

i) provide rules for making contract information available to third parties;

j) have an operational presence at the site of the provision of the service for the duration of the contract, or at least for the duration of the execution of the services;

k) disclose the structure of its ownership as well the *curricula vitae* of its management;

l) disclose upon request of a potential customer any unspent criminal convictions or undercharged bankruptcy of a principal or director;

m) give information on its membership in professional organizations;

n) give information on the compliance of its activities with applicable legislation regarding the protection of environment.

The provider shall be able to demonstrate to the potential customer, should the potential customer require so, the above before signing the contract.

The provider can disclose to the potential customer other relevant information such as on other certification.

The provider shall demonstrate that it will be able to employ at the start of the contract enough screened, certified and trained staff to fulfil all of its contractual obligations.

In case of a renewal of a contract to the same provider, the provider shall demonstrate that it has a comprehensive methodology (transition plan) to implement a smooth detailed and efficient transition from the existing services to the ones it is providing on the new contract.

In case of the transition of a contract to a new provider, the out-going provider shall establish and implement a transition plan that shall also cover all the relevant procedures for transition to the new provider.

7.2.2 Financial and economic capacity

The provider shall disclose the following information to the potential customer regarding:

— balance sheets and profit and loss statements for the past three financial years if their publication is compulsory under the legislation or practice in the country in which the applicant is registered;

— valid tax clearance certificate where relevant;

— current bankers references;

— clearance certificate from social security authorities with regard to necessary social security fees where relevant.

7.2.3 Incident preparedness and operational continuity management

The provider shall establish a documented business continuity policy including operational contingency plans.

7.2.4 Human resources management

7.2.4.1 General

The provider shall have a human resource policy in place, which shall include the following:

a) respect of labour and social law and conventions (such as collective labour agreements);

b) respect of law and regulations regarding health and safety and appropriate internal policies for health and safety;

c) maintaining information/data on staff structure, staff numbers (operational and administrative staff, the level of staff turnover among full-time, part-time and temporary staff and the evolution of employee turnover over the last three years);

d) recruitment policy including job description;

e) policies for retention of staff;

f) policies for career development;

g) training policy;

h) absenteeism reduction policies;

i) policies for equal opportunities;

j) disciplinary procedures;

k) inspection/supervision;

l) operational management;

m) staff satisfaction ratios;

n) staff representation (participation in decision-making).

7.2.4.2 Staff motivation

The provider shall demonstrate its policy for motivating security staff. This policy shall include at least the following:

— methodologies used;

— motivation measuring system;

— motivation techniques;

— responsibility on the job;

— self-management (shift work, measures against boredom);

— communication on the job (dealing with passenger/staff);

— safety consciousness.

7.2.4.3 Staff performance management policy

The provider shall implement a clearly defined staff performance management policy.

7.2.4.4 Terms and conditions of employment

A security officer/security guard shall only be employed by the provider through a written employment contract signed by both parties.

This contract shall state the terms and conditions of employment, which shall at least include details of the following:

a) job title;

b) effective start date;

c) a probationary period, if required;

d) a provisional period subject to individual security screening;

e) pay and allowances in accordance with existing and applicable rates in force;

f) hours and days of work;

g) leave entitlement;

h) conditions of payment during absences through illness;

i) pension entitlement;

j) industrial injuries procedures;

k) equipment and/or clothing supplied;

l) disciplinary and appeals procedures;

m) terms of notice of termination of employment.

7.2.4.5 Breach of terms and conditions of employment

The provider shall clearly demonstrate in a written way that in its contractual conditions is stated that the following elements can constitute a breach of terms and conditions of employment by a member of staff if this member of staff

a) neglects to complete a required task at work promptly and diligently, without sufficient cause,

b) leaves a place of work without permission, or without sufficient cause,

c) makes or signs any false statements, of any description,

d) destroys, alters or erases documents or records without permission,

e) divulges matters confidential to the organization or customer, either past or present, without permission,

f) receives gratuities or other consideration from any person, fails to account for equipment, moneys or properties received in connection with the business,

g) is incivic to persons encountered in the course of duties, or misuses authority in connection with business,

h) uses uniform, equipment or identification without permission,

i) reports for duty under the influence of alcohol or drugs, or use of these while on duty,

j) fails to notify the organization immediately of any conviction for a criminal or motoring offence, or any law enforcement caution or any summons or charge with any offence,

k) permits unauthorized access to the customer's premises to any person,

l) carries off equipment not issued as essential to an employee's duties, or uses a customer's equipment or facilities without permission,

m) does not respect or violates the customer policies, regulations and guidelines.

7.2.4.6 Identification of staff

The provider shall ensure that all his staff can be identified as being employed by it. The identification shall include the following elements, in a clearly visible way, as far as national regulations do not exist:

— identification details of the provider;

— identification details of the licensed security officer/security guard;

— the identity card's expiry date;

— a photograph of the licensed security officer/security guard.

The provider shall ensure that all his staff complies with all national and international legislation related to identification of staff.

Providers shall have strict procedures for managing issuing, delivering, withdrawing, renewing and keeping records and tracks, disposing of badges and for keeping all concerned parties informed.

7.2.4.7 Uniform

Providers shall comply with national regulations regarding uniforms.

When on duty, security officers/security guards shall wear the uniform supplied by the provider and/or the customer.

Security officer's/security guard's uniforms shall clearly display the insignia of the provider. Uniforms shall be readily distinguishable from those of the civil emergency services or armed forces or other public security forces. When and where necessary, personal protective equipment (PPE) shall be worn in line with international, national regulations or as agreed with the customer.

Providers shall ensure that the staff maintains appropriate standard of appearance.

Provisions of this paragraph will not be applied to non-uniformed security officers/security guards as allowed by national regulations.

7.2.5 Insurances

Providers shall comply with international and/or national regulations regarding insurances.

Insurances of the provider shall cover the following:

— accidents to employees while on duty;

— general liability;

— social security/public liability.

The provider shall disclose to the customer information and its policy and views regarding third party liability.

The provider shall ensure there is sufficient evidence of appropriate insurance coverage to the customer.

When using sub-contractors the provider shall ensure that sufficient insurance to cover commensurate with the business undertaken.

7.2.6 References

Provider shall disclose all necessary relevant references to the customer.

7.2.7 Corporate governance

The provider shall have a structured corporate governance policy or equivalent and shall establish proof of it.

EXAMPLE Governance policy or equivalent includes for example:

— code of conduct for directors and employees;

— internal and external control procedures and audits;

— reporting arrangements – financial and operational;

— strategic and corporate planning.

7.2.8 Contract

A written contract between the provider and the customer shall be signed by both parties (see also Clause 9). The contract shall state the rights and obligations of the provider and of the customer including respective liabilities and responsibilities and financial and economic aspects. It shall also mention agreement between parties regarding sub-contracting.

7.2.9 Working environment and systematic improvements

Provider shall have a structured occupational health and safety management system, e.g. OHSAS 18001 [14]. OHSAS 18001 is an Occupation Health and Safety Assessment Series for health and safety management systems. Such a management system is intended to help the provider to control occupational health and safety risks. The provider shall demonstrate that the customer is always actively involved.

The provider shall prevent occupational hazards.

Working environment shall be in line with social and technical development that has an impact on health and safety.

Work shall be planned in a manner that it can be performed in a safe and healthy environment.

The provider shall investigate accidents together with the health and safety representative of the staff if present, continuously assess risks and take all precautions necessary.

The provider shall document the working conditions and the action plans and measures to improve them.

The provider shall also make preventative medical care available to the employees suited to their working conditions. In case of a health and safety incident the provider shall also make medical treatment available.

8 Staff

8.1 Staff selection (operational) – Methodology

8.1.1 General

The provider shall have documented processes for the identification, selection and recruitment of staff.

8.1.2 Function profile

A job description and assignment instruction for each function shall be available.

8.1.3 Publicity of needed profiles

If requested by the customer, the provider shall inform on the policy of identifying potential candidate security officers/guards.

8.1.4 Criteria to be fulfilled for employment

All candidates shall meet all applicable international and/or national legal conditions for employment in maritime and port security services.

Criteria shall include the following:

— valid ID – recognized official identification;

— minimum legal age for employment;

— certificate of good conduct;

— security vetting;

— medical certificate required where relevant to the job description;

— necessary interpersonal skills relevant to the activity to be undertaken;

— language skills in the relevant and needed working language(s);

— eligibility for all other necessary licences and authorizations needed.

The provider shall make sure that all the criteria are met, at any stage of the recruitment process.

8.1.5 Selection

The provider shall have each candidate security officer/guard to fully complete a written application document containing the following information:

— personal data;

— educational background;

— professional experience;

— employment and personal references;

— details on work and residence permits, if applicable;

— statement on criminal records, if applicable;

— driver's licence details, if applicable;

— general information on physical and/or medical condition applicable to the job description;

— possibilities of geographical mobility.

8.1.6 Interview

The provider shall conduct with every eligible candidate security guard/officer an interview. This interview shall be conducted by a competent recruitment officer.

The provider shall use an interview assessment form. The interview assessment form shall include as a minimum the following criteria:

— application form verification;

— understanding of the job and its requirements;

— motivational assessment;

— external appearance;

— personality characteristics;

— communication skills;

— relevant language skills;

— social attitudes (e.g. equality to work, security, colleagues, superiors, customer service and team spirit);

— integrity;

— personal interests;

— inform candidate of wage, job description (also on the company's policy on drugs, alcohol and other company's code of conduct), company details and applicable national legislation.

8.2 Recruiting

8.2.1 General

The provider shall ensure that only candidate security guards/officers having met all the requirements set out in this European Standard enter the company on the basis of an employment agreement in order to do maritime and port security services.

8.2.2 Individual/personal file

8.2.2.1 General

An individual file shall be established and maintained for each security staff member.

The file shall contain all documents, training certificates, proofs and other information related to the individual as required by this European Standard and/or by national regulation.

8.2.2.2 Psychometric and psycho-technical tests

Psychometric and psycho-technical tests shall be recommended to be used as an additional selection tool where applicable and feasible.

8.2.2.3 Career opportunities

The provider shall inform staff entering the company about career opportunities.

8.3 Training

8.3.1 References for training

Training of port and maritime security staff should take into account the following:

— EN 15602, *Security services providers – Terminology*;

— EN 15713, *Secure destruction of confidential material – Code of practice*;

— International Convention for the Safety of Life at Sea (SOLAS), 1974 and subsequent amendments

— ISPS (International Ship and Port Facility Security) Code [10],

— EU Directive 2005/65/EC of 26 October 2005 on enhancing port security [20];

— Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security [21];

— IMDG Code training for the Port Security Operations.

The detailed content of this training may vary from country to country.

8.3.2 Training policy and methodology

All training for maritime and port security shall be performed in such a way that maximum training results are obtained and that maximum skills can be acquired by the security officers/security guards. Given the variety of already established training levels at national level, either by law, or by providers' investments and efforts, or by candidate security officer's/security guard's own initiative, all instruments, tools, and methodology used for training shall be adapted to national needs and designed in such a way that maximum results can be achieved.

All training shall be conducted in a learning environment and in conditions, which shall include learning blocks and shall facilitate the teaching and the learning process from both the didactical and the pedagogical aspects. A specified procedure shall outline the standards of the training, in all its aspects.

All training tools shall be user-friendly, covering all subjects of the training (as detailed in the training syllabus) and detailing all the elements of the training session(s), such as time frames, accessories, hand-outs, training methods etc.

A detailed and contract/site/environment/tasks adapted training itinerary for entitled security officers/security guards (training syllabus) shall reflect the defined needs of the client, the requirements of national and international regulations.

Training policy and methodology requirements are as follows:

a) Training policy, planning, contents and performance of training shall include, as a minimum, all elements mandated by national and international regulations.

b) The provider shall ensure that the requirements and expectations of clients (contract specific training) shall be reflected in the training contents.

c) Staff of providers implementing maritime and port security shall be trained for each assignment that they shall perform.

d) All training sessions shall be planned and contents defined including theoretical, practical and on-the-job training, as to fit the necessities of the job assignment.

e) Training shall be concluded with a trainee (candidate security officer/security guard or security officer/security guard) assessment, in order to verify and ensure that the trainee (candidate security officer/security guard or security officer/security guard) has performed to the level defined by the appropriate authority/regulator/company or other body that shall make entitlement possible. The requirements and expectations of clients shall be reflected in the training assessment.

f) All training shall be followed by a purposeful, planned, monitored and improvement oriented on-the-job training.

g) Training shall be performed in appropriate training environment and conditions in order to enable an effective and efficient learning process.

h) Training shall be performed in duly recognized training centres for maritime and port security and/or in internal training departments established by the provider.

i) Training shall be performed by qualified trainers or experts in their own area of competence; this area of competence shall be directly related to the training content.

j) Recurrent training shall be conducted for every security officer/security guard so as to ensure updating of know-how and expertise.

k) An internal self-testing system shall be established by the provider, in order to verify and measure staff's proficiency and alertness level.

l) Training as well as testing shall be documented.

8.3.3 Basic training content

Before being able to perform any port or maritime security task, every security guard/officer shall have acquired basic knowledge and understanding of at least the issues listed below.

The acquirement of the knowledge and skills necessary for each security task can be done through basic training and/or specialized training and/or additional training.

The basic requirements shall include the following:

a) rights, role, responsibility and procedures as a security guard/officer;

b) maritime and port stakeholder introduction (e.g. tasks, entities) and definitions (e.g. oil harbour, passenger terminal, container terminal);

c) international and/or national maritime and port security legislation, regulations and policies;

d) general maritime and port safety issues with a security aspect;

e) general security responsibilities (e.g. designed authority, coast guard, police, customs, port and vessels companies own responsibilities);

f) security awareness, threat identification, recognition and response (e.g. inventory of the threats, modus operandi);

g) port versus vessel security actions (including waterside security), including as a part of the supply chain security;

h) knowledge of emergency preparedness procedures and contingency plans (e.g. evacuations, firefighting, detailed procedures);

i) drills and exercises (e.g. quarterly drills, yearly exercises);

j) techniques used to circumvent security measures (e.g. modus operandi);

k) crowd management and control techniques (e.g. evacuation, riot management, strikes);

l) security related communications and reporting (e.g. handle equipment in a secure way, security and incident reporting) and vocabulary in relation to maritime and port security;

m) operational procedures and operations of security equipment and systems (e.g. access control systems);

n) general inspection, control, and monitoring techniques, including basic access and exit controls;

o) basic customer relations and customer services;

p) methods of physical searches of persons, personal effects, baggage, cargo and ship's stores (e.g. screening, profiling, random searches, procedures);

q) general introduction to data and privacy protection;

r) knowledge of terms, abbreviations and definitions;

s) knowledge of the location of the security restricted areas and the access procedures;

t) basic knowledge of English language for professional purposes;

u) interpersonal interactions (e.g. assistance to persons, assistance to persons with specials needs, facilitation, stress handling).

8.3.4 Training for specific tasks

For the performance of the specific security tasks listed below, the training shall include at least the issues identified below for each task:

— screening of persons, cargo, goods, vehicles or any other screenable objects in view of detection arms, weapons, explosives, radioactive or other dangerous goods which constitute a security threat;

— profiling of persons in view of detecting and preventing criminal activity or intention of such activity;

— handling of detection dogs in view of detecting persons, drugs, explosives etc.;

— X-ray screening of containers and freight;

— performance of public security duties;

— use of weapons;

— secure loading/unloading of dangerous goods and/or substances (liquid or dry bulk products).

All selected training programs listed below shall be provided to security officers/security guards if and where needed. If provided, they shall at least include the elements listed below for each specialized training:

a) specialized training for screening process of passengers, personnel and crew, cargo, cabin baggage/carry-on items that shall cover following issues:

   1) general:

      — the organization of the structure of the security checkpoints;

      — questioning of persons about their items;

      — knowledge of exempted categories of persons and items;

      — profiling of people;

   2) screening of persons:

      — key elements of effective screening of persons;

      — technology versus search by hand;

      — specific issues related to search by hand (e.g. sex, culture, disabilities);

   3) screening of items:

      — key elements of effective screening of items;

      — technology versus search by hand;

      — key elements of an effective search of cargo or carry-on items;

b) screening of hold baggage that shall cover following issues:

   1) the organization of the structure of the hold baggage screening;

   2) key elements of effective screening of hold baggage;

   3) procedures for unaccompanied hold baggage;

   4) key safety procedures (e.g. dangerous goods);

c) cargo and mail security that shall cover the following issues:

   1) the organizational structure of cargo facilitation;

   2) key elements of effective screening of cargo and mail;

   3) key safety procedures (e.g. dangerous goods);

d) X-ray and other detection systems and devices training that shall cover the following issues:

   1) organizational structure of the X-ray screening point and of other detection systems and devices;

   2) understanding the operational procedures;

   3) aspects of radiation, health and safety;

   4) knowledge of threat image projection (TIP) software;

   5) use of computer based training (CBT) for the interpretation of X-ray images and other detection system images;

e) searching of vehicles that shall cover following issues:

   1) the organizational structure of the vehicle check point(s);

   2) principles of random selection of vehicles and search ratio;

   3) key elements of effective screening of vehicles and its occupants;

f) ship and port protection and check/search procedure that shall cover following issues:

   1) the organizational structure;

   2) principles of check/search and protection;

   3) key elements of effective check/search of port operation vehicles.

8.3.5 Additional training

If and when necessary to supplement all above-mentioned trainings, all security officers/security guards shall receive additional training to develop previously achieved skills and/or to acquire new skills.

8.3.6 Training for supervision

Security officers/security guards who perform supervisory tasks, in their role as field-managers, generally reporting directly to middle or higher management, need to be able to confront and solve skilfully a wide variety of complex maritime and port security related situations. For this purpose, they shall be specifically trained, in both management and purely profession-related subjects: experience and seniority alone do not suffice in fulfilling supervisory duties and responsibilities.

Training for supervision shall be conducted by qualified trainers. The standards of sessions of training for supervision shall be appropriate to this level of training.

A security officer/security guard who performs the supervision of tasks executed by security officers/security guards with a basic training shall at least have successfully completed basic training themselves.

A security officer/security guard who performs the supervision of tasks executed by security officers/security guards with a specialized training shall have successfully completed the concerned specific training.

The training for supervision is additional to the legislative requirements and shall cover at least the following items:

— management skills (including people management and leadership skills);

— problem solving skills (e.g. internal conflicts);

— contingency and continuity management;

— enhanced level customer relations and passenger service skills;

— advanced knowledge of port authorities and other relevant parties.

8.3.7 Structured on-the-job training

Structured on-the-job training of every security officer/security guard is a necessary and critical phase in each entitled security officer's/security guard's professional development, as it aims to translate theoretical knowledge acquired during the basic training and/or specialized training into practical implementation, to develop team attitude and to enhance the feeling of belonging and loyalty.

All successfully completed basic training shall be followed by a comprehensive structured and monitored on-the-job training.

All successfully completed specialized training shall be followed by a comprehensive structured and monitored on-the-job training.

On-the-job training shall be supervised by a person fulfilling the following qualities:

— thoroughly knowledgeable and authoritative;

— proven record of experience;

— ability to transfer knowledge;

— trained for mentoring;

— having completed successfully the basic training and/or specialized concerned training.

The monitoring/supervision process of the on-the-job-training shall include

— observation,

— drills and exercises,

— feed-back to and from trainees,

— instructions and corrections,

— final testing (theoretical, practise) and assessment.

On-the-job training shall be thoroughly and continuously documented in appropriate checklists and assessment forms, so as reflect the trainee's progress and level of expertise. The parameters of assessment shall be based at least on following elements:

— compliance with procedures;

— functioning in the real environment and under pressure;

— customer service;

— work- and company-attitudes.

8.3.8 Refresher training

To maintain a high level of alertness and security awareness, refresher (recurrent) training shall be mandatory to all entitled security officers/security guards, whether the security officer/security guard has only received basic training or whether the security officer/security guard has also received specialized training.

The refresher training is additional to the legislative requirements.

The main purpose of the refresher training shall be

— to maintain a high level of alertness and security awareness,

— to refresh and review knowledge,

— to review and learn from past events,

— to adapt skills to changed requirements and conditions,

— to maintain a high level of expertise.

Refresher training shall

— follow a yearly plan which takes into consideration any new relevant elements of material related to national and international regulations, by policies, by clients or by the provider,

— Include an update of theoretical and practical knowledge,

— include elements of testing (e.g. exams, role play, practical testing, drills),

— be given by skilled and qualified trainers,

— be adapted to the related security plans of the facility,

— be undertaken at least every 12 months,

— require a minimum number of hours per year and per entitled security officer/security guard, unless already stipulated by legislation. This minimum number of hours shall be specified by the providers and can be no less than 8 h.

8.3.9 Trainer's tasks and responsibilities

The trainer's responsibilities shall be to determine the appropriate teaching and learning methods and tools for the information to be delivered meeting the requirements of the legislation (when applicable), of the provider, of the client, and - most importantly - of the trainee.

The trainer responsible for testing the trainee shall not be the trainer responsible for the training of the trainee.

8.3.10 Testing of training

The provider shall establish its own internal training testing system to measure the quality of the training followed by every security officer/security guard.

The results of these tests shall clearly indicate the outcome of the training and, if and when necessary, measures for improvement of training, form a methodological, formal or content point of view. In case such measures are indicated, the provider shall implement them as soon as possible.

8.3.11 Evaluation of training results

The provider shall establish its own internal testing methodology, which shall include the following elements:

— verification of theoretical knowledge;

— verification of practical implementation skills (exercises, role-play etc.);

— vigilance tests (drills, simulation of real events etc.);

— audits and inspections;

— implementing corrective action plans.

All entitled security officers/security guards shall be tested regularly (and at least every 6 months) to prove competency, using any of the methods mentioned above.

A newly entitled security officer/security guard shall pass a vigilance test (drill) during the first 30 days following the qualification. The security officer/security guard shall be informed about this.

8.3.12 Training data

The provider or training centre shall nominate a training supervisor.

In case training has been followed in a training centre outside the provider, the training supervisor of the training centre shall inform the training supervisor of the provider of all elements listed below.

Training data revealing any personal data shall not be made available to third parties other than relevant management of the providers, unless stipulated otherwise by international or national applicable legislation and regulations.

Information about whether or not an entitled security officer/security guard is qualified for the tasks to perform or information regarding the evaluation of training of a security officer/security guard shall only be made available to the customer if this is explicitly stipulated in the commercial contract between the provider and the customer and in accordance with relevant regulations regarding the respect of privacy and data protection.

Information about the provider's education and training programs, methodology, content and duration shall be accessible to the customer if the customer requires so.

The provider shall maintain for every security officer/security guard a documented and written training file. This file shall be at all times accessible by the concerned security officer/security guard, shall be co-signed by both parties (both the initial files and all subsequent additions and modifications) and shall include the following information:

— training certificates, type of training courses followed, training courses successfully completed, training subjects, dates, location, time frame etc.;

— all written and graded exam(s), test(s), assessment(s) and results thereof;

— documentation of all practical exams, test, role plays, and situation exercises etc., on a form describing the contents and results;

— trainee evaluation form(s), detailing results of assessment(s), job related evaluation(s) of the trainee and recommendations for further coaching and training;

— trainee on-the-job evaluation form(s) with qualification and/or recommendation for further coaching and/or training.

9 Contracts

9.1 Quality management system

The provider shall run a quality management system and be able to demonstrate it (e.g. EN ISO 9001 [1]).

9.2 Contract management/operations

9.2.1 Security performance/results measurement system

The provider shall maintain a measurement system to regularly and periodically evaluate the performance of the security services and to, if and when necessary, implement corrective measures.

9.2.2 Contract manager

The provider shall appoint a contract manager, who bears the responsibility for the fulfilment of the terms of contract.

9.2.3 On-site supervision

The provider shall ensure that the site is regularly visited by a supervisor designated by the provider to deal with all operational issues related to the contract.

9.2.4 Interaction and communication with the customer

The provider shall demonstrate that in the contract there is a clear structure that covers both the suppliers and the client operational and administrative designated person(s):

The supplier shall use a KPI (Key Performance Indicator) to continuously and consistently evaluate the quality of the services.

9.2.5 Operational plan and rostering

The provider shall define an operational plan, which shall include the following:

a) risk assessment for the contract in question;

b) rostering;

c) standard operation procedure;

d) mobilization plan;

e) backup arrangements;

f) contingency arrangements;

g) 24-hour manned emergency telephone line;

h) transition plan;

i) performance monitoring and assessment;

j) training plan;

k) reversibility plan (transferability between providers);

l) reporting structure (within the provider and with the client);

m) disaster recovery;

n) insurance arrangements and relevant procedures;

o) licensed security officer/security guard appropriate qualifications.

9.3 Equipment, systems, vehicles and dogs

The owner of equipment, systems and vehicles being used by the provider is responsible for the full maintenance and proper operational use of it. International, national or local regulations shall apply as well as manufacturer's guidelines. The responsibility for maintenance can alternatively be delegated by the owner to another party.

International, national or local regulations shall apply to the use of dogs provided in carrying out specific screening activities of the contract.

9.4 Cooperation with other relevant parties

The provider shall cooperate with other relevant parties (e.g. police, fire brigade, port authority (e.g. regulated by ISPS Code [10], EU Directive 2005/65/EC [20]), ship staff, other providers) when required.

While on board any vessel in client's area of responsibility, the provider and the security staff shall comply with the owners' health and safety requirements as far as the client notified this to the providers' security staff.

9.5 Provider's right to sub-contract

The provider shall not sub-contract any of their contracted obligations without the prior written consent of the client. In the event of such permitted sub-contracting, the provider shall remain fully liable for the due performance of their obligations under contract.

Where the providers' sub-contracted staff is not in direct employment by the provider, then the provider shall ensure that such sub-contracted staff agrees to be bound by all the terms and conditions under the contract with the client.

9.6 Confidentiality

All documents and information between provider and customer and related to the contract are confidential to both parties (see EU Directive 95/46/EC [19]).

The provider shall maintain a separate record for each contract accessible only to authorized persons.

Amended and/or updated records shall be identifiable by date and clearly distinguishable from previous versions.

Information stored in an electronic retrieval system shall be regularly backed-up. The back-up copies shall be stored separately.

NOTE Further information on the management of electronic data can be found in ISO/IEC 27002 [5].

All documentation concerning the contract shall be kept for duration in accordance with national legislation and for at least 12 months after termination of the contract.

Disposal of documentation shall be in accordance with EN 15713.

Annex A
(informative)

A-deviations

A-deviation: National deviation due to regulations, the alteration of which is for the time being outside the competence of the CEN-CENELEC national member.

This European Standard does not fall under any Directive of the EU.

In the relevant CEN-CENELEC countries, these A-deviations are valid instead of the provisions of the European Standard until they have been removed.

Clause	Deviation
7.2.4.4 "Terms and conditions of employment"	Sweden - The Swedish Employment protection act SFS 1982:80 (Lagen om anställningsskydd) specifically § 6c and generally § 4 – § 6g contains rules about employment contracts and referring to the social partners
7.2.4.5 "Breach of terms and conditions of employment"	Sweden - The Swedish Employment protection act SFS 1982:80 (Lagen om anställningsskydd) § 7, § 18 and generally § 7 – § 27 regulates the procedures for the breach of employment

Bibliography

[1] EN ISO 9001, *Quality management systems — Requirements (ISO 9001)*

[2] EN ISO 14001, *Environmental management systems — Requirements with guidance for use (ISO 14001)*

[3] ISO 26000, *Guidance on social responsibility*

[4] ISO 31000, *Risk management — Principles and guidelines*

[5] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[6] ISO/PAS 28007:2012, *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)*

[7] ADR 1.10, *Carriage of Dangerous Goods by Road – Guidance on the appointment of a Dangerous Goods Safety Adviser*

[8] IMO IE110E, *International Convention for the Safety of Life at Sea (SOLAS) – Consolidated edition, 2009*

[9] IMO I175E, *SOLAS Amendments 2008 and 2009*

[10] IMO I116E, *ISPS Code, 2003 edition (International Ship and Port Facility Security Code and SOLAS Amendments 2002)*

[11] IMO IH200E, *International Maritime Dangerous Goods (IMDG) Code, 2010 Edition (inc Amendment 35-10), 2 Volumes*

[12] IMO IH210E, *International Maritime Dangerous Goods (IMDG) Code Supplement*, 2010 Edition

[13] IMO IB117E, *ISM Code: International Safety Management Code and Guidelines on Implementation of the ISM Code, 2010 Edition*

[14] OHSAS 18001, *Occupational Health and Safety Management*

[15] *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,* 1988 URL: http://www.unodc.org/unodc/en/treaties/illicit-trafficking.html (2015-07-28)

[16] *United Nations Convention against Transnational Organized Crime and the Protocols Thereto* URL: http://www.unodc.org/unodc/en/treaties/CTOC/ (2015-07-28)

[17] *European Training Programme for Maritime Security Personnel – ISPS Code*, Confederation of European Security Services, 2008

[18] *European Training Programme for Maritime Security Personnel – ISPS Code Trainer Guidelines*, Confederation of European Security Services, 2008

[19] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11.1995, p. 31–50

[20] *Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security*, OJ L 310, 25.11.2005, p. 28–39

[21] *Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security*, OJ L 129, 29.4.2004, p. 6–91

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™