SLOVENSKI STANDARD
oSIST prEN 17483-1:2020

01-julij-2020

Zagotavljanje zasebne varnosti za zaščito kritične infrastrukture - 1. del: Splošne zahteve

Private security provision for the protection of Critical Infrastructure - Part 1: General requirements

Private Sicherheitsmaßnahmen zum Schutz kritischer Infrastrukturen

Dispositions de sécurité privée pour la protection des infrastructures critiques - Partie 1 : Exigences générales

Ta slovenski standard je istoveten z: prEN 17483-1

ICS:

03.080.99	Druge storitve	Other services
13.310	Varstvo pred kriminalom	Protection against crime

oSIST prEN 17483-1:2020 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 17483-1

April 2020

ICS 03.080.99; 13.310

English Version

Private security provision for the protection of Critical Infrastructure - Part 1: General requirements

Dispositions de sécurité privée pour la protection des infrastructures critiques - Partie 1 : Exigences générales

Private Sicherheitsmaßnahmen zum Schutz kritischer Infrastrukturen

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 439.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. prEN 17483-1:2020 E

Contents

Page

European foreword

This document (prEN 17483-1:2020) has been prepared by Technical Committee CEN/TC 439 “Private security services”, the secretariat of which is held by ASI.

This document is currently submitted to the CEN Enquiry.

1 Scope

This document is the overarching standard for the provision of private security services for critical infrastructure. It is complemented by vertical substandards for specific sectors with more detailed focus on the related services such as e.g. aviation security and maritime/port security.

It specifies service requirements for quality in organization, processes, personnel and management of a security service provider and/or its independent branches and establishments under commercial law and trade as a provider with regard to security services.

It lays down quality criteria for the delivery of security services requested by public and private clients.

This document is suitable for the selection, attribution, awarding and reviewing of the most suitable provider of security services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 15602:2008, *Security service providers — Terminology*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
critical infrastructure
asset, system or part thereof which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a society as a result of the failure to maintain those functions

Note 1 to entry: Examples of critical infrastructure sectors are given in Annex A.

3.2
insider threat
threat posed by unauthorised access, use or disclosure of privileged information, techniques, technology, assets or premises by an individual with legitimate or indirect access, which could cause harm or damage

3.3
insider threat policy
policy aimed to detect and mitigate insider threats

3.4
risk assessment
systematic process for the identification, analysis and evaluation of threats to determine the impact of the consequences of hazards and threats relative to the probability of their occurrence

3.5
security analysis

total of defined organisational, personnel, technical and structural security measures for the prevention and/or averting of dangers through written analysis of possible attack and damage scenarios with the aim of achieving a defined level of protection

Note 1 to entry: Security analyses are based on a structured approach which generally includes the following criteria:

— determination of the object to be protected and the protection aims;

— analysis of threats / damage scenarios / dangers;

— evaluation of probability of occurrence and potential extent of damage;

— development of measures to reduce damages and their probability of occurrence;

— development of measures to initiate security as early as possible (e.g. coordination of electronic and mechanical security devices to trigger an alarm before the mechanical security devices have been completely overcome);

— planning of measures and provision of means for damage control and containment in the event of damage;

— analysis of the own risk bearing capacity and assessment of the residual risk.

Even a sophisticated security analysis is not able to eliminate the residual risk completely. For this reason, crisis and disaster management is often introduced to protect life and property as far as possible in an emergency.

3.6
staff performance management policy

systematic process by which the provider involves its employees, as individuals and members of a group, in improving organizational effectiveness in the accomplishment of the providers mission and goals

Note 1 to entry: This policy is a tool which is used to communicate the organizational goal to the employees individually, allot individual accountability towards that goal and tracking of the progress in the achievement of the goals assigned and evaluating their individual performance. The staff performance management policy reflects the individual performance or the accomplishment of an employee, which evaluates and keeps track of all the employees of the organization.

3.7
sector-specific substandard

complementary vertical standards to this overarching standards within the critical infrastructure sectors

Note 1 to entry: Examples of critical infrastructure sectors are given in Annex A.

Note 2 to entry: See Figure 1

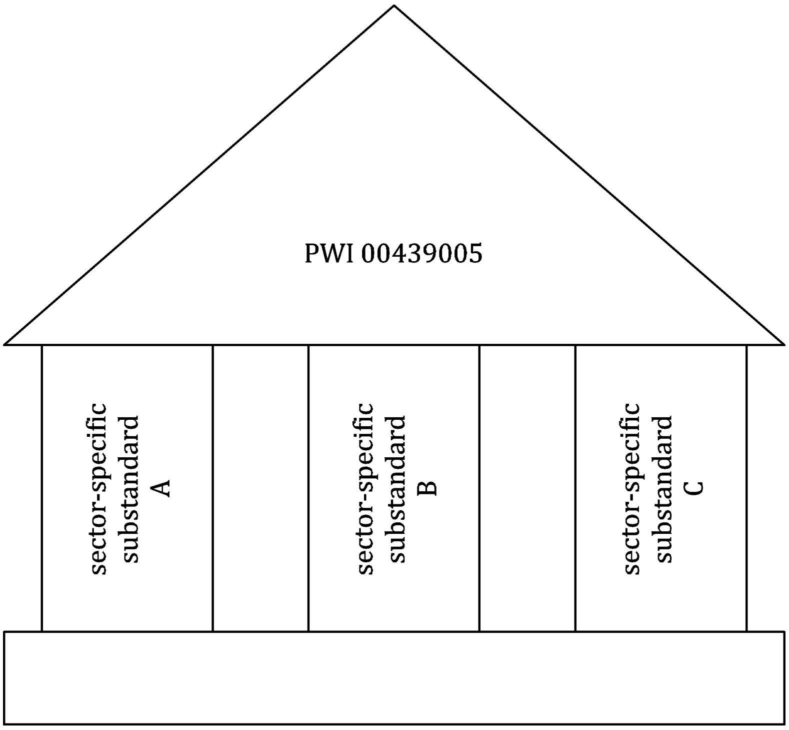
PWI 00439005
sector-specific substandard A
sector-specific substandard B
sector-specific substandard C

Figure 1 — Structure for sector-specific substandards

4 Provider

4.1 General

The provider shall be authorized by the competent authorities to provide private security services for critical infrastructure if those are already specified and/or regulated by public authorities in accordance with the national legal frameworks.

A provider shall only provide those private security services for critical infrastructure for which the provider has obtained the necessary authorization from the competent authority corresponding to the sector-specific substandard(s).

4.2 Structure

4.2.1 Management structure

The provider shall demonstrate that its owners, board members and management have a clean record, e.g. not been convicted for or pending charges for any crimes such as:

a) weapons and/or drug trafficking and/or organized crime;

b) bribery and/or corruption;

c) fraud and/or money laundering and/or financing of terrorism;

d) attempting or committing terrorist offences;

e) child labour and/or trafficking in human beings;

f) intentional crimes against human beings and public or private property;

g) tax evasion or evasion of social security contributions.

They need to hold the required licence for their function where legally applicable.

The provider shall:

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

2) have a code of conduct on ethics, drugs and alcohol;

3) have a code of conduct on compliance and corporate social responsibility;

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

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

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

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

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

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

10) have an operational presence within an appropriate distance to 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;

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

12) disclose any unspent criminal convictions or undercharged bankruptcy of a principal or director;

13) give information on its membership in professional organizations;

14) 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 client the above before signing the contract, if the potential client requires so. The provider can disclose to the potential client other relevant information such as on other certification.

4.2.2 Human resources management

4.2.2.1 General

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

a) abide by labour and social law and collective labour agreements;

b) abide by law and regulations regarding health and safety and appropriate internal policies for health and safety;

c) maintaining accurate information/data on staff structure and staff numbers;

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 and grievance procedures;

k) inspection/supervision;

l) operational management;

m) staff satisfaction ratios;

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

4.2.2.2 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 clients and colleagues);
- safety consciousness.

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

4.2.2.3 Staff performance management policy

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

4.3 Health and Safety Management

The provider shall have a structured occupational health and safety management system (e.g. ISO 45001 [10]).

NOTE ISO 45001 [10] (old: OHSAS 18001:2007 [12]) 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 prevent occupational hazards and demonstrate that the client is always actively involved.

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