

1. CONTAINERS AND LOCKS

1.1. CONTAINERS

1.1.1. Type 4 container:

SS1 = 4

A Type 4 container shall be certified by the National Security Authority (hereinafter “the Authority”) and it shall meet requirements of the security Class II or above according to ČSN EN 1143-1 – Security containers – Requirements, classification and methods of intrusion resistance testing – Part 1: Box safes, safes doors and strong-rooms.

In accordance with ČSN EN 1143-1, the Type 4 container shall be fitted with a Class A lock as a minimum according to ČSN EN 1300 Security containers – Classification of high security locks in the light of their resistance to unauthorised opening (Type 2 lock, article 1.2.3. of the Annex).

If a cryptographic material is stored in the Type 4 container, then this container shall be fitted with at least three-position combination mechanical lock.

1.1.2. Type 3 container:

SS1 = 3

A Type 3 container shall be certified by the Authority and it shall meet requirements of the security Class I according to ČSN EN 1143-1.

In accordance with ČSN EN 1143-1, the Type 3 container shall be fitted with a Class A lock as a minimum according to ČSN EN 1300 (Type 2 lock, article 1.2.3. of the Annex).

If a cryptographic material is stored in the Type 3 container, then this container shall be fitted with at least three-position combination mechanical lock.

1.1.3. Type 2 container:

SS1 = 2

A Type 2 container shall be certified by the Authority and it shall meet requirements of the security Class 0 according to ČSN EN 1143-1.

In accordance with ČSN EN 1143-1, the Type 2 container shall be fitted with a Class A lock as a minimum according to ČSN EN 1300 (Type 2 lock, article 1.2.3. of the Annex).

1.1.4. Type 1 container:

S1 = 1

A Type 1 container shall be an undismountable steel box of solid construction, its door locking device shall be fitted with the three-sided cross-bolt mechanism and locked. The door locking device shall be self-locking in the closed state.

The Type 1 container is not certified by the Authority. The compliance of the quality of these containers with above mentioned requirements shall be assessed by the user of the facility. A record of compliance assessment shall become a part of the physical security project.

1.1.5.Type 1A container:**S1 = 1**

A Type 1A container shall be certified by the Authority and it shall meet, including the locking system, requirements of the security Class Z1 according to ČSN 91 6012 – Security containers – Requirements, classification and testing methods of resistance to burglary – Safes of the basic security.

1.1.6.Type 1B container:**S1 = 2**

A Type 1B container shall be certified by the Authority and it shall meet, including the locking system, requirements of the security Class Z2 according to ČSN 91 6012.

1.1.7.Type 1C container:**S1 = 3**

A Type 1C container shall be certified by the Authority and it shall meet, including the locking system, requirements of the security Class Z3 according to ČSN 91 6012.

1.1.8.Type 1T container:**S1 = 1**

A Type 1T container shall be a technical equipment, which will be assessed according to its design concept and related difficulty to obtain classified information. This is a security equivalent of the container and locking system.

The Type 1 container is not certified by the Authority. The compliance of the quality of Type 1T containers with conditions stated below shall be assessed by the user of the facility. A record of the compliance assessment shall become part of the physical security project.

The record of the compliance assessment for technical equipment may be made subject to the conditions set forth below:

- its characteristic does not allow and its manual does not determine that any part (containing classified information) should be removed from the technical equipment while not in use. The technical equipment stored contains classified information;
- classified information cannot be overlooked from the technical equipment;
- its parts (containing classified information) cannot be removed in a non-destructive manner within the time limit less than five minutes;
- the level of guards of the technical equipment containing RESTRICTED classified information shall be of the Type 3 or above;
- the level of guards of the technical equipment containing information classified CONFIDENTIAL and above shall be of the Type 4 or above.

1.1.9.Type T container:**S1 = unspecified**

A Type T container shall be a technical equipment, which shall be assessed according to its design concept and related difficulty to obtain classified information. This is the security equivalent of the container and locking system.

The Type 1 container shall be certified by the Authority and it shall meet requirements for the Type T1 container. Other conditions of the technical equipment certification and marks score S1 shall be determined by the security standard (S. 2 j) of the Act).

1.2.LOCKS OF CONTAINERS**1.2.1.Type 4 lock:****SS2 = 4**

A Type 4 lock shall be certified by the Authority in the conduct of container certification and it shall meet requirements for security Class C according to ČSN EN 1300.

1.2.2.Type 3 lock:**SS2 = 3**

A Type 3 lock shall be certified by the Authority in the conduct of container certification and it shall meet requirements for security Class B according to ČSN EN 1300.

1.2.3.Type 2 lock:**SS2 = 2**

A Type 2 lock shall be certified by the Authority in the conduct of container certification and it shall meet requirements for security Class A according to ČSN EN 1300.

Note to the article 1:

The conversion Table of the container marks score

Type of the container	Security classification level, for which storing capability has been approved, shall be entered in words	Marks score	Marks score
	Until 31 December 1999	SS1	SS2
Type 4	TOP SECRET	4	2
Type 3	SECRET	3	2
Type 2	CONFIDENTIAL	2	2

2. SECURITY AREAS AND THEIR LOCKING SYSTEMS

The term mechanical barriers in this Chapter includes in particular locks, doors, bars, shatter resistant window films and other security structural elements, with the exception of containers (article 1. of the Annex).

Man-openings shall be protected by the mechanical barriers, which allow the following gauging template to pass through:

Opening	Size in its greatest dimension
rectangular	400mm x 250mm
elliptical	400mm x 300mm
circular	Diameter 350 mm

2.1. SECURITY AREAS

Determination of the security area type shall be given by the least resistance point of the perimeter.

2.1.1. Type 4 security area

SS3 = 4

Walls, floors and ceilings shall be constructed as follows:

- masonry construction (brick block or lime-cement blocks, porous concrete blocks) thickness over 300 mm; or
- reinforced concrete, thickness over 150 mm.

The marks score of other mechanical barriers must be equal to SS3 = 4. The mechanical barriers shall not exhibit such signs of damage or physical wear and tear, which could render identification of attempted access impossible.

Windows, doors and other barriers must satisfy the conditions of security Class 4 or 5 according to ČSN P ENV 1627 Windows, doors, barriers – Resistance to the forced entry – Requirements and classification.

2.1.2. Type 3 security area

SS3 = 3

Walls, floors and ceilings shall be constructed as follows:

- masonry construction (brick block or lime-cement blocks, porous concrete blocks) thickness over 150 mm; or
- reinforced concrete, thickness over 100 mm.

The marks score of other mechanical barriers must be equal to SS3 = 3 as a minimum. The mechanical barriers shall not exhibit such signs of damage or physical wear and tear, which could render identification of attempted access impossible.

Windows, doors and barriers must satisfy the conditions of security Class 3 according to ČSN P ENV 1627.

2.1.3. Type 2 security area

SS3 = 2

Walls, floors and ceilings shall be constructed as follows:

- masonry construction (brick block or lime-cement blocks, porous concrete blocks) thickness 100 to 150mm; or
- reinforced concrete, thickness to 100mm.

The marks score of other mechanical barriers must be equal to SS3 = 2 as a minimum.

Windows, doors and barriers must satisfy the conditions of security Class 2 according to ČSN P ENV 1627.

Man-openings need not be protected by certified mechanical barriers if the lower edge of the man-opening satisfies the following conditions:

- it shall be at least 5.5m above ground;
- it shall not be easily accessible from a roof or with the aid of lightning conductors, from gutter, window sills, other building components, undulations, trees or any other construction.

The mechanical barriers shall not exhibit such signs of damage or physical wear and tear, which could render identification of attempted access impossible.

2.1.4.Type 1 security area

SS3 = 1

Walls, floors and ceilings are of lightweight construction, where for example the following material may be used:

- plasterboard;
- light weight masonry
- wood, chipboard;
- plastic hardened materials;
- profiled metal sheet or corrugated sheet;
- shatter resistant window films reinforced glass, which was certified by the Authority (may also be used for covering of man-openings).

The man-opening shall be protected by mechanical barriers, which provide the same degree of resistance as remaining parts of the perimeter of the Type 1 security area or which are protected by certified electrical security alarm annunciation equipment, installation of which corresponds to the level (score) SS92 = 3 as a minimum.

Man-openings need not be protected if the lower edge of the man-opening satisfies the following conditions:

- it shall be at least 5.5m above ground; and
- it shall not be easily accessible from a roof or with the aid of lightning conductors, from gutters, window sills, other building components, undulations, trees or any other construction.

The mechanical barriers must be of solid construction and they shall not exhibit such signs of damage or physical wear and tear, which could render identification of attempted access impossible, and the compliance with above mentioned requirements shall be assessed by the user of the facility.

A record of the compliance assessment shall become a part of the physical security project.

2.2.LOCKING SYSTEMS FOR LOCKING OF SECURITY AREAS

2.2.1.Type 4 locking system

SS4 = 4

A Type 4 locking system shall be certified by the Authority.

The locking system and its components shall meet requirements of the security Class 5 according to ČSN P ENV 1627.

2.2.2.Type 3 locking system

SS4 = 3

A Type 3 locking system shall be certified by the Authority.

The locking system and its components shall meet requirements of the security Class 4 according to ČSN P ENV 1627.

2.2.3.Type 2 locking system

SS4 = 2

A Type 2 locking system shall be certified by the Authority.

The locking system and its components shall meet requirements of the security Class 3 according to ČSN P ENV 1627.

2.2.4.Type 1 locking system

SS4 = 1

A Type 1 locking system shall be certified by the Authority.

The locking system and its components shall meet requirements of the security Class 2 according to ČSN P ENV 1627.

Note to the article 1:

Should the security area be a strong room, the entry to the strong room must not be in that part of the security area perimeter, which is also the perimeter of the facility. In this case the score S2 will be equal to 0.

3. FACILITY PERIMETER

Critical to determination of the facility type shall be the part of the facility perimeter with the least resistance. If the facility perimeter is the same along the total lengths as the security area perimeter, only the security area shall be assessed and the facility score S3 = 0; in this case the visitors regime will not score SS7 = 0.

A special case of the facility perimeter is a perimeter (fence, etc.) where along its total lengths and in access points the Type 5 guards are employed. In this case the score S3 may be replaced by the product of sub-scores SS10 (Type 2 /or above/ physical barrier) and SS11. Sub-scores of SS10 and SS11, which has been used in the score S3, will no more be

added in the calculation of S6, but it shall be given for information purposes in the marks score table.

Another case of the facility perimeter is a perimeter (fence, etc.) where along its total lengths and in access points the Type 5 (or lower) guards are employed. Marks score for the perimeter will be added in only in parts from SS10 to SS15. In addition, in this case the building enclosure may also be taken into account, which will be evaluated according to the part 3 and added in S3. If the facility perimeter is the same along the total lengths as the security area perimeter, only the security area shall be assessed and S3 will not score S3 = 0.

3.1. Type 4 facility

S3 = 4

Walls, floors and ceiling shall have an elevated structure or be of an extra solid construction (e.g. of reinforced concrete). The type 4 facility shall have minimum doors, windows and other man-openings, which shall be protected by mechanical barriers and offer the same degree of resistance to an intruder as the rest of the perimeter of the Type 4 facility.

3.2. Type 3 facility

S3 = 3

Walls, floors and ceiling shall be of solid construction of bricks or blocks, or a building technology shall be used, which uses pre-cast and prefabricated panels, etc. Man-openings shall be protected by mechanical barriers offering the same degree of resistance to an intruder as the rest of the perimeter of the Type 3 facility.

Man-openings need not be protected by mechanical barriers if the lower edge of the man-opening satisfies the following conditions:

- it shall be at least 5.5m above ground;
- it shall not be easily accessible from a roof or with the aid of lightning conductors, from gutters, window sills, other building components, undulations, trees or any other construction.

3.3. Type 2 facility

S3 = 2

The facility is of lightweight construction. Man-openings shall be protected by mechanical barriers or by electrical security alarm annunciation equipment with installation score SS92 = 1 as a minimum. This does not apply if the lower edge of the man-opening satisfies the following conditions:

- it shall be at least 5.5m above ground;
- it shall not be easily accessible from a roof or with the aid of lightning conductors, from gutters, window sills, other building components, undulations, trees or any other construction.

3.4. Type 1 facility**SS3 = 1**

Normally a lightweight prefabricated structure intended simply to protect its contents and those who work in it from the elements.

4. ENTRY CONTROL SYSTEM WHICH ADMITS ACCESS TO THE SECURITY AREA OR FACILITY AND VISITORS REGIME**4.1. ENTRY CONTROL SYSTEM WHICH ADMITS ACCESS TO THE SECURITY AREA OR FACILITY****4.1.1. Type 4 entry control system****SS6 = 4**

A Type 4 entry control system shall be certified by the Authority and satisfy conditions according to ČSN EN 50 133-1 Alarm systems – Entry control systems for the use in security applications – Part 1: System requirements for the Class B of the access and Class 3 of the identification.

The Type 4 entry control system shall be supported by an access barrier, which shall render any repeated access impossible and provide the regime “one transaction – one access”.

The entry control shall be implemented at all access points to the facility or to the security area.

The output warning signal of the Type 4 entry control system shall be connected to the resident guards post.

4.1.2. Type 3 entry control system**SS6 = 3**

A Type 3 entry control system shall be certified by the Authority and satisfy conditions according to ČSN EN 50 133-1 for the Class B of the access and Class 2 of the identification.

The entry control shall be implemented at all access points to the facility or to the security area.

The output warning signal of the Type 3 entry control system shall be connected to the resident guards post.

4.1.3. Type 2 entry control system**SS6 = 2**

A Type 2 entry control system shall be certified by the Authority and satisfy conditions according to ČSN EN 50 133-1 for the Class A of the access and Class 1 of the identification.

The access control shall be implemented at all access points to the facility or to the security area.

The output warning signal of the Type 2 entry control system shall be connected to the resident guards post.

The Type 2 entry control system can be replaced by the entry control, which shall be continuously carried out by members of armed forces or armed corps at all access points to the facility or security area.

4.1.4. Type 1 entry control system

SS6 = 1

A Type 1 entry control system shall be a lockable mechanical barrier at the access point.

The entry control shall be implemented at all access points to the facility or at all access points to the security area.

Note to article 4.1.:

The Type 1 entry control system may only be used at access points to the CONFIDENTIAL or RESTRICTED category security area.

In carrying out entry control to the TOP SECRET category facility or security area, the devices for search of dangerous substances or objects shall be used, which have been certified by the Authority.

4.2. RANDOM ENTRY AND EXIT SEARCHES

4.2.1. Random searches

SS12 = 1

Random entry and exit searches are to be undertaken by the State body, legal person or the natural person pursuing business, which are designed to act as a deterrent to the breach of protection of classified information.

4.3. VISITORS REGIME WITHIN THE FACILITY

4.3.1. Escorted visits

SS7 = 3

Visitors who require an escort within the facility shall be accompanied at all times.

Visitor's register shall be kept, which contains personal identification data of visitors, accompanying persons and period of time when the visit took place.

4.3.2. Unescorted visits

SS7 = 1

Visitors who are permitted unescorted entry to an area, or parts of it shall be required to wear a pass that identifies them as a visitor. In this case all regular staff shall be required to wear a pass.

Visitor's register shall be kept, which contains personal identification data of visitors and period of time when the visit took place.

4.3.3. Visits without control**SS7 = 0**

These are visitors who are permitted unescorted entry to an area and entry without control.

**5. GUARDS AND ELECTRICAL SECURITY ALARM
ANNUNCIATION EQUIPMENT****5.1. GUARDS****5.1.1. Type 5 guards****SS8 = 5**

Duties of a Type 5 guards shall be carried out only by members of armed forces or armed corps in the form of random patrols.

The guards shall ensure patrolling on random routes and at random intervals, not exceeding two hours.

During the performance of duties of guards, including for the duration of a patrol, a resident guards post shall be continuously manned at least by one guards member.

5.1.2. Type 4 guards**SS8 = 4**

Duties of a Type 4 guards shall be carried out only by members of armed forces or armed corps in the form of random patrols.

The guards shall ensure periodic patrols at intervals not exceeding six hours.

During the night and during non-duty hours the frequency of periodic patrols shall be increased.

During the performance of duties of guards, including for the duration of a patrol, a resident guards post shall be continuously manned at least by one guards member.

5.1.3. Type 3 guards**SS8 = 3**

Duties of a Type 3 guards shall be carried out by employees of the State body, legal person or of the natural person pursuing business who use or own the facility in question, by members of armed forces or armed corps or by the security protection service staff.

The frequency of patrolling will depend on internal operational environment and the level of assumed risk.

During the performance of duties of guards, including for the duration of a patrol, a resident guards post shall be continuously manned at least by one guards member.

5.1.4. Type 2 guards

SS8 = 2

Duties of a Type 2 guards shall be carried out by employees of the State body, legal person or of the natural person pursuing business who use or own the facility in question, by members of armed forces or armed corps or by the security protection service staff.

No patrols are required in the case of Type 2 guards.

5.1.5.Type 1 guards

SS8 = 1

Type 1 guards are commensurate with guarding of the facility by connecting with the centralized protection desk and thus enabling to react within a reasonable timescale.

Note to the article 5.1.:

In the case of facility housing the CONFIDENTIAL, SECRET or TOP SECRET category security area, or an area designated as the meeting room, the rules governing performance of guards shall be determined in writing.

The protection of security areas housing classified information of the European Union classified CONFIDENTIAL and above shall be ensured by Type 2 guards or above and the condition must be met that the frequency of patrols will not exceed two hours. The guards shall start patrolling immediately after normal working hours.

The distance of the resident guards post from the TOP SECRET and SECRET category security area shall not exceed 500m or, if the distance exceeds 500m, the guards shall be able to take action within five minutes after an alarm annunciation or receiving an emergency signal from the facility, security area or area designated as the meeting room.

The Type 1 guards may be used only in the case of the CONFIDENTIAL or RESTRICTED category security areas.

On the patrol the guards shall be provided with means allowing communication with the resident guards post. Guards' response time to alarms or emergency signals shall be tested by the user of the facility.

5.2.ELECTRICAL SECURITY ALARM ANNUNCIATION EQUIPMENT

5.2.1.Type 4 electrical security alarm annunciation equipment
--

SS91 = 4

Type 4 electrical security alarm annunciation equipment shall be certified by the Authority and it shall meet requirements according to ČSN EN 50 131-1 Alarm systems – Electronic alarm systems – for the security level 4 – High level of risk. In addition the emergency system shall meet conditions of ČSN EN 50 134-1 – Alarm systems – Response systems.

5.2.2.Type 3 electrical security alarm annunciation equipment
--

SS91 = 3

Type 3 electrical security alarm annunciation equipment shall be certified by the Authority and it shall meet requirements according to ČSN EN 50 131-1 for the security level 3 – Medium to High level of risk. In addition the emergency system shall meet conditions of ČSN EN 50 134-1.

5.2.3.Type 2 electrical security alarm annunciation equipment**SS91 = 2**

Type 2 electrical security alarm annunciation equipment shall be certified by the Authority and it shall meet requirements according to ČSN EN 50 131-1 for the security level 2 – Low to Medium level of risk. In addition the emergency system shall meet conditions of ČSN EN 50 134-1.

5.2.4.Type 1 electrical security alarm annunciation equipment**SS91 = 1**

Type 1 electrical security alarm annunciation equipment will not be certified by the Authority.

Note to the article 5.2.:

The following shall be the subject of the electrical security alarm annunciation equipment certification:

- electrical security alarm centres;
- electrical security alarm sensors;
- perimeter detection systems; and
- emergency systems.

The Table of assignment of categories to types of technical means of the electrical security alarm annunciation equipment (ESAAE)

Type of technical means of the ESAAE	Security classification level, for which capability has been approved, shall be entered in words or as the abbreviation		Marks score
	Until 31 December 1999	From 1 January 2000	
Type 4	-	“TS”	4
Type 3	“TOP SECRET”	“T”	3
Type 2	“CONFIDENTIAL”	“C”	2

5.2.5.Type 4 installation of the electrical security alarm annunciation equipment

SS92 = 4

Type 4 installation shall be to the following extent in the security area:

- space protection;
- building facades protection;
- emergency system; and
- vibration detection devices.

Type 4 installation is subject to CCTV monitoring of man-openings in the security area.

5.2.6.Type 3 installation of the electrical security alarm annunciation equipment**SS92 = 3**

Type 3 installation shall be to the following extent in the security area:

- space protection;
- building facades protection;
- emergency system.

5.2.7.Type 2 installation of the electrical security alarm annunciation equipment**SS92 = 2**

Type 2 installation shall be to the following extent in the security area:

- space protection; and
- building facades protection.

If the Type 2 electrical security alarm annunciation equipment has been installed then the man-openings on the boundary of the security area need not be protected by elements of the building facades protection if the lower edge of the man-opening satisfies the following conditions:

- it shall be at least 5.5m above ground;
- it shall not be easily accessible from a roof or with the aid of lightning conductors, from gutters, other building components, undulations, trees or any other construction.

5.2.8.Type 1 installation of the electrical security alarm annunciation equipment**SS92 = 1**

Type 1 installation shall be performed to the extent of the space protection of the security area.

Note to articles 5.2.5 to 5.2.8:

Output signal of the electrical security alarm annunciation equipment and the CCTV signal shall be connected to the resident guards post.

Operating of the electrical security alarm annunciation equipment in the security area shall be independent on operating of the electrical security alarm annunciation equipment in other security areas or in other areas.

The installation of the electrical security alarm annunciation equipment shall be verified by operational test according to TNI 33 45 91-3. The extent of operational tests is

laid down in the table A1 (level 1). The operational test shall be recorded in the operational book or by a test protocol, which shall be deposited with the user of the facility.

5.2.9. Calculation of SS9 according to SS91 and SS92 score

$$SS9 = (SS91 + SS92)/2 \times SS92/OBL$$

SS9 shall be mathematically rounded to an integer.
Maximum value of SS9 can be 4.

OBL is the marks score determined by the security area category:

Security area category	Marks score OBL
TOP SECRET	4
SECRET	3
CONFIDENTIAL	2
RESTRICTED	1

No electrical security alarm annunciation equipment need to be installed in the security area permanently manned by at least one person; in this case SS9 = 4.

The final marks score of the electrical security alarm annunciation equipment level shall be determined by the marks score of the lowest Type technical means used.

5.3. CCTV

CCTV serves for picking-up, transmission and displaying motion of persons and vehicles, and it shall be certified by the Authority.

A subject of certification of CCTV shall be cameras and controllers.

6. PERIMETER PROTECTION

The perimeter shall be made of physical barrier along its total lengths.

6.1. PHYSICAL BARRIERS

Physical barriers are required along the total length of the facility perimeter where its character permits it. The security level of construction of access points (access gateways) shall be at least as that of the construction of the physical barrier (fence). The same standard of access control shall be provided at all access points.

6.1.1. Type 7 physical barrier

SS10 = 12

A Type 7 physical barrier shall consist of three barriers situated one after another of below mentioned resistance and it shall be guarded by Type 5 guards. The distance between the barriers shall be at least 3m. The access control shall be carried out at all access points by the Type 5 guards. The facility shall be defined by the outer perimeter.

If the distance between barriers is up to six meters, then CCTV and the security lighting shall be installed in the area between the intermediary and outer barriers as part of the perimeters protection. Only Type 5 guards may have access to the area between the barriers. Other persons may have access to this area only if accompanied by the Type 5 guards at all times.

If the distance between barriers exceeds six meters, then CCTV and the security lighting shall be installed at the intermediary and outer barrier on their internal parts as part of the protection of the perimeter. Only persons who have been permitted to have access to the facility may access to the area between the barriers. Other persons may have access to this area only if accompanied by the Type 5 guards at all times.

Should the part of the Type 7 physical barrier be the wall of a building it shall meet requirements of the Type 4 facility and it shall be safeguarded by the electrical security alarm annunciation system, CCTV – from the outer site on the level of the barrier, and by the security lighting.

The intermediary and outer physical barriers shall be equipped with a perimeter detection system. Perimeter detection systems being installed, of which at least one shall be installed as a covert system, operate on various physical principles.

Requirements:

- **The inner perimeter barrier** shall enable surveillance of an adjacent terrain. If possible, depending on the local situation, a 25m free area must be left between the barrier and the security area perimeter. The barrier shall be protected by a concrete plate resistant to creeping under, which shall be at least 0,5m under ground. The barrier shall be designed and constructed so as to constitute as great as reasonably achievable obstacle to breaching attacks – welded wire netting high at least 2.15m, maximum dimension of holes 80x40mm, and the wire diameter shall be 3mm as a minimum. A top part of the barrier shall be directly connected to the wire fencing and provide resistance to climbing – two-sided inclined bars protruding outwards and inwards at an angle of 45°, long 400mm as a minimum, where barbed wire has been fixed on each bar along its total lengths, at least three lines. A space between bars shall be filled with spiral made of a blade wire.
- **The intermediary perimeter barrier** shall enable surveillance of an adjacent terrain. Axis distance of posts shall be 2.7m as a maximum. The barrier shall be protected by a concrete plate resistant to creeping under, which shall be at least 0,5m under ground. The high of the barrier shall be at least 4.8m. The barrier shall be designed and constructed so as to constitute as great as reasonably achievable obstacle to breaching attacks – welded wire netting high at least 4m, maximum dimension of holes 80x20mm, and the wire diameter shall be 3mm as a minimum. A top part of the barrier shall be directly connected to the wire fencing and provide resistance to climbing – two-sided straight horizontal bars protruding outwards and inwards, long 400mm as a minimum, where blade wire has been fixed on each bar along its total lengths, at least three lines. A space above bars shall be filled with spiral made of a blade wire with diameter 680mm as a minimum. The physical barrier shall be supported by the perimeter detection system.
- **The outer perimeter barrier** shall enable surveillance of an adjacent terrain. The barrier shall be protected by a concrete plate resistant to creeping under, which shall be at least 0,5m under ground. The barrier shall be designed and constructed so as to constitute as great as reasonably achievable obstacle to breaching attacks –

welded wire netting high at least 2.15m, maximum dimension of holes 80x40mm, and the wire diameter shall be 3mm as a minimum. A top part of the barrier shall be directly connected to the wire fencing and provide resistance to climbing – two-sided inclined bars protruding outwards and inwards at an angle of 45°, long 400mm as a minimum, where barbed wire has been fixed on each bar along its total lengths, at least three lines. A space between bars shall be filled with spiral made of a blade wire. The physical barrier shall be supported by the perimeter detection system.

6.1.2.Type 6 physical barrier

SS10 = 9

A Type 6 physical barrier shall consist of two barriers situated one after another of below mentioned resistance and it shall be guarded by Type 5 guards. The distance between the barriers shall be at least 3m. The access control shall be carried out at all access points by the Type 5 guards. The facility shall be defined by the outer perimeter.

If the distance between barriers is up to six meters, then CCTV and the security lighting shall be installed between the inner and outer area as part of the protection of perimeters. Only Type 5 guards may have access to the area between the barriers. Other persons may have access to this area only if accompanied by the Type 5 guards at all times.

If the distance between barriers exceeds six meters, then CCTV and the security lighting shall be installed at the inner and outer barriers on their internal parts as part of the protection of the perimeter. Only persons who have been permitted to have access to the facility may have access to the area between the barriers. Other persons may have access to this area only if accompanied by the Type 5 guards at all times.

Should the part of the Type 6 physical barrier be the wall of a building it shall meet requirements of the Type 3 facility and it shall be safeguarded by the electrical security alarm annunciation system, CCTV – from the outer site on the level of the barrier, and by the security lighting.

The inner and outer physical barriers shall be equipped with a perimeter detection system. Perimeter detection systems being installed, of which at least one shall be installed as a covert system, operate on various physical principles.

The Type 6 physical barrier may be used for the protection of the TOP SECRET category security area at the level of risk “low”, or for the protection of the lower level category security area. If used for the protection of the TOP SECRET category security area at the level of risk “medium” or “high”, the score shall be reduced to SS10 = 6.

Requirements:

- **The inner perimeter barrier** shall enable surveillance of an adjacent terrain. If possible, depending on the local situation, a 25m free area must be left between the barrier and the security area perimeter. Axis distance of posts shall be 2.7m as a maximum. The barrier shall be protected by a concrete plate resistant to creeping under, which shall be at least 0,5m under ground. The high of the barrier shall be at least 4.8m. The barrier shall be designed and constructed so as to constitute as great as reasonably achievable obstacle to breaching attacks – welded wire netting high at least 4m, maximum dimension of holes 80x20mm, and the wire diameter shall be 3mm as a minimum. A top part of the barrier shall be directly connected to the wire fencing and provide resistance to climbing - two-sided straight horizontal bars

protruding outwards and inwards, long 400mm as a minimum, where blade wire has been fixed on each bar along its total lengths, at least three lines. A space above bars shall be filled with spiral made of a barbed wire with diameter 680mm as a minimum. The physical barrier shall be supported by the perimeter detection system.

- **The outer perimeter barrier** shall enable surveillance of an adjacent terrain. The barrier shall be protected by a concrete plate resistant to creeping under, which shall be at least 0,5m under ground. The barrier shall be designed and constructed so as to constitute as great as reasonably achievable obstacle to breaching attacks – welded wire netting high at least 2.15m, maximum dimension of holes 80x40mm, and the wire diameter shall be 3mm as a minimum. A top part of the barrier shall be directly connected to the wire fencing and provide resistance to climbing – two-sided inclined bars protruding outwards and inwards at an angle of 45°, long 400mm as a minimum, where barbed wire has been fixed on each bar along its total lengths, at least three lines. A space between bars shall be filled with spiral made of a blade wire. The physical barrier shall be supported by the perimeter detection system.

6.1.3.Type 5 physical barrier

SS10 = 7

A Type 5 physical barrier shall be only one barrier of below mentioned resistance and it shall be guarded by Type 5 guards. The access control shall be carried out at all access points by the Type 5 guards.

CCTV and the security lighting shall always be installed on the inner side of the barrier as part of the protection of perimeters. The physical barrier shall be equipped with a covert perimeter detection system.

Should the part of the Type 5 physical barrier be the wall of a building it shall meet requirements of the Type 2 facility and it shall be safeguarded by the electrical security alarm annunciation system, CCTV – from the outer site on the level of the barrier, and by the security lighting as part of the protection of perimeter.

The Type 5 physical barrier may be used for the protection of the SECRET category security area at the level of risk “low”, or for the protection of the lower level category security area. If used for the protection of the SECRET category security area at the level of risk “medium” or for the protection of the higher category security area, than the score shall be reduced to SS10 = 4.

Requirements:

- **The perimeter barrier** shall enable surveillance of an adjacent terrain. If possible, depending on the local situation, a 25m free area must be left between the barrier and the security area perimeter. Axis distance of posts shall be 2.7m as a maximum. The barrier shall be protected by a concrete plate resistant to creeping under, which shall be at least 0,5m under ground. The high of the barrier shall be at least 4.8m. The barrier shall be designed and constructed so as to constitute as great as reasonably achievable obstacle to breaching attacks – welded wire netting high at least 4m, maximum dimension of holes 80x20mm, and the wire diameter shall be 3mm as a minimum. A top part of the barrier shall be directly connected to the wire fencing and provide resistance to climbing - two-sided straight horizontal bars

protruding outwards and inwards, long 400mm as a minimum, where blade wire has been fixed on each bar along its total lengths, at least three lines. A space above bars shall be filled with spiral made of a blade wire with diameter 680mm as a minimum. The physical barrier shall be supported by the perimeter detection system.

6.1.4.Type 4 physical barrier**SS10 = 4**

- A Type 4 physical barrier shall enable surveillance of an adjacent terrain. If possible, a 25m free area must be left around a protected facility. A high of the vertical part of the barrier shall be 2.15m as a minimum. It shall be designed and constructed so as to constitute as great as reasonably achievable obstacle to breaching attacks. A top part of the barrier shall provide resistance to climbing – two-sided inclined bars protruding outwards and inwards at an angle of 45°, long 40cm as a minimum, where barbed wire has been fixed on each bar along its total lengths. The Type 4 physical barrier shall be supported by the perimeter detection system.

6.1.5.Type 3 physical barrier**SS10 = 3**

A Type 3 physical barrier shall enable surveillance of an adjacent terrain. If possible, a 25m free area must be left around a protected facility. A high of the vertical part of the barrier shall be 2.15m as a minimum. It shall be designed and constructed so as to constitute as great as reasonably achievable obstacle to breaching attacks. A top part of the barrier shall provide resistance to climbing – one-sided inclined bars protruding outwards at an angle of 45°, long 40cm as a minimum, where barbed wire has been fixed on each bar along its total lengths.

6.1.6.Type 2 physical barrier**SS10 = 2**

A Type 2 physical barrier shall provide resistance to climbing or breaching attacks. A high of the vertical part of the barrier shall be 2.15m as a minimum.

6.1.7.Type 1 physical barrier**SS10 = 1**

A Type 1 physical barrier is equal to a fence with no particular security requirements. The purpose of this fence is to mark boundaries and to offer the minimum level of deterrence or resistance. The Type 1 physical barrier may be constructed of any type of material.

6.2.Access control at all access points of the perimeter

SS11 = 1

6.3.Perimeter Intrusion Detection System (PIDS)
--

SS13 = 2

The Perimeter Intrusion Detection System used for the protection of the perimeter shall be certified by the Authority and requirements laid down in paragraph 5.2 of the Annex shall apply for this system.

6.4.Security lighting of the perimeter

SS14 = 2

Requirements for the security lighting installation shall be given for example by requirements for the CCTV on the perimeter.

6.5.CCTV on the perimeter

SS15 = 2

7. ELECTRICAL FIRE ALARM EQUIPMENT

Fire detection devices shall be connected to electrical fire alarm centres or to electrical security alarm annunciation centres. In either case the alarm signal shall be connected to the resident guards post.

Electrical fire alarm equipment shall be certified by the Authority and meet requirements as stated in standards.

ČSN EN 54-1 Electrical fire alarm – Part 1: Introduction

ČSN EN 54-2 Electrical fire alarm – Part 2: Centre

ČSN EN 54-3 Electrical fire alarm – Part 3: Fire alarm devices – sirens

ČSN EN 54-4 Electrical fire alarm – Part 4: Power supply

ČSN EN 54-5 Electrical fire alarm – Part 5: Heat fire detectors – Point detectors

ČSN EN 54-7 Electrical fire alarm – Part 7: Smoke fire detectors – Scattered-light, emitted light and ionization point fire detectors

ČSN EN 54-11 Electrical fire alarm – Part 11: Break glass push button switches, manual call points, remote manual control.

8. DEVICES FOR SEARCH OF DANGEROUS SUBSTANCES OR OBJECTS

The devices for search of dangerous substances or objects shall be certified by the Authority and used at the access points to the TOP SECRET category facility or security area, or at the access points to the area designated as the meeting room, in which information classified TOP SECRET is regularly discussed.

9. DEVICES FOR PHYSICAL DESTRUCTION OF DATA CARRIERS

9.1.Type 4 devices for physical destruction of data carriers**No marks**

Type 4 devices for physical destruction of data carriers are designed to destruction of TOP SECRET classified information or information classified below. The devices for physical destruction of data carriers shall be certified by the Authority.

Information carrier	Size of particles after destruction	
E.g. paper, polyester film, where information is stored in original size, metal, plastic, identification cards	width of particles	$\leq 0.8\text{mm}$
	length of particles	$\leq 13.0\text{mm}$
E.g. polyester film, where information is stored in reduced size, as microfilm, chip cards	surface of particles	$\leq 0.2\text{mm}^2$

9.2.Type 3 devices for physical destruction of data carriers**No marks**

Type 3 devices for physical destruction of data carriers are designed to destruction of SECRET classified information or information classified below. The devices for physical destruction of data carriers shall be certified by the Authority.

Information carrier	Size of particles after destruction	
E.g. paper, polyester film, where information is stored in original size, metal, plastic, identification cards	width of particles	$\leq 2.0\text{mm}$
	length of particles	$\leq 15.0\text{mm}$
E.g. polyester film, where information is stored in reduced size, as microfilm, chip cards	surface of particles	$\leq 0.5\text{mm}^2$

9.3.Type 2 devices for physical destruction of data carriers**No marks**

Type 2 devices for physical destruction of data carriers are designed to destruction of CONFIDENTIAL classified information or information classified below. The devices for physical destruction of data carriers shall be certified by the Authority.

Information carrier	Size of particles after destruction
---------------------	-------------------------------------

E.g. paper, polyester film, where information is stored in original size, metal	Cross-cut	width of particles	$\leq 4.0\text{mm}$
		length of particles	$\leq 80.0\text{mm}$
	Straight-cut	width of the strip	$\leq 2.0\text{mm}$
		length of the strip	$\leq 297.0\text{mm}$
		surface of particles*	$\leq 320.0\text{mm}^2$
Plastic, e.g. identification cards	width of particles	$\leq 4.0\text{mm}$	
	length of particles	$\leq 80.0\text{mm}$	
E.g. polyester film, where information is stored in reduced size, as microfilm, chip cards	surface of particles	$\leq 1.0\text{mm}^2$	

9.4.Type 1 devices for physical destruction of data carriers

No marks

Type 1 devices for physical destruction of data carriers are designed to destruction of RESTRICTED classified information. The devices for physical destruction of data carriers shall be certified by the Authority.

Information carrier	Size of particles after destruction		
E.g. paper, polyester film, where information is stored in original size, metal	Straight-cut	width of the strip	$\leq 6.0\text{mm}$
		length of the strip	not limited
		surface of particles*	$\leq 320.0\text{mm}^2$

9.5.Type 0 devices for physical destruction of data carriers

No marks

Type 0 devices for physical destruction of data carriers are designed to destruction of TOP SECRET classified information or information classified below. Incineration or melting shall be used for destruction of the information carrier in such a way that the temperature, to which the carrier will be exposed, and time of its exposure to that temperature shall result in its full destruction. The user of the facility, who discards classified information, shall ensure that the carrier will be completely destroyed by incineration or melting and that classified information will be thus transformed into an unrecognisable and non-reconstitutable form.

10. PROTECTION AGAINST PASSIVE AND ACTIVE EAVESDROPPING

* This applies only for high capacity device with capacity ≥ 500 kg/h.

The area designated as the meeting room, in which information classified SECRET and TOP SECRET is regularly discussed shall be protected against passive and active eavesdropping by technical means certified by the Authority.

Requirements for protection of the area designated as the meeting room against passive and active eavesdropping shall be as follows:

- the area designated as the meeting room shall be protected against passive eavesdropping by soundproofing walls, doors, floors and ceiling (attenuation on the perimeter of the area designated as the meeting room shall be 50dB as a minimum);
- windows, vents or ducts shall be protected by Type 4 technical means certified by the Authority (article 2.1.1. of the Annex). The area designated as the meeting room shall be protected against overlooking from outside;
- no item or furnishings or equipment shall be allowed into the area designated as the meeting room until it has been thoroughly examined physically for eavesdropping device by trained security staff. A records of the type, serial and inventory numbers shall be kept of equipment and furniture moved into and out the area designated as the meeting room, including the history of its movement;
- telephones should not normally be installed in the area designated as the meeting room. However, where their installation is unavoidable, they shall be provided with a positive disconnect device or shall be physically disconnected before classified discussions take place;
- the presence of mobile telephones, any recording devices, transmitting devices, any testing, measuring and diagnostic devices and other electronic items shall be prohibited in the areas designated as the meeting room. This requirement does not apply with respect to devices used in connection with protective inspections conducted with the knowledge of the responsible person or person authorised by him/her.

According to S. 26 par. 1 of the Act the responsible person shall request the Authority to carry out the security inspection of the area designated as the meeting room in order to establish that no technical means is used without authorization, which are designed to obtain information (hereinafter “the Security inspections”). Installation of technical means against passive and active eavesdropping of classified information shall be verified during the Security inspection.

Periodicity of Security inspections of areas designated as the meeting room shall be according to S. 10 par. 1 of the Regulation and Security inspection shall also be undertaken following any unauthorised entry or suspicion of such and entry by external personnel for maintenance work or other works within the area designated as the meeting room.

The application for carrying out the Security inspection shall contain the following:

- a company's name, title or name and surname should the applicant be a person pursuing business, or the name of the State body including registration number if this has been assigned;
- the address of location of an area designated as the meeting room;

- the floor area and ceiling height;
- the date of anticipated Security inspection;
- reasons for Security inspection (e.g. completing with furniture or suspicion of unauthorised entry);
- the name and surname of a contact officer and his/her contact address;
- the signature of the responsible person.

Requirements for carrying out Security inspections:

- a natural person carrying out Security inspections shall be a holder of the valid personnel security clearance for access to information classified SECRET or above;
- a report shall be produced on the course of the Security inspection, which shall contain:
 1. data concerning the State body that carries out the Security inspection;
 2. name of the company should the applicant be a facility or the name of the State body including registration number if this has been assigned, which uses the mentioned area designated as the meeting room;
 3. address of location of the area designated as the meeting room;
 4. date and time when the Security inspection has been carried out;
 5. description of the area designated as the meeting room (of the area being controlled) including photo documents;
 6. acts undertaken;
 7. control, measuring and test devices used;
 8. results of the measurement;
 9. results of the Security inspection (evaluation).

Report on the course of the Security inspection shall be attached to the physical security project.

11. CONDITIONS GOVERNING THE USE OF TECHNICAL MEANS BEYOND THE VALIDITY PERIOD OF ITS CERTIFICATE

11.1.CERTIFICATE OF THE “T” TYPE TECHNICAL MEANS

Number of the certificate: T xxxx / year

No procurement of the technical means or its re-use may be allowed beyond the validity period of its certificate.

Usage of installed technical means shall be bound by rules as laid down below in paragraph 11.3 of the Annex.

11.2.INDIVIDUAL TECHNICAL MEANS CERTIFICATE

Number of the certificate: TU xxxx / year

This certificate is issued only for individual technical means, the identification of which will be quoted in the certificate. It will be issued upon request of a user of the technical means and granted on the basis of evaluation according to S. 46 par. 14 of the Act.

Beyond the validity period of the certificate the technical means may be used for extended validity period not exceeding six years.

11.3. RULES GOVERNING THE USE OF CERTIFIED TECHNICAL MEANS BEYOND THE VALIDITY PERIOD OF THE “T” CERTIFICATE

a) mechanical barriers (number of the certificate T 0xxx / year)

Beyond the validity period of the certificate the technical means of this type may be used for extended validity period not exceeding 15 years. If the user plans to use the technical means even if the extended validity period ends, he/she/it may ask to be issued with the certificate according to paragraph 11.2 in connection with its expiration.

b) electrical locking devices and entry control systems (number of the certificate T 1xxx/year)

electrical security alarm annunciation equipment (number of the certificate T 3xxx / year)

CCTV (number of the certificate T 2xxx / year)

emergency systems (number of the certificate T 1xxx / year)

electrical fire alarm equipment (number of the certificate T 4xxx / year)

devices for search of dangerous substances or objects (number of the certificate T 6xxx / year)

device for protection against passive and active eavesdropping (number of the certificate T 7xxx / year)

Beyond the validity period of the certificate these technical means may be used on the condition that they are fully operational. This must be verified by operation test supported by the test certificate or by the record in the log book. Periodicity is determined in S. 10 of this Regulation.

c) devices for physical destruction of data carriers (number of the certificate T 5xxx / year)

Beyond the validity period of the certificate the technical means of this type may be used on the condition that it is fully operational. The functionality shall be verified in periods determined in S. 10 of the Regulation and the record shall be made thereof.

12. MINIMUM BASELINE SECURITY MEASURES MATRIX

12.1. MINIMUM BASELINE SECURITY MEASURES MATRIX FOR THE SECURITY AREA

TOP SECRET CATEGORY SECURITY AREA	Risks levels		
	Low	Medium	High
Mandatory: (S1) + (S2) + (S3)	10	11	13
Mandatory: (S4) + (S5)*	6	7	7
Additional: (S6)	4	5	5
Total score	20	23	25

SECRET CATEGORY SECURITY AREA	Risks levels		
	Low	Medium	High
Mandatory: (S1) + (S2) + (S3)	8	9	10
Mandatory: (S4) + (S5)**	4	5	5
Additional: (S6)	4	5	5
Total score	16	19	20

CONFIDENTIAL CATEGORY SECURITY AREA	Risks levels		
	Low	Medium	High
Mandatory: (S1) + (S2) + (S3)	6	8	9
Mandatory: (S4) + (S5)	2	3	3
Additional: (S6)	3	3	4
Total score	11	14	16

RESTRICTED CATEGORY SECURITY AREA	Risks levels		
	Low	Medium	High
Mandatory: (S1) + (S2) + (S3)	2	2	2
Additional: (S4) + (S5) + (S6)	0	1	2
Total score	2	3	4

Note: Only one State body, legal person or a person pursuing business may use a specified facility, security area for activities relating to the protection of classified information.

Only one of (S1), (S2) or (S3) may score zero.

12.2. MINIMUM BASELINE SECURITY MEASURES MATRIX FOR AN AREA DESIGNATED AS THE MEETING ROOM

* (S5) shall score at least 5 points.

** (S5) shall score at least 4 points.

AREA DESIGNATED AS THE MEETING ROOM (in which TOP SECRET information is regularly discussed)	Risks levels		
	Low	Medium	High
Mandatory: (S2) + (S3)	6	6	7
Mandatory: (S4) + (S5)*	6	7	7
Additional: (S6)	4	5	5
Total score	16	18	19

AREA DESIGNATED AS THE MEETING ROOM (in which SECRET information is regularly discussed)	Risks levels		
	Low	Medium	High
Mandatory: (S2) + (S3)	5	5	6
Mandatory: (S4) + (S5)**	4	5	5
Additional: (S6)	4	5	5
Total score	13	15	16

Note: (S2) shall not score zero.

13. INFORMATION SYSTEMS PHYSICAL SECURITY

If such part of an information system is located in a security area or facility, which can contain classified information, it shall be assessed as the security equivalent of a container. The identification together with the authentication of the user constitutes the security equivalent of lock of the container.

13.1. DATA PROCESSING

Information systems used only for displaying, processing or transmission of classified information up to SECRET level may be located within the facility outside the security area.

13.1.1. Classified information may only be displayed and processed or transmitted by the given part of the information system

SS1 = 4

If one or more parts of the information system are located in a security area, the lowest SS1 shall be applied with respect to individual parts of the information system.

13.2. STORAGE OF CLASSIFIED INFORMATION ON COMPUTER STORAGE MEDIA (ALL NON-VOLATILE STORAGE MEDIA)

Areas, in which information systems are used for storage of information classified RESTRICTED or above, shall be established as security areas.

* (S5) shall score at least 5 points.

** (S5) shall score at least 4 points.

13.2.1. Stored data has been encrypted by certified cryptographic device**SS = 4**

In addition to SS1, which relates to encrypted data stored, also SS1 of the cryptographic device shall be taken into account.

13.2.2. Stored data has not been encrypted**SS = 1**

This manner of the data storage constitutes the security equivalent of a Type 1 container.

13.2.3. Destruction of data carriers**No marks**

Only certified devices designed solely for the purposes of destruction of mentioned data carriers or certified devices for the physical destruction of information carriers may be used for the physical destruction of data carriers, which meet the requirements stated below. Also incineration or melting may be used for their destruction in such a way that the temperature, to which the carrier will be exposed, and time of its exposure to the temperature shall result in its full destruction. The user of the facility, who discards classified information, shall ensure that the carrier will be completely destroyed by incineration or melting and that classified information will be thus transformed into an unrecognisable and non-reconstitutable form. However, the condition must be present that the certified means in question shall be determined by the producer for destruction of these types of material.

Requirements for destruction of diskettes and compact discs shall be as follows:

- requirements for devices designed solely for the purposes of physical destruction of diskettes and compact discs for all security levels:

Data carrier	Size of particles after destruction		
Diskettes, compact discs and similar media	Straight-cut	width of the strip	≤ 12.0mm
		length of the strip	not limited
		surface of particles*	≤ 320.0mm ²

or

Data carrier	Size of particles after destruction
Diskettes, compact discs and similar media	Certified devices for physical destruction of information carriers at least of the Type 1

- requirements for destruction of magnetic tapes, memory chips and hard discs:

* This applies only for high capacity device with capacity ≥ 500 kg/h.

Data carrier	Size of particles after destruction	
Magnetic tapes, hard discs	width of particles	$\leq 0.8\text{mm}$
	length of particles	$\leq 13.0\text{mm}$
Memory chips	surface of particles	$\leq 0.2\text{mm}^2$

or

Data carrier	Size of particles after destruction
Magnetic tapes	Certified device for physical destruction of information carriers Type 4

13.3.IDENTIFICATION AND AUTHENTICATION OF THE USER

13.3.1.Identification by name and authentication by token with encrypted content and transmission

SS2 = 4

Cryptographic mechanisms of the token used for authentication shall be certified by the Authority.

This method of authentication constitutes the security equivalent of a Type 4 lock of the container.

13.3.2.Identification by name and authentication by token with encrypted content

SS2 = 3

Cryptographic mechanisms of the token used for authentication shall be certified by the Authority.

This method of authentication constitutes the security equivalent of a Type 3 lock of the container.

13.3.3.Identification by name and authentication by token

SS2 = 2

The token used for authentication shall be certified by the Authority within the frame of the information system certification.

This method of authentication constitutes the security equivalent of a Type 2 lock of the container.

13.3.4.Identification by name and authentication by password

SS2 = 1

The minimum length of the password and the method of its generation shall be approved by the Authority within the frame of the information system certification.

This method of authentication constitutes the security equivalent of a Type 1 lock of the container.

The section score S1 will be calculated from SS1 and SS2 obtained according to articles 13.1 or 13.2 and 13.3:

$$(S1) = SS1 \times SS2$$

The section score (S1) will be used in the minimum baseline security measures matrix for the secure area and for the area designated as the meeting room (article 12 of the Annex).

14. STRUCTURE OF THE PHYSICAL SECURITY PROJECT

14.1. RISKS ASSESSMENT

The following stages shall be the part of the risk assessment process:

- specification of assets – anticipated volume of classified information according to classification levels;
- determination and assessment of threats and vulnerabilities;
- determination of the total risk level as “low”, “medium” or “high”.

14.2. DETERMINATION OF FACILITIES, SECURITY AREAS AND AREAS DESIGNATED AS THE MEETING ROOM INCLUDING THEIR PERIMETERS, AND DETERMINATION OF CATEGORIES AND CLASSES OF SECURITY AREAS AND AREAS DESIGNATED AS THE MEETING ROOM

- General introduction (address), territory/premises description (perimeter description, number of buildings/number of floors, points of access, safeguarding, if any), surrounding area (particularly objects that could affect security), external subjects in the area/building (number, or the name and aiming of activities), schema.
- Determination of the facility and of its type.
- Determination of the perimeter surrounding the facility (location in the area/building, strength of walls, points of access, length of windows, resident guards post).
- Description of the facility safeguarding.
- The facility perimeter shall be drawn in the drawing part of the Technical documentation of the physical security (article 14.3.2 of the Annex).
- Determination of security areas within the facility, their type, category and class. The distinction shall be drawn whether these are storage rooms for classified information, sites with information system, permanently manned areas by staff normally working in these areas, areas designated as the meeting room or combination of these types.
- Determination of the perimeter of security areas and areas designated as the meeting room (location within the facility, strength of walls, points of access, height of the lower edge of man-openings above surrounding ground) and drawing it in the drawing part of the Technical documentation of the physical security.
- The marks score table of physical security measures shall be drawn up for each security area and area designated as the meeting room.

14.3. METHODS OF APPLICATION OF PHYSICAL SECURITY MEASURES

14.3.1.MARKS SCORE TABLE OF PHYSICAL SECURITY MEASURES IN THE SECURITY AREA AND IN THE AREA DESIGNATED AS THE MEETING ROOM

The heading of the table shall contain the following data:

- the name of the security area (of the area designated as the meeting room);
- the category and class of the security area;
- the type of the area designated as the meeting room according to classified information regularly discussed in this area;
- the purpose of the security area (of the area designated as the meeting room).

SECURITY MEASURE	TYPE	MARKS SCORE
Containers	<ul style="list-style-type: none"> ○ T.4 – 4 marks ○ T.3 – 3 marks ○ T.2 – 2 marks ○ T.1 – 1 mark 	SS1 =
Locks of containers	<ul style="list-style-type: none"> ○ T.4 – 4 marks ○ T.3 – 3 marks ○ T.2 – 2 marks ○ T.1 – 1 mark 	SS2 =
Container, including the locking system	<ul style="list-style-type: none"> ○ T.1A – 1 mark ○ T.1B – 2 marks ○ T.1C – 3 marks ○ T.1T – 1 mark ○ T.T – not indicated 	S1 =
The total score of the container and its lock	$S1 = SS1 \times SS2$	S1 =
Security areas	<ul style="list-style-type: none"> ○ T.4 – 4 marks ○ T.3 – 3 marks ○ T.2 – 2 marks ○ T.1 – 1 mark 	SS3 =
Locking systems of the security area	<ul style="list-style-type: none"> ○ T.4 – 4 marks ○ T.3 – 3 marks ○ T.2 – 2 marks ○ T.1 – 1 mark 	SS4 =
The total score of the security area and its locking system	$S2 = SS3 \times SS4$	S2 =
Facility	<ul style="list-style-type: none"> ○ T.4 – 5 marks ○ T.3 – 3 marks ○ T.2 – 2 marks ○ T.1 – 1 mark 	S3 =
Access control	<ul style="list-style-type: none"> ○ T.4 – 4 marks ○ T.3 – 3 marks 	SS6 =

	<ul style="list-style-type: none"> ○ T.2 – 2 marks ○ T.1 – 1 mark 	
Visitors regime within the facility a)Escorted visits b)Unescorted visits c)Visits without control	<ul style="list-style-type: none"> ○ ad a) – 3 marks ○ ad b) – 1 mark ○ ad c) – 0 	SS7 =
The total score of the access control	S4 = SS6 + SS7	S4 =
Guards	<ul style="list-style-type: none"> ○ T.5 – 5 marks ○ T.4 – 4 marks ○ T.3 – 3 marks ○ T.2 – 2 marks ○ T.1 – 1 mark 	SS8 =
Electrical security alarm annunciation equipment	<ul style="list-style-type: none"> ○ T.4 – 4 marks ○ T.3 – 3 marks ○ T.2 – 2 marks ○ T.1 – 1 mark 	SS91 =
Installation of the electrical security alarm annunciation equipment	<ul style="list-style-type: none"> ○ T.4 – 4 marks ○ T.3 – 3 marks ○ T.2 – 2 marks ○ T.1 – 1 mark 	SS92 =
Sub-score (SS9)		SS9 =
Total evaluation of guards and of the electrical security alarm annunciation system	S5 = SS8 + SS9	S5 =
Physical barriers	<ul style="list-style-type: none"> ○ T.7 – 12 marks ○ T.6 – 9 marks ○ T.5 – 7 marks ○ T.4 – 4 marks ○ T.3 – 3 marks ○ T.2 – 2 marks ○ T.1 – 1 mark 	SS10 =
Access control at access points of the physical barrier a)The control is in place b)No control	<ul style="list-style-type: none"> ○ ad a) – 1 mark ○ ad b) - 0 	SS11 =
Random exit and entry searches a)The searches are undertaken b)The searches are not undertaken	<ul style="list-style-type: none"> ○ ad a) – 1 mark ○ ad b) - 0 	SS12 =
Perimeter detection system (PDS)	2 marks	SS13 =
Security lighting of the perimeter	2 marks	SS14 =
CCTV on the perimeter	2 marks	SS15 =
The total section score of the perimeter protection	S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15	S6 =

Section scores S1 to S6 resulting from completion of the marks score table of physical security measures in the security area shall be compared with the minimum baseline security measures matrix for the security area and for the area designated as the meeting room, according to the section 12 of the Annex.

A decision shall be taken on the basis of this comparison on whether the measures of the physical security implemented are sufficient for the given risk level and for the given category of the security area.

A decision shall be taken on the basis of this comparison on whether the measures of the physical security implemented are sufficient for the given risk level and with respect to classification level of classified information being regularly discussed in the area designated as the meeting room.

Verification whether physical security measures applied and risks assessment correspond with the physical security project and legal regulations in the area of protection of classified information shall be the responsibility of the user of the facility or of a person authorised by him/her.

Operational tests of electrical security alarm systems shall be carried out according to TNI 33 45 91-3. The scope and periodicity of operational tests is provided for in the Table A1 (level 1). Conditions of operational test of other technical devices shall be determined by the user of the facility or by a person authorised by him/her.

Records of operational tests made of technical means outlined in S. 30 par. 1 of the Act shall be deposited with the user of the facility.

14.3.2. TECHNICAL DOCUMENTATION OF THE PHYSICAL SECURITY

This documentation shall be structured as follows:

- **Drawing documentation**, which identifies in particular the boundary of the facility, perimeters of security areas and areas designated as the meeting room and location of technical means designed for the protection of classified information within the facility and within security areas and areas designated as the meeting room.
- **Technical means documentation**, which contains in particular specification (the name, number, and also the location in the case of more types of one class of technical means) and basic data:
 - a) Certified technical means – a copy of the certificate and annexes from the installation period (in the absence of the annex the type and evaluation of the technical means shall be entered).
 - b) Uncertified technical means – a record of check of compliance from the installation period (the specification shall be stated and methods by which the means was used).

14.4 OPERATING INSTRUCTIONS

Following shall be contained in the operating instructions:

- rules governing the movement of persons (including visitors) and traffic flow regime within the area/building;
- rules governing the movement of persons (including visitors) and traffic flow regime within the facility and within the security areas;

- rules governing the regime of movement of classified information within the facility;
- technical means operational documentation, which shall contain instructions for application of technical means, date of installation and determination of periodic inspections of technical means functionality (e.g. log books, electrical security alarm annunciation equipment manuals, CCTV, electronic access control, fire detection devices and devices for protection against passive and active eavesdropping, etc.);
- rules governing handling of keys (of identification elements of the electronic access control) to the facility and security areas and of keys to containers. In particular these rules shall address the system and method of marking, providing and handing over of these keys, safekeeping and accounting, procedures in the case of loss, storage of duplicates and rules governing their use. If the user of the facility took a decision on the storage of keys or identification data outside the facility, he/she shall keep records of this fact and ensure that observance of rules governing handling of keys or identification data outside the facility will be controlled. Similar rules should also be determined to govern handling of characters combinations used as passwords enabling access to facilities, security areas or containers.
- description of regime measures for the protection of areas designated as the meeting rooms;
- rules governing fulfilling duties of guards which shall lay down the number of guards, the manner of fulfilling the duties of guards, in particular the method of exit and entry searches of persons and vehicles, the manner in which patrols should be operating and the guard force response plan in the event of an alarm from technical means being given;
- should the guards duties be performed on the basis of a contractual relation, then the copy of the contract shall be enclosed.

14.5 SECURITY CONTINGENCY PLANS FOR FACILITIES, SECURITY AREAS AND AREAS DESIGNATED AS THE MEETING ROOMS

- Description of measures used to reduce threats and vulnerabilities outlined in the chapter titled Risks Assessment.
- Instructions for the protection of classified information in cases of emergency.

Note to the article 14.

Articles 14.1, 14.4 and 14.5 will be omitted in the physical security project in the case of the facility housing not higher than RESTRICTED category security area.

NATIONAL SECURITY AUTHORITY
P.O.Box 49
 150 06 Prague 56

The National Security Authority issues according to S. 46 of the Act N. 412/2005 Coll., on
 the protection of Classified Information

CERTIFICATE
of the technical means

Registration number:

.....
 (the name and type designation of the technical means)

Producer:

Location/permanent residence/place
 of business/address:

Identification number/personal identity number:

Holder:

Location/permanent residence/place
 of business/address:

Identification number/personal identity number:

This certificate confirms verification of capability of the technical means of the Type:

.....

Marks score of the technical means according to the Annex 1 to the Regulation N. 528/2005 Coll.,
 on the Physical Security and Certification of Technical Means:

.....

Date of expiry of the certificate:

Date of issuance of the certificate:

Stamp

Signature of authorised representative

Enclosures:

(The enclosure shall be the integral part of the certificate and may only be reproduced together.)