528/2005 Coll.

DECREE

of 14 December 2005

on Physical Security and Certification of Technical Means

Amendment: 19/2008 Coll.
Amendment: 454/2011 Coll.
Amendment: 204/2016 Coll.

Pursuant to Section 33 and Section 53 points (a), (c), (d), (f) to (j) of Act No. 412/2005 Coll. on the Protection of Classified Information and Security Eligibility (hereinafter referred to as "the Act"), the National Security Authority lays down:

Section 1

Subject Matter

This decree sets out scores for individual physical security measures[1)], the minimum level of security for security areas[2)] and meeting areas[3)], the basic method for risk assessment, additional requirements for physical security measures and the required elements for certification of technical means.

Section 2

Definitions

For the purpose of this Decree, the following definitions shall apply:

a) facility means a building or other enclosed premises in which security areas or meeting areas are usually located,

b) facility boundary means the building shell, a physical barrier (fencing) or another visibly delineated boundary,

c) security area boundary or meeting area boundary means a structurally enclosed or otherwise visibly delineated space,

d) facility, security area or meeting area entrance means a place designated for the entry and exit of persons and means of transport,

e) means of transport mean land, underground, air and water means used to transport persons, objects and material,

f) threat means the possibility of disclosure or exploitation of Classified Information in the event of a physical security breach,

g) risk means the probability of a given threat materialising,

h) emergency means a situation where Classified Information is in imminent danger of being disclosed or exploited,

i) technical means mean security features used to prevent, impede, report or record breaches of security of facilities, security areas or meeting areas and to destroy Classified Information,

j) secure cabinet means a safe or another lockable container as set out in Annex 1 to this Decree,

k) technical equipment means military material[5)], in particular electronic, photo-technical, chemical, physico-chemical, radiotechnical, optical and mechanical military technology and military gear containing Classified Information.

Section 3

Facility and Security Area Security

(1) The facility or security area boundary, the classification of facilities or security areas into appropriate categories[6)] and the classification of security areas into appropriate classes shall be determined by the responsible person or their delegate.

(2) The facility and security area security shall be ensured by a combination of physical security measures as set out in Paragraphs 3 to 10 and Sections 6 to 9.

(3) Facilities are secured using the following technical means based on their category, taking into account the nature of the facility boundary and depending on the risk assessment

a) for the Restricted category – mechanical barriers,

b) for the Confidential and Secret categories – mechanical barriers and intrusion detection systems,

c) for the Top Secret category – mechanical barriers, intrusion detection systems and video surveillance systems. Video surveillance systems must not compromise the security of Classified Information.

(4) Security areas are secured using the following technical means depending on their category, class and risk assessment

a) for the Restricted category – mechanical barriers,

b) for the Confidential category – mechanical barriers and intrusion detection systems,

c) for the Secret and Top Secret categories – mechanical barriers, access control systems, intrusion detection systems, video surveillance systems, electrical fire detection devices. Video surveillance systems may be replaced by emergency systems. When using video surveillance systems, the security of Classified Information must not be compromised.

(5) The point scores for the minimum level of security of security areas are set out in Annex 1 to this Decree.

(6) Facilities and security areas of the category Confidential and above in which the continuous presence of persons working there is ensured shall be secured by mechanical barriers.

(7) Certified or non-certified technical means shall be used to secure security areas. Non-certified technical means may be used only when the conditions laid down in Annex 1 to this Decree are met.

(8) Classified Information shall be stored in security areas of the appropriate category or above, alternatively in a secure cabinet, provided its point score is reflected in the physical security project for the security area in question.

(9) Devices for the physical destruction of media carrying information shall be placed in the facility in accordance with Annex 1 to this Decree.

(10) If a facility boundary and a security area boundary are shared, the extent of physical security measures applied shall be determined by the requirements for the security area category.

Section 4

Meeting Area Security

(1) The meeting area boundary shall be determined by the responsible person or their delegate.

(2) The meeting area security shall be ensured by a combination of physical security measures as set out in Paragraphs 3 to 8 and Sections 6 to 9.

(3) The extent of physical security measures applied in meeting areas shall be determined based on the classification level of the Classified Information regularly discussed in the meeting area and on risk assessment.

(4) Meeting areas in which information classified Secret and Top Secret is regularly discussed shall be secured by mechanical barriers, access control systems, intrusion detection systems, video surveillance systems, electrical fire detection devices, devices protecting against passive and active eavesdropping of Classified Information.

(5) Video surveillance systems referred to in Paragraph 4 may be replaced by emergency systems. Video surveillance systems must not compromise the security of Classified Information.

(6) The point scores for the minimum level of security of meeting areas are set out in Annex 1 to this Decree.

(7) The provisions of Annex 1 to this Decree concerning meeting area security shall apply mutatis mutandis to meeting area security, unless otherwise specified in Annex 1 to this Decree.

(8) Certified or non-certified technical means shall be used to secure meeting areas. Non-certified technical means may be used only when the conditions laid down in Annex 1 to this Decree are met.

(9) If a facility boundary and a meeting area boundary are shared, the extent of physical security measures applied shall be determined by the security requirements for the meeting area.

Section 5

Technical Equipment Security

(1) Technical equipment shall be secured using physical security measures as set out in Sections 3, 6 to 10 or in Paragraphs 2 to 4.

(2) The extent of special handling measures and technical means used to secure technical equipment shall be determined by the responsible person or their delegate depending on the risk assessment.

(3) Guarding of stored technical equipment containing information classified

a) Top Secret shall be provided according to type 5 as set out in Annex 1 to this Decree,

b) Secret shall be provided at minimum according to type 4 as set out in Annex 1 to this Decree,

c) Confidential shall be provided at minimum according to type 3 as set out in Annex 1 to this Decree,

d) Restricted shall be provided to the extent determined by the responsible person or their delegate.

(4) The extent of physical security measures used to secure technical equipment shall be set out in the physical security project. The content and format of the physical security project shall be applied as appropriate.

Section 6

Special Arrangements

(1) Special handling measures are

a) authorisation of persons and means of transport for entry to facilities, authorisation of persons for entry to security areas and meeting areas and the method for the control of these authorisations,

b) control measures for access to facilities, security areas and meeting areas and the method for the control of these measures,

c) the conditions and method of control of the movement of persons in facilities, security areas and meeting areas and the method of control and removal of Classified Information from facilities, security areas and meeting areas,

d) arrangements for the handling of keys and combinations, in particular their marking, allocation, storage and accountability,

e) arrangements for the handling and the use of technical means,

f) arrangements for the movement of Classified Information in facilities, security areas and meeting areas.

(2) The point scores for the special handling measures are set out in Annex 1 to this Decree.

Section 7

Arrangements for the Movement of Persons and Means of Transport

(1) Authorisations for entry to facilities, security areas or meeting areas are granted by the responsible person or their delegate. Authorisation for entry to security areas or meeting areas of a given category may be granted to a person who has been briefed and has been granted a Notice of Compliance with Conditions for Access to Restricted Classified Information or a Personnel Security Clearance at the corresponding level or above. A list of persons authorised for access to facilities of the category Confidential, Secret or Top Secret, to security areas and meeting areas and of means of transport authorised for entry to facilities of the category Confidential, Secret or Top Secret, to security areas and meeting areas shall be held by the responsible person or their delegate.

(2) Persons without access authorisation can only enter facilities of the category Confidential, Secret or Top Secret, security areas or meeting areas when escorted by a person with access authorisation to the facility, security area or meeting area in question, provided that the entry is necessary and the security of Classified Information is not compromised.

(3) At the entrance to facilities of the category Confidential, Secret or Top Secret, access control shall be exercised and the data of persons without access authorisation shall be recorded and arrangements for escorted visit shall be established. At the entrance to security areas of the category Restricted located within facilities of the category Restricted, access control shall be exercised.

(4) When persons without access authorisation enter facilities of the category Top Secret, they shall be searched using a device for the detection of dangerous substances or items.

Section 8

Arrangements for the Control of Keys and Combinations

(1) The arrangements for the control of keys and combinations determine the system and manner of their marking, allocation and handing in, their storage and accountability, the storage of duplicates and the manner of their use.

(2) Keys and combinations to meeting areas and also security areas and secure cabinets where information classified Confidential or above is stored must be marked, shall be stored in a manner that allows for the control of their use and their issuance shall be recorded. Keys shall

be handled by the responsible person or their delegate.

(3) The arrangements for the control of keys and combinations to security areas and secure cabinets where information classified Restricted is stored shall be determined by the responsible person.

(4) When persons with access authorisation are not present, security areas and meeting areas must be locked. When persons with access authorisation to Classified Information[7)] stored there are not present, secure cabinets shall be locked. Persons in possession of keys and combinations to security areas, meeting areas and secure cabinets shall store them at the facility, unless another place for storage is designated by the responsible person or their delegate.

(5) The loss of keys and combinations shall be immediately reported to the responsible person or their delegate who shall ensure the situation is rectified.

Section 9

Security guards

The point scores for the different types of facility security guards are set out in Annex 1 to this Decree.

Section 10

Verification of Physical Security Measures and Risk Assessment

(1) Verification that individual physical security measures and risk assessment are in accordance with the physical security project and the laws and regulations on the protection of Classified Information shall be carried out by the responsible person or their delegate on a regular basis, but at least once every 12 months.

(2) In the case of technical means referred to in Section 30(1) of the Act, carrying out a functional test in accordance with Annex 1 to this Decree is a prerequisite for the verification referred to in Paragraph 1.

(3) Risk assessment is carried out

a) by identifying the classification level of Classified Information and determining the amount of Classified Information which is or will be present at the facility, particularly with respect to the consequences of its disclosure or misuse,

b) by describing and assessing the threats Classified Information is exposed to,

c) by describing and assessing the vulnerability of Classified Information to these threats,

d) by determining the risk level as “low”, “medium” or “high” based on the assessment of threats to and vulnerability of Classified Information.

(4) In the event of a change to the physical security measures, the responsible person or

their delegate shall immediately ensure that it is reflected in the physical security project.

(5) The structure of the physical security project is set out in Annex 1 to this Decree.

Section 11

Requirements for Technical Means Certification Applications

(1) Technical Means Certification Applications shall include

a) identification of the applicant by
1. business name, or name, address and identification number if the applicant is a legal person,
2. business name, or name and surname and, where appropriate, distinguishing addition, permanent residence and place of business if different from permanent residence, date of birth and identification number if the applicant is a natural person who is an entrepreneur, or
3. name, address, identification number and name of surname of the responsible person, if the applicant is a government authority,

b) a list and identification of the technical means and a list of the submitted documentation.

(2) Applications in accordance with Paragraph 1 shall be accompanied by the following documentation

a) specifications and description of the technical means,

b) a declaration of safety or conformity of the technical means[8)],

c) a certificate of conformity – not required for single technical means,

d) an evaluation as referred to in Section 46(14) of the Act.

Section 12

The validity period of the certificate shall be set by the National Security Authority, up to a maximum of the validity period of the evaluation referred to in Section 46(14) of the Act.

Section 13

The template for the technical means certification is provided in Annex 2 to this Decree.

Section 14

After the expiry of the validity period of their certification, the technical means referred to in Section 30(1) of the Act may be used in the manner and under the conditions specified in Annex 1 to this Decree.

Section 15

Requirements for Applications for Contracts for Providing Services

Applications for Contracts for Providing Services[9] shall include

a) identification of the applicant in accordance with Section 11(1)(a),

b) the name and surname of the applicant's contact person and contact details,

c) identification of the applicant's place of work (activities and detailed specification of the location of the workplace in question, name and surname of the contact person and contact details),

d) specification of the activities to be carried out under the contract for providing services,

e) an extract from the Commercial Register or the Trade Licensing Register and a certified copy of a valid decision or certificate:
1. A decision granting authorisation in which the scope of activities during conformity assessment includes the technical means referred to in Section 30(1) of the Act, issued by the Czech Office for Standards, Metrology and Testing[10],
2. An accreditation certificate including an annex in which the subject of accreditation includes the certification of the technical means referred to in Section 30(1) of the Act, issued by the Czech Accreditation Institute[11], or
3. An accreditation certificate including an annex in which the subject of accreditation includes the testing of the technical means referred to in Section 30(1) of the Act, issued by the Czech Accreditation Institute[11].

Section 16

Entry into Force

This Decree shall enter into force on 1 January 2006.

Director:

Mgr. Mareš v. r.

---

1) Section 27 of Act No. 412/2005 Coll. on the Protection of Classified Information and Security Eligibility.

2) Section 24(3) of Act No. 412/2005 Coll.

3) Section 24(4) of Act No. 412/2005 Coll.

4) Section 2(e) of Act No. 412/2005 Coll.

5) Section 2(7) of Act No. 219/1999 Coll. on The Armed Forces of the Czech Republic, as subsequently amended.

6) Section 25(1) of Act No. 412/2005 Coll. as amended by Act No. 255/2011 Coll.

7) Section 6(1) and Section 11(1) of Act No. 412/2005 Coll.

8) Act No. 22/1997 Coll. on Technical Requirements for Products and on Amendments to Some Acts, as subsequently amended.

Act No. 102/2001 Coll. on General Product Safety and on Amendments to Some Acts (Act on General Product Safety), as subsequently amended.

9) Section 46(15) and Section 52 of Act No. 412/2005 Coll.

10) Section 13 of Act No. 505/1990 Coll. on Metrology, as subsequently amended.

11) Section 14 of Act No. 22/1997 Coll.

Communication from the Ministry of Industry and Trade No. 272/1998 Coll.