SLOVENSKI STANDARD
SIST EN 17483-1:2021

01-september-2021

Storitve zasebnega varovanja - Zaščita kritične infrastrukture - 1. del: Splošne zahteve

Private security services - Protection of critical infrastructure - Part 1: General requirements

Private Sicherheitsvorkehrungen zum Schutz kritischer Infrastrukturen - Teil 1: Allgemeine Anforderungen

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

SIST EN 17483-1:2021
https://standards.iteh.ai/catalog/standards/sist/43d14ecf-eaf1-4f24-9872-4ab9075a71b2/sist-en-17483-1-2021

Ta slovenski standard je istoveten z: **EN 17483-1:2021**

ICS:

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

SIST EN 17483-1:2021 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

SIST EN 17483-1:2021

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 17483-1:2021
https://standards.iteh.ai/catalog/standards/sist/43d14ecf-eaf1-4f24-9872-4ab9075a71b2/sist-en-17483-1-2021

SIST EN 17483-1:2021

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 17483-1

June 2021

ICS 03.080.99; 13.310

English Version

Private security services - Protection of critical infrastructure - Part 1: General requirements

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

Private Sicherheitsvorkehrungen zum Schutz kritischer Infrastrukturen - Teil 1: Allgemeine Anforderungen

This European Standard was approved by CEN on 23 May 2021.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

SIST EN 17483-1:2021
https://standards.iteh.ai/catalog/standards/sist/43d14ecf-eaf1-4f24-9872-4ab9075a71b2/sist-en-17483-1-2021

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

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

© 2021 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

SIST EN 17483-1:2021

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 17483-1:2021
https://standards.iteh.ai/catalog/standards/sist/43d14ecf-eaf1-4f24-9872-4ab9075a71b2/sist-en-17483-1-2021

SIST EN 17483-1:2021

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 17483-1:2021
https://standards.iteh.ai/catalog/standards/sist/43d14ecf-eaf1-4f24-9872-4ab9075a71b2/sist-en-17483-1-2021

SIST EN 17483-1:2021

European foreword

This document (EN 17483-1:2021) has been prepared by Technical Committee CEN/TC 439 “Private 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 December 2021, and conflicting national standards shall be withdrawn at the latest by December 2021.

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

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: 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 the United Kingdom.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 17483-1:2021
https://standards.iteh.ai/catalog/standards/sist/43d14ecf-eaf1-4f24-9872-4ab9075a71b2/sist-en-17483-1-2021

SIST EN 17483-1:2021

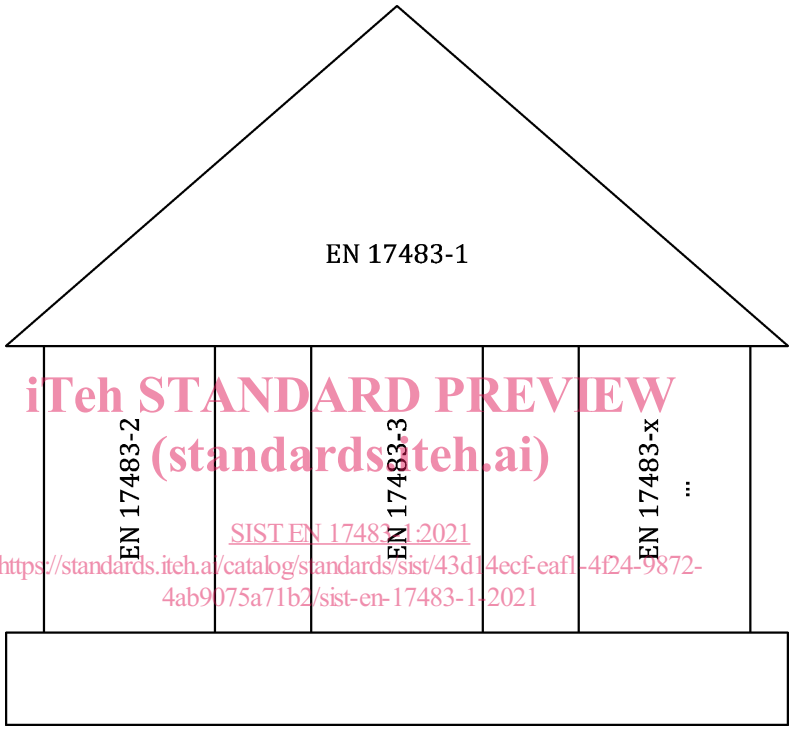
1 Scope

This document includes the main overarching requirements for the provision of private security services for critical infrastructure.

NOTE 1 This document is the first part of a series of standards on the provision of private security services for critical infrastructure. It will be complemented by other sector specific parts, which give more detailed requirements for related services such as aviation, maritime and port security.

NOTE 2 Examples of critical infrastructure sectors are given in Annex A.

NOTE 3 See Figure 1.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 17483-1:2021
https://standards.iteh.ai/catalog/standards/sist/43d14ecf-eaf1-4f24-9872-4ab9075a71b2/sist-en-17483-1-2021

Figure 1 — Structure for sector-specific standards

NOTE 4 It is important that the selection of a private security service provider always represents the best balance between quality and price. This document sets out the minimum requirements that providers should comply with in order for this balance to be struck.

It specifies service requirements for quality in the 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 of 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.

SIST EN 17483-1:2021

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, *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 https://www.electropedia.org/

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

3.1
critical infrastructure
asset, system, or a part thereof, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, where 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

SIST EN 17483-1:2021
https://standards.iteh.ai/catalog/standards/sist/45d14ec1-ea11-4124-9872-4ab9075a71b2/sist-en-17483-1-2021

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

SIST EN 17483-1:2021

3.5
security analysis
total of defined organizational, 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

SIST EN 17483-1:2021
https://standards.iteh.ai/catalog/standards/sist/43d14ecf-eaf1-4f24-9872-4ab907a71b2/sist-en-17483-1-2021

3.6
staff performance management policy
systematic process by which the provider involves its employees, as individuals and members of a group, in improving organisational effectiveness in the accomplishment of the provider's mission and goals

Note 1 to entry: This policy is a tool which is used to communicate the organisational 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.

SIST EN 17483-1:2021

3.7
management system
set of interrelated or interacting elements of an organisation to establish policies and objectives, and processes to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines, e.g. quality management, financial management or environmental management.

Note 2 to entry: The management system elements establish the organization's structure, roles and responsibilities, planning, operation, policies, practices, rules, beliefs, objectives and processes to achieve those objectives.

Note 3 to entry: The scope of a management system can include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organisations.

Note 4 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified by modifying Notes 1 to 3 to entry.

[SOURCE: EN ISO 9000:2015, 3.5.3]

3.8
key performance indicator
KPI
business statistics which measure an organisation's performance

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Note 1 to entry: KPIs show the progress (or lack of it) toward realizing the organization's objectives or strategic plans by monitoring activities which (if not properly performed) would likely cause degradation of the performance of the provider.

https://standards.iteh.ai/catalog/standards/sist/43d14ecf-eaf1-4f24-9872-4ab9075a71b2/sist-en-17483-1-2021

[SOURCE: EN 50518:2019, 3.1.21 modified — At Note 1 to entry the term provider is used instead of ARC]

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 standard(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 any of the following crimes:

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;

SIST EN 17483-1:2021

d) attempting or committing terrorist offences;

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

f) intentional crimes against human beings;

g) tax or social security fraud;

h) cyber and information security crimes.

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 code of conduct documents on ethics, drugs and alcohol, compliance and corporate social responsibility and about operational procedures (e.g. hygiene and cleanliness, behaviour, punctuality);

3) clearly communicate organizational structures and procedures to all operational levels;

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

iTeh STANDARD PREVIEW

5) have secure storage for important and confidential documents relating to the contract;

(standards.iteh.ai)

6) operate under confidentiality procedures for the management of information and data related to the business;

SIST EN 17483-1:2021
https://standards.iteh.ai/catalog/standards/sist/43d14ecf-eaf1-4f24-9872-4ab9075a7102/sist-en-17483-1-2021

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

8) have an operational presence within an appropriate distance to the site where the services are provided for the duration of the contract, or at least for the duration of the provision of the services;

9) disclose the structure of its ownership as well as demonstrate the professional competence of its management for the provision of private security services;

10) disclose any unspent criminal convictions and current or discharged bankruptcy of a principal or director;

11) give information on its membership of professional organisations;

12) give information on the provider's activities with regards to its compliance with applicable legislation regarding the protection of environment;

13) have a management system implemented that covers the quality for the provision of the declared services.

NOTE A management system such as EN ISO 9001 or similar fulfils the requirement.