

336**REGULATION
Of the National Security Authority****Of 10 May 2004****On Physical Security and Building Security**

The National Security Authority (hereinafter referred to as „the Authority“) stipulates, pursuant to Article 6, paragraph 10 and Article 53, paragraph 6 of Act No. 215/2004 Coll. on protection of classified information and on amending and supplementing certain laws (hereinafter referred to as „the Act“), the following:

**Article 1
Subject of Regulation**

This Regulation establishes the security standard of physical security and building security (hereinafter referred to as „security standard“) and the particulars of protection of buildings and protected areas.

**Article 2
Security Standard**

(1) The security standard of physical security and building security determines the rules and conditions providing for the minimum required level of securing buildings and protected areas designed for the storage and handling classified information.

(2) The structure of the security standard enables generating a variable system of securing measures, depending on the local conditions (location and structure of the building, evaluation of potential endangerment risks of the classified information, etc.) in compliance with generally binding legal regulations.

(3) The objective of the security standard is to create functional, efficient, and financially optimized systems for protecting classified information. The level of physical security and building security shall be evaluated in a points system, enabling to select, in dependence on the specific conditions, the combination of security measures best suiting the given conditions.

(4) Minimum numbers of points have been specified, which must be reached in the buildings and protected areas. A mathematical method is used to allocate predefined numbers of points to the individual security measures and evaluate the total sum of points by applicable methods. The measures designated as discretionary need not be realized, but the total prescribed number of points must be reached.

**Article 3
Protected Area**

(1) For purposes of securing classified information a protected area¹ shall be defined as the protected area in one of the following categories:

- a) Top Secret, or "TS", when designed for the storage or handling classified information at the security classification level Top Secret,
- b) Secret, or "S", when designed for the storage or handling classified information at the security classification level Secret,
- c) Confidential, or "C", when designed for the storage or handling classified information at the security classification level Confidential,
- d) Restricted, or "R", when designed for the storage or handling classified information at the security classification level Restricted.

(2) The protected area's category shall be determined by the head²; the determination shall include the definition of boundaries and regime measures applying to that protected area.

(3) Depending on access to classified information, protected areas in the categories "C", "S" and "TS" shall be designated Category I or Category II protected areas.

(4) Category I protected areas are those designed for the storage or handling classified information at the security classification level Confidential or higher, in such a way that access to such areas means acquainting with classified information. Such protected areas shall have/

- a) Defined perimeters, with checkpoints established at all entries for controlling all incoming and outgoing persons and vehicles,
- b) Clearance systems, allowing access only to authorised persons³ specifically authorised by the head to enter,
- c) Specifications of classified information in the form of lists of classified information, usually maintained in the given protected area.

(5) Category II protected areas are those designed for the storage or handling classified information at the security classification level Confidential or higher, in such a way that classified information are protected from unauthorised handling by defined measures, and that access to such areas does not mean acquainting with classified information. Such protected areas shall have/

- a) Defined perimeters, with checkpoints established at all entries for controlling all incoming and outgoing persons and vehicles,
- b) Clearance systems, allowing unaccompanied entry only to authorised persons; all other persons shall be accompanied and measures accepted to prevent unauthorised handling of classified information.

(6) The head shall decide on designating Category I or Category II protected areas pursuant to paragraph 3, and specify the conditions of access within the regime measures.

¹ Article 2, indent s) of Act No. 215/2004 Coll. on protection of classified information and on amending and supplementing certain laws

² Article 8, paragraph 1 of Act No. 215/2004 Coll.

³ Article 2, indent f) of Act No. 215/2004 Coll.

(7) Upon implementing measures to prevent unauthorised handling of classified information the head may decide to change the category of the protected area by written record, which shall be part of the security plan of the building protection within the physical security and building security documentation.

(8) The rules determined by a foreign power⁴, based on an international agreement binding the Slovak Republic, also apply to the securing of buildings and protected areas designed for the storage and handling classified information submitted to the Slovak Republic by that foreign power.

Article 4 Mechanical Barrier Devices and Technical Protection Devices

- (1) Mechanical barrier devices are/
- a) Security lockers,
 - b) Lock systems and components thereof,
 - c) Doors and components thereof,
 - d) Grates,
 - e) Security foils,
 - f) Windows,
 - g) Glazing.
- (2) Technical protection devices are/
- a) Clearance systems and systems for electronic verification of the identity and authorisation of persons,
 - b) Electrical security devices and systems (violation alarm systems),
 - c) Cameras operated in closed-circuit television systems,
 - d) Emergency systems,
 - e) Devices enabling the detection of substances and things,
 - f) Devices designed to physically destroy information carriers.

Article 5 Securing Buildings and Protected Areas

- (1) The head shall determine the risks of potential endangerment of classified information in the protected area upon assessing the/
- a) Classification level of the classified information,
 - b) Amounts of classified information,
 - c) Requirements for restricting the number of authorised persons designated to acquaint with the classified information,
 - d) The need to acquaint with classified information own employees, as well as employees who, in connection with the discharge of their duties or tasks, carry out the physical protection and who, considering their authorisation and access to protected areas,

⁴ Article 2, indent h) of Act No. 215/2004 Coll.

could become accessories to external violators or themselves turn into violators (resulting, for example, in intentional damage, leakage of classified information, theft, passive or active interception, etc.),

- e) Risks of endangerment of classified information, mainly from the following viewpoints: location, placement and physical protection of the building and protected area, activities of foreign intelligence services, saboteurs, terrorist and criminal groups, technical defects, risks derived from employees' activities (lack of knowledge, forgetfulness, chance, etc.) and extraordinary situations⁵; in addition, any surrounding structures whose failure could potentially disable and/or violate the security of protected buildings shall be evaluated as risks,
- f) Risks of endangerment of classified information at times of war, belligerence, state of emergency and state of distress⁶.

(2) Based on the assessment made pursuant to paragraph 1, the head shall/

- a) Evaluate the conditions of securing the building and protected area and the security measures taken in compliance with this Regulation, and decide on the acceptance of additional measures, should the existing measures be evaluated as insufficient,
- b) Evaluate residual risks,
- c) Determine the rates of risk to the classified information as small, medium or large rate of risk.

(3) Protection of buildings shall be ensured mainly by using mechanical barrier devices specified in Article 4, paragraph 1, subparagraphs b) through g), and technical protection devices specified in Article 4, paragraph 2, subparagraphs a) through c). In cases where the boundaries of a building are identical with the boundaries of the protected area, protection shall be ensured by using certified⁷ mechanical barrier devices and certified technical protection devices of the appropriate category; devices of a lower category shall be used, when they meet the requirements of the security standard.

(4) The protected area designed for the storage of classified information shall be protected by using mechanical barrier devices of the applicable category in accordance with Article 4, paragraph 1, and technical protection devices of the applicable category specified in Article 4, paragraph 2; devices of a lower category may be used, when they meet the requirements of Section 12.1. of the security standard.

(5) The protected area designed for the storage of classified information submitted to the Slovak Republic by a foreign power shall be protected by using mechanical barrier devices of the applicable category in accordance with Article 4, paragraph 1, and technical protection devices of the applicable category specified in Article 4, paragraph 2; devices of a lower category may be used, when they meet the requirements of Section 12.2. of the security standard.

⁵ Article 3 of National Council of the Slovak Republic Act No. 42/1994 Coll. on civil defence of the population, as amended by later legislation.

⁶ Constitutional Act No. 227/2002 Coll. on state security at times of war, belligerence, state of emergency and state of distress.

⁷ National Security Authority Regulation No. 337/2004 Coll., regulating the particulars of certifying mechanical barrier devices and technical protection devices, and of their use.

(6) The protected area designed for the storage of classified information at the security classification level Top Secret, and of classified information submitted to the Slovak Republic by a foreign power at the security classification level Top Secret shall be additionally protected by using electric fire-signalling devices. Other protected areas shall be protected from fire in accordance with separate legislation⁸.

(7) Classified information at the security classification level Restricted, Confidential and Secret may be created, displayed, transferred on technical means and recorded in the protected area that is protected by using mechanical barrier devices in accordance with Article 4, paragraph 1, subparagraphs b) and c), and technical protection devices in accordance with Article 4, paragraph 2, subparagraphs a) and b).

(8) Classified information at the security classification level Top Secret may be created, displayed, transferred on technical means and recorded in the protected area that is protected in accordance with the requirements of Section 12.3. of the security standard.

(9) Classified information submitted to the Slovak Republic by a foreign power at the security classification level Restricted and Confidential may be created, displayed, transferred on technical means and recorded in the protected area that is protected by using mechanical barrier devices in accordance with Article 4, paragraph 1, subparagraphs b) and c), and technical protection devices in accordance with Article 4, paragraph 2, subparagraphs a) and b). When there are in the area windows or manholes (hereinafter referred to as “openings”) with their bottom edges less than 5.5 m above the surrounding terrain, or easily accessible from the roof, lightning conductor, eaves or other structural elements, unevenness of the terrain, trees or other structures, the windows and openings shall be secured with mechanical barrier devices in accordance with Article 4, paragraph 1, subparagraph d); this measure shall not be realized, when the perimeters of the area are secured with at least Type 3 barriers in accordance with Section 6.1 of the security standard.

(10) Classified information submitted to the Slovak Republic by a foreign power at the security classification level Secret and Top Secret may be created, displayed, transferred on technical means and recorded in the protected area that is protected in accordance with the requirements of Section 12.3 of the security standard.

(11) Protected areas of the category Confidential and higher, designed for the storage of classified information, which are permanently manned by duty personnel shall be secured mainly by using certified mechanical barrier devices of the applicable category specified in Article 4, paragraph 1, subparagraphs a) through c), and certified technical protection devices of the applicable category specified in Article 4, paragraph 2, subparagraphs a) and d). Lower category devices may be used only when they fulfil the requirements of the security standard. When there are in the area windows or openings, with their bottom edges less than 5.5 m above the surrounding terrain, or easily accessible from the roof, lightning conductor, eaves or other structural elements, unevenness of the terrain, trees or other structures, the windows and openings shall be secured with mechanical barrier devices in accordance with Article 4, paragraph 2, subparagraph d); this measure shall not be realized, when the perimeters of the area are secured with at least Type 3 barriers in accordance with Section 6.1 of the security standard.

⁸ Act No. 314/2001 Coll. on protection against fires, as amended by later legislation.

(12) Protected areas designed for the storage and handling of classified information submitted to the Slovak Republic by a foreign power, which are not permanently manned by duty personnel shall be checked after office hours, whether there are no freely accessible classified information or wastes therein, and whether the security lockers, doors and windows are locked. The head shall appoint an employee for the execution of the check, the results of which shall be recorded in writing.

Article 6 Protection of Conference Rooms

(1) Conference rooms used to discuss classified information shall be protected from active and passive interception by regime measures and technical security inspections.

(2) Conference rooms regularly used to discuss classified information shall be protected from active and passive interception by using regime measures, technical security inspections, mechanical barrier devices and technical protection devices.

Article 7 Duplication and Destruction of Classified information

(1) Classified information at all security classification levels, exchanged between the Slovak Republic and a foreign power, and other classified information at the security classification level Top Secret may be duplicated and destroyed only in a protected area of the appropriate category in compliance with Section 12.3 of the security standard, which must meet the conditions specified in separate legislation⁹.

(2) Classified information at all levels of security classification, except for those specified in paragraph 1 may be duplicated and destroyed also in a building outside of the protected area, providing fulfilment of the conditions specified in separate legislation⁹.

(3) Classified information at the security classification level Confidential and higher shall be destroyed by using a certified device for physical destruction of information carriers of the applicable category. The head may decide on different methods of destroying classified information (incineration, crushing, grinding). The destruction shall be accomplished while fulfilling the conditions of separate legislation⁹ and must result in such destruction of the classified information that any acquaintance with their contents would be impossible.

Article 8 Security Keys

- (1) Security keys are keys to/
- a) Security lockers, designed for the storage of classified information,
 - b) Entrances to protected areas,
 - c) Entrances to conference rooms,

⁹ National Security Authority Regulation No. 338/2004 Coll. on administrative security.

d) Entrances to buildings.

(2) Security keys are issued against signature to employees. The head, or the employee appointed by the head maintains records showing the location of all security keys, and records of their corresponding lock numbers or security locker numbers.

(3) Security keys specified in paragraph 1, subparagraph a) through c) shall be kept after office hours in a security locker or in a locked cabinet, which must be secured against unauthorised handling.

(4) Duplicate security keys shall be kept by the head or by the employee appointed by the head, who maintains the security key records and records of their corresponding lock numbers or security locker numbers. The duplicate security keys shall be kept in envelopes or in other packages marked so as to identify the persons authorised to draw these keys. The envelopes or other packages with the duplicate security keys shall be placed in a security locker other than that used for keeping the original security keys.

(5) Additional duplicate security keys may be produced only with written consent of the head or the employee appointed by the head, and their production shall be entered in the records on security keys.

Article 9

Physical Protection of Buildings and Protected Areas

(1) Physical protection of buildings and protected areas (hereinafter referred to as “physical protection”) is carried out by members of the armed forces, armed security corps, other security corps, employees of private security services, employees of the entity operating the building, or by own employees.

(2) The persons who carry out physical protection shall be trained, and equipped with appropriate means of communications.

(3) Entry to the protected area shall be allowed only to those persons carrying out physical protection, who meet the conditions specified in Article 3, paragraph 4, subparagraph b), or in Article 3, paragraph 5, subparagraph b).

(4) When, in a building or protected areas designed for the storage and handling of classified information submitted to the Slovak Republic by a foreign power, response is carried out by persons executing physical protection, or by persons responding to a signal from an electric signalling device terminating at the alarm registration centre or otherwise terminating, at least two such persons shall take action in the response at any place of violation of the protection of classified information, whereby the taking of such action must not result in weakening of the protection of other parts of the building. In other cases the method of responding shall be decided by the head.

(5) The head shall determine the response time of physical protection to alarm signals so that it would be shorter than the time required to overcome the measures realized to protect classified information. The head shall also determine the frequency of verification of

the response of physical protection to alarm signals; such verification shall be accomplished at least once in the year.

(6) The rules of providing physical protection shall be determined by the head in the security documentation of physical security and building security, in accordance with the requirements of the security standard.

(7) The persons executing physical protection of buildings and protected areas designed for the storage and handling of classified information submitted to the Slovak Republic by a foreign power shall make rounds along random-selected routes in irregular time intervals/

- a) not exceeding 2 hours in buildings or protected areas designed for the storage or handling of classified information at the security classification level Top Secret,
- b) not exceeding 4 hours in buildings or protected areas designed for the storage or handling of classified information at the security classification level Secret,
- c) not exceeding 6 hours in buildings or protected areas designed for the storage or handling of classified information at the security classification level Confidential,
- d) Rounds shall be made in shorter intervals during night hours and after office hours, depending on the risks of endangerment of classified information, as decided by the head.

(8) The method of executing physical protection and the frequency of rounds in other cases shall be decided by the head.

(9) The physical protection of buildings or protected areas designed for the storage and handling of classified information exchanged between the Slovak Republic and a foreign power shall be at least Type 3 according to Section 5.1 of the security standard, shown in the Annex.

Article 10 Regime Measures

(1) Regime measures are measures designed to/

- a) Determine the conditions of entry of buildings and protected areas by persons and transport means and the conditions of leaving buildings and protected areas by persons and transport means,
- b) Determine the conditions of movement of persons and transport means in the building and protected area during and after office hours,
- c) Determine the conditions of use of mobile telephones, video recorders, cameras, audio recording equipment, etc.,
- d) Determine the conditions of protecting areas for processing, duplication and destruction of classified information,
- e) Determine the conditions and methods of checking buildings and protected areas after leaving of employees, so as to exclude unauthorised handling of classified information,
- f) Protect the conference rooms,
- g) Determine the conditions of use, allocation, marking and storage of original and duplicate keys and records thereof, and of the lock and lockable system mediums,
- h) Determine the conditions of use, allocation, marking, storage and records of code settings and passwords enabling access to buildings, protected areas and security lockers,

- i) Determine the conditions of handling and using mechanical barrier devices and technical protection devices,
- j) Determine procedure applying to any case of violation or attempted violation of buildings and protected areas,
- k) Determine procedure applying to any extraordinary situation, including plans of securing, evacuation or destruction of classified information and identification of the person responsible for its implementation.

(2) The measures specified in paragraph 1, subparagraphs j) and k) shall be verified as decided by the head but at least once in a year.

(3) Changes in the code settings and of passwords shall be carried out at the time of installation of the mechanical protection device or technical security device, at any change of personnel with allocated code settings or passwords, or always at the occurrence of any endangerment or suspected endangerment of classified information. Changes in the code settings and of passwords shall be carried out in intervals not exceeding 6 months when such code settings or passwords enable access to classified information at the security classification level Top Secret or Secret, and in intervals not exceeding 12 months when such code settings or passwords enable access to classified information at the security classification level Confidential or Restricted. All changes of passwords or code settings shall be recorded. The code settings and passwords shall be placed at the assigned employee.

Article 11

Security Documentation of Physical Security and Building Security

(1) The security documentation of physical security and building security (hereinafter referred to as “security documentation”) applying to buildings and protected areas of the category Confidential and higher comprises the/

- a) Evaluation of risks in accordance with Article 5, paragraphs 1 and 2,
- b) Security plan of the building protection,
- c) Technical documentation of the building,
- d) Rules of operation of the building,
- e) Rules of executing physical protection of the building,
- f) Crisis plan of the building protection,
- g) Logbook of checks,
- h) Logbook of visitors to the protected area.

(2) The security documentation of the building comprises/

- a) The address and description of the building, mainly the description of its enclosure, number of entries, description of surroundings, or the number of structures or floors, when the building has several structures or floors,
- b) Determination of the category and class of protected areas located in the building and the description of activities performed therein,
- c) Determination of the enclosure of the building and of the protected area, including the description of its location, entries, thickness of walls, dimensions of windows, above-ground height of windows, etc.,
- d) Graphic representation of the building and of its enclosure, of the protected area and of its enclosure,

e) The security evaluation table separately for each protected area, showing the points allocated to the security measures in accordance with the security standard.

(3) The technical documentation comprises/

- a) The list and specifications of mechanical barrier devices and technical protection devices designed to secure the building and the protected area,
- b) Rules and instructions of use of mechanical barrier devices and technical protection devices, their operation and maintenance manuals, plans for their inspection, maintenance and functional verification, records of inspections of the mechanical barrier devices and technical protection devices; unless specified differently by this Regulation, functional checks of mechanical barrier devices and technical protection devices shall be carried out at least once in the year,
- c) Copies of certificates of mechanical barrier devices and technical protection devices,
- d) Technical security clearance reports.

(4) The rules of operation comprise regime arrangements specified in Article 10, paragraph 1, subparagraphs a) through i), and the method of checking compliance therewith.

(5) The rules of physical protection of the building and protected area comprise the/

- a) Method of securing the physical protection of the building and protected area,
- b) Instructions for the securing of physical protection,
- c) Determination of the number of persons securing the physical protection,
- d) Method of checking incoming and outgoing persons and vehicles to and from the building and protected area,
- e) Method of making random inspections,
- f) Method of making rounds,
- g) Method of responding to alarm warnings, provided by technical devices,
- h) Method of controlling the execution of physical protection.

(6) The building protection crisis plan comprises the regime arrangements specified in Article 10, paragraph 1, subparagraphs j) and k), and the method of checking compliance therewith.

(7) The logbook of visitors to the protected area comprises the given name, family name, title and number of the identification card or other valid identification document.

(8) The security documentation of buildings and protected areas in the category Restricted comprises the/

- a) Evaluation of risks in accordance with Article 5, paragraphs 1 and 2,
- b) Address and description of the building and of the protected area, mainly definition of the enclosure of the building and of the protected area, including description of the location, entries, wall thicknesses, dimensions of windows, above-ground height of windows, etc.,
- c) Security evaluation table, separately for each protected area, showing the points allocated to the security measures in accordance with the security standard,
- d) List and specifications of mechanical barrier devices and technical protection devices, rules and instructions of use of mechanical barrier devices and of technical protection devices, their operation and maintenance manuals, plans for their inspection, maintenance

and functional verification, inspection records; functional checks shall be carried out at least once in the year,

- e) Regime arrangements according to Article 10, paragraph 1, and the method of checking compliance therewith.

(9) The security documentation shall be clear, brief, explicit and accurate. It shall be kept by the head or by his appointee. The head is responsible for compliance of the documentation with the actual conditions and for acquainting the employees with the security documentation, in the range necessary for the discharge of their duties or tasks, at least once in a year. The security documentation shall be updated after any change influencing its contents.

(10) The security documentation shall be checked/

- a) At least once in two years, when applying to protected areas of the category Restricted,
b) At least once in a year, when applying to protected areas of the categories Confidential, Secret and Top Secret.

(11) Each change in the security documentation shall be recorded in the logbook of checks, and employees shall be acquainted therewith in the range necessary for the discharge of their duties or tasks.

Article 12 Joint Provision

The provisions of Articles 5 through 11 shall appropriately apply to the dislocation of technical devices¹⁰, means of cipher protection of information¹¹ and cryptographic systems of protecting information¹² used to discharge duties in accordance with separate legislation¹³ outside of the territory of the Slovak Republic, or used by the armed forces of the Slovak Republic under field campaign conditions.

Article 13 Effective Date

This Regulation shall enter into force on 1 June 2004.

Aurel Ugor, by hand

¹⁰ Article 2, indent i) of Act No. 215/2004 Coll.

¹¹ Article 2, indent p) of Act No. 215/2004 Coll.

¹² Article 2, indent o) of Act No. 215/2004 Coll.

¹³ For example, Articles 88, 88a, 88c and 88d of the Code of Criminal Procedure; Article 10 of National Council of the Slovak Republic Act No. 46/1993 Coll. on the Slovak Information Service, as amended by later legislation; Article 39 of National Council of the Slovak Republic Act No. 171/1993 Coll. on the police force, as amended by later legislation; Article 10 of National Council of the Slovak Republic Act No. 198/1994 Coll. on the military intelligence service, as amended by later legislation; Article 37 of Act No. 57/1998 Coll. on the railway police, as amended by later legislation; Article 26 of Act No. 4/2001 Coll. on the Corps of prison and judicial guards, as amended by later legislation; Article 25 of Act No. 240/2001 Coll. on state customs administration bodies, as amended by later legislation.

SECURITY STANDARD OF PHYSICAL SECURITY AND BUILDING SECURITY

1. STORAGE OF CLASSIFIED INFORMATION

Classified information are stored in security lockers, defined as portable safes and strong rooms. Security lockers are evaluated by their resistance against clandestine and violent penetration. When the risk of clandestine penetration exceeds the risk of violent penetration, a lower-type locker room may be used in combination with a lock belonging to a higher-type security locker. Security lockers ensure protection of classified information stored therein by their break-in resistance, expressed in the appropriate security class in accordance with the standard¹.

Security lockers designed for the storage of classified information of cryptographic nature shall be equipped with two locks, one of which shall be an at least three-positioned mechanical combination lock.

Security lockers designed for the storage of classified information submitted to the Slovak Republic by a foreign power shall be equipped with two locks, at least one of which shall be a mechanical combination lock and at least a three-positioned mechanical or electric combination lock in accordance with the requirements of Section 12.2 of the security standard. The security locker shall be always checked after office hours.

Strong rooms designed for the storage of classified information shall be equipped with a minimally emergency illumination system, a fire extinguisher and devices enabling to summon assistance. Entry to the strong room shall be monitored with a camera operated in a closed-circuit television system. The strong room manufacturer shall apply for its certification.

When the security locker is equipped with two locks, only one of them shall be evaluated in the point evaluation system.

1.1. Security lockers

1.1.1. Security locker – Type 4	SS₁= 4 points
--	---------------------------------

- a) Security locker designed for the storage of classified information at all levels of security classification, providing it is placed in a Class I or II protected area,

¹ STN EN 1143-1, STN EN 1143-2 and related standards, or the testing procedures of authorised persons, approved by the Authority.

- b) Security locker in the Top Secret category meeting the requirements of Class II or higher according to the standard¹, equipped minimally with one A type lock according to the standard².

1.1.2. Security locker – Type 3

SS₁= 3 points

- a) Security locker designed for the storage of classified information at all levels of security classification, providing it is placed in a Class I or II protected area,
b) Security locker in the Secret category meeting the requirements of Class I or higher according to the standard¹, equipped minimally with one A type lock according to the standard².

1.1.3. Security locker – Type 2

SS₁= 2 points

- a) Security locker designed for the storage of classified information at the security classification level Secret or lower, providing that it is placed in a Class I or II protected area,
b) Security locker in the Confidential category, meeting the requirements of Class 0 according to the standard¹, equipped minimally with one C type lock according to the standard².

1.1.4. Security locker – Type 1

SS₁= 1 point

- a) Security locker designed for the storage of classified information in the category Confidential or lower,
b) Security locker at the security classification level Restricted, comprising at least a locked cabinet made of sheet metal so that it cannot be disassembled, equipped minimally with a Type 1 lock (Section 1.2.4.); its specification shall be shown in the security documentation of physical security and building security.

1.2. Locks for security lockers

1.2.1. Lock for security lockers – Type 4

SS₂= 4 points

- a) Lock providing high degree of resistance against expert and professional penetration by a violator using specially developed technologies and commercially unavailable tools,
b) The lock meets the requirements of security class C according to the standard².

1.2.2. Lock for security lockers – Type 3

SS₂= 3 points

- a) Lock providing high level of resistance against expert and professional penetration, using specially developed technologies and commercially unavailable tools,
b) Lock meeting the requirements of security class B according to the standard².

1.2.3. Lock for security lockers – Type 2

SS₂= 2 points

² STN P ENV 1300 and related standards, or the testing procedures of authorised persons, approved by the Authority.

- a) Lock providing a certain degree of resistance against a skilled violator equipped with a minimum of tools,
- b) Lock meeting the requirements of security class A according to the standard²).

1.2.4. Lock for security lockers – Type 1
--

SS₂= 1 point

- a) Lock providing resistance against unauthorised opening by a casual perpetrator,
- b) Type 1 locks may be used only with Type 1 security lockers.

2. MEASURES FOR SECURING PROTECTED AREAS

The decisive part in determining the resistance of a protected area's envelope is the part offering the least resistance.

The entry to a strong room or to a protected area designed for open storage of classified information must not be established in the part of the protected area's enclosure which simultaneously represents the enclosure of the building.

The resistance class of the locking systems of mechanical barrier devices used for securing protected areas is defined by the lowest resistance class of the locking systems used therein.

2.1. Protected area

Mechanical barrier devices shall be used for the securing of openings leading into the protected area, when their dimensions exceed those in the following table:

Shape of opening	Dimensions
Rectangular	400 mm x 250 mm
Ellipsoidal	400 mm x 300 mm
Circular	Diameter 350 mm

Ventilation openings, including those smaller than shown in the above table shall be ensured against unauthorised penetration by any solid materials.

Windows with bottom edges situated less than 5.5 m above the surrounding terrain, or those offering easy view from adjoining structures or from the uneven terrain shall be provided with screens or darkening means.

The part of the protected area's enclosure that is not simultaneously the enclosure of the building, and to which the conditions of points 2.1.1 through 2.1.4, indent b) do not apply may be equipped with a detection system, combined with the electric signalling device.

The door leading into the protected area shall be equipped with a device enabling emergency opening, and with an automatic closing device. The hinges of doors leading into the protected area shall be installed from the internal side or secured against unauthorised unhinging of the doors. The strength of the door frame and of its fastenings shall at least equal the door strength. Checkpoints shall be established at all entries to the protected area.

2.1.1. Protected area – Type 4

SS₃ = 4 points

- a) Protected area, providing a high degree of resistance against the violator who uses force and is equipped with efficient portable tools; the envelope of the protected area provides a high degree of resistance against clandestine penetration,
- b) The walls, floors and roofs of the protected area are of a particularly strong construction design, made from full bricks or blocks at least 300 mm thick, or from reinforced concrete

at least 150 mm thick, or from other construction materials with comparable properties in accordance with the standard³,

- c) The doors and closures, including grates and all components thereof in the category Top Secret shall meet minimally the requirements of resistance class 4 in accordance with the standard³),
- d) The windows and all components thereof, or grates in the category Top Secret shall meet minimally the requirements of resistance class 4 in accordance with the standard³,
- e) The locking systems of the mechanical barrier devices in the category Top Secret shall meet minimally the requirements of resistance class 4 in accordance with the standard³,
- f) The requirements specified in indent d) shall not be realised, when the bottom edge of the window or manhole is more than 5.5 m above the surrounding terrain and not easily accessible from the roof, lightning conductor, eaves or other structural elements, unevenness of the terrain, trees or other structures; this provision does not apply, when the protected area is designed for open placement of classified information,
- g) The protected area designed for open placement of classified information shall have minimum number of windows and other openings; all openings with any of their diameters exceeding 150 mm shall be secured with steel grates minimally of the category Secret, embedded in the walls and comprising at least 20 mm thick rods in 150 mm spacing.

2.1.2. Protected area – Type 3

SS₃ = 3 points

- a) Protected area providing a high degree of resistance against the violator equipped with portable tools; the envelope of the protected area provides a high degree of resistance against clandestine penetration,
- b) The walls, floors and roofs of the protected area are of a particularly strong construction design, made from full bricks or blocks at least 150 mm thick, or from reinforced concrete at least 100 mm thick, or from other construction materials with comparable properties in accordance with the standard³,
- c) The doors and closures, including grates and all components thereof in the category Secret shall meet minimally the requirements of resistance class 3 in accordance with the standard³,
- d) The windows and all components thereof, or grates in the category Secret shall meet minimally the requirements of resistance class 3 in accordance with the standard³,
- e) The locking systems of the mechanical barrier devices in the category Secret shall meet minimally the requirements of resistance class 3 in accordance with the standard³,
- f) The requirements specified in indent d) shall not be realised when the bottom edge of the window or opening is more than 5.5 m above the surrounding terrain and not easily accessible from the roof, lightning conductor, eaves or other structural elements, unevenness of the terrain, trees or other structures.

2.1.3. Protected area – Type 2

SS₃ = 2 points

³ STN P ENV 1627, STN P ENV 1628, STN P ENV 1629, STN P ENV 1630, STN EN 356 (70 0595), STN 74 7731, STN EN 1303 (16 5191), STN EN 1906 (16 5192), STN 16 5190, STN EN 5772, STN EN 12320 (16 6240), STN 96 7701, STN 96 7703 and related standards, or the testing procedures of authorised persons, approved by the Authority.

- a) Protected area providing a high degree of resistance against violent penetration using a limited range of manual tools; the envelope of the protected area provides a high degree of resistance against clandestine penetration,
- b) The walls, floors and roofs of the protected area are of a strong construction design, made from reinforced concrete at least 75 thick or from other construction materials with comparable properties in accordance with the standard³,
- c) The doors and closures, including grates and all components thereof in the category Confidential shall meet minimally the requirements of resistance class 2 in accordance with the standard³,
- d) The windows and all components thereof, or grates in the category Confidential shall meet minimally the requirements of resistance class 2 in accordance with the standard³; when this measure cannot be realised, the glazing must be protected with security foil at least in the Confidential category, certified by the Authority,
- e) The locking systems of the mechanical barrier devices in the category Confidential shall meet minimally the requirements of resistance class 2 in accordance with the standard³,
- f) The requirements specified in indent d) shall not be realised when the bottom edge of the window or opening is more than 5.5 m above the surrounding terrain and not easily accessible from the roof, lightning conductor, eaves or other structural elements, unevenness of the terrain, trees or other structures.

2.1.4. Protected area – Type 1	SS₃ = 1 point
---------------------------------------	---------------------------------

- a) The protected area may be locked and provides protection against physical violence and clandestine penetration,
- b) The walls, floors and roofs of the protected area are of lightweight construction (for example, from porous concrete, gypsum plasterboard, slip bricks, wood chipboards, hardened plastic materials, riffled or corrugated steel sheets or from other construction materials with comparable properties),
- c) The windows, doors and closures, including grating and all components thereof shall provide the same protection level against a violator as the remaining parts of the protected area's envelope,
- d) Any mechanical barrier devices, which may be opened, shall be equipped with locks,
- e) A lock system of the applicable category shall be used, when the protected area is designed for the storage of classified information at the security classification level Confidential and higher,
- f) Certified technical devices in the electric securing system protected at least as Type 2 according to Section 5.2.2 shall be used, when the protected area is designed for the storage of classified information at the security classification level Secret,
- g) The protected area shall not be used for the storage of classified information at the security classification level Top Secret.

2.2. Lock systems, designed for locking protected areas

2.2.1. Lock system – Type 4	SS₄ = 4 points
------------------------------------	----------------------------------

- a) The lock system provides high degree of resistance against expert and professional penetration using specially developed tools and technologies which are commercially unavailable,
- b) The lock system and its components in the Top Secret category shall meet minimally the requirements of resistance class 4 according to the standard³.

2.2.2. Lock system – Type 3**SS₄ = 3 points**

- a) The lock system provides high degree of resistance against expert and professional penetration using specially developed tools and technologies which are commercially available to a professional locksmith,
- b) The lock system and its components in the Secret category shall meet minimally the requirements of resistance class 3 according to the standard³.

2.2.3. Lock system – Type 2**SS₄ = 2 points**

- a) The lock system provides resistance against a skilled violator using a limited range of tools,
- b) The lock system and its components in the category Confidential shall meet minimally the requirements of resistance class 2 according to the standard³.

2.2.4. Lock system – Type 1**SS₄ = 1 point**

- a) The lock system is lockable and provides protection against physical violence and clandestine penetration,
- b) The specification of the lock system and of its components shall be shown in the security documentation of physical security and building security.

3. MEASURES FOR SECURING PROTECTED BUILDINGS

The decisive part determining the resistance of enclosure of the protected building is the part offering the least resistance. When the enclosure of the protected area is identical with the building's enclosure along the entire length, the provisions specified in Chapter 2 shall apply to the protection of the building, and its evaluation by points shall use only the points allocated to the protected area.

Evaluation of the building by points shall be determined by its level of protection to the height 5.5 m above the surrounding terrain.

Measures used to protect the building include mechanical protection systems - doors, windows, closures of entry openings, grates and their locking systems.

Checkpoints shall be established at all entries to the protected area.

3.1. Building – Type 4	S₃ = 5 points
-------------------------------	---------------------------------

- a) Building of massive construction, offering high level of resistance against violent penetration, corresponding to the resistance of concrete at least 150 mm thick and of full bricks at least 300 mm thick, or of other materials with comparable properties in accordance with the standard³,
- b) Mechanical barrier devices, offering the same level of resistance against violators as the remaining parts of the building enclosure.

3.2. Building – Type 3	S₃ = 3 points
-------------------------------	---------------------------------

- c) The building offers increased level of resistance against violent penetration, corresponding to the resistance of concrete at least 100 mm thick and of full bricks at least 150 mm thick or of other materials with comparable properties in accordance with the standard³,
- d) Mechanical barrier devices, offering the same level of resistance against violators as the remaining parts of the building enclosure.

3.3. Building – Type 2	S₃ = 2 points
-------------------------------	---------------------------------

- e) The building offers basic level of resistance against violent penetration, corresponding to the resistance of concrete at least 75 mm thick or of other materials with comparable properties in accordance with the standard³,
- f) Mechanical barrier devices, offering the same level of resistance against violators as the remaining parts of the building enclosure.

3.4. Building – Type 1	S₃ = 1 point
-------------------------------	--------------------------------

- a) The building offers minimal level of resistance against violent penetration, with external walls, floors and roofs of lightweight construction (for example from porous concrete, slip bricks, wood chipboards, hardened plastic materials, riffled or corrugated steel sheets or similar materials),

- b) Mechanical barrier devices, offering the same level of resistance against violators as the remaining parts of the building enclosure.

4. ENTRY CHECKS, RANDOM INSPECTIONS AND REGIME OF VISITS

4.1. Check of entries to protected areas or buildings

Entry checkpoints shall be established at all entries to the building or protected area. Checking is carried out by electronic, electro-mechanical or physical means, or in the form of a guard service or receptionist service. The entry check method shall be specified in the security documentation. Only one entry checkpoint shall be considered, when calculating the sum of evaluation points.

Entry checkpoints to a Secret or higher category protected area shall meet at least the conditions specified in Section 4.1.3. The rule of simultaneous entry of at least two persons should be applied in certain protected areas and specific cases.

Where entry is allowed on the basis of entry documents, the required ID shall show mainly the following:

- a) Serial number or other identifying number,
- b) Basic data of the holder (given name, family name, title) including his/her photograph,
- c) Identification of the certificate level and access level (e.g. by colour coding, etc.).

Permanent entry documents (identification elements) allowing unaccompanied access to the protected area may be issued to persons/

- a) Holding appropriate security clearances,
- b) Meeting access conditions on a need-to-know basis, while performing tasks or discharging duties.

Unless decided differently by the head, entry documents shall be carried continuously and visibly, so as to enable differentiation and identification. Loss of entry documents shall be reported as soon as possible to the appointed security employee of the organization to enable taking the necessary measures.

Cleaning and maintenance personnel should not be allowed unaccompanied entry to the protected area. Unaccompanied entry to Category II protected areas may be allowed to such personnel when it holds the appropriate security clearance, with prior arrangements realised to prevent visual or aural observation and clandestine interception, including when such personnel unknowingly enters the protected area.

4.1.1. Entry check system – Type 4	SS₆ = 4 points
---	----------------------------------

- a) Entry check corresponding to an automatic electric checkpoint system, requiring minimum supervision by physical protection,
- b) Electric entry clearance system of the Top Secret category, in combination with an unequivocally allocated personal identification number (PIN) or with a biometric

identification system, meeting the requirements of access class B and differentiation class 3 in accordance with the standard⁴,

- c) Output signal, terminating at a permanently manned security checkpoint,
- d) Entry clearance system, supplemented with an (area-wide) access barrier, physically preventing unauthorised entry; the barrier should prevent repeated access and provide for “one transaction - transit of a single person” regime.

4.1.2. Entry check system – Type 3

SS₆ = 3 points

- a) Entry check, corresponding to an electric checkpoint system, requiring direct supervision by physical protection,
- b) Electric entry clearance system of the Top Secret category, in combination with an unequivocally allocated personal identification number (PIN) or with a biometric identification system, meeting the requirements of access class B and differentiation class 3 in accordance with the standard⁴,
- c) Entry clearance system, supplemented with an appropriate barrier, supervised by a person executing physical protection.

4.1.3. Entry check system – Type 2

SS₆ = 2 points

- a) Entry check, based on authorisation to enter by unequivocally identifying entry documents with a photograph, realised through the person executing physical protection,
or
- b) Electric entry clearance system of the Secret category, meeting the requirements of access class B and differentiation class 2 in accordance with the standard⁴,
or
- c) Entry check carried out from behind a lockable door by permanent supervising personnel, using a camera system or video door opener.

4.1.4. Entry check system – Type 1

SS₆ = 1 point

- a) Entry check system, consisting of a lockable door enabling access with an assigned key, code setting or by other access systems allocated to the designated persons,
- b) This entry check system may be used only for protected areas in the Confidential or lower category.

4.2. Random inspections

4.2.1. Random inspections - realised

SS₁₂ = 1 point

The organisation carries out random incoming and outgoing inspections, serving as a deterrent element against unauthorised handling of classified information.

4.2.2. Random inspections - not realised

SS₁₂ = 0 points

⁴ STN EN 50133-1, STN EN 50133-2-1, STN EN 50133-7 and related standards, or the testing procedures of authorised persons, approved by the Authority.

4.3. Visitor regime

4.3.1. Visitors accompanied

SS₇ = 1 point

- a) Visitors are accompanied all the time while in the building or in the protected area,
- b) Visitors visiting several protected areas in the building shall be handed over to the next accompanying person, including accompanying documentation (gate passes, etc.),
- c) Records of visits must be kept in logbooks, showing identification data (given name, family name, title, ID, service ID or travel document number) of the visits, and time data of visits; detailed rules shall be determined in the security documentation.

4.3.2. Visitors unaccompanied

SS₇ = 0 points

- a) Unaccompanied visitors may enter Category “R” buildings, providing that they do not enter a protected area,
- b) Unaccompanied visitors may enter Category “C” and higher category buildings only when they are security clearance holders at the appropriate level, providing that they do not enter a protected area,
- c) Visitors must wear visible tags while staying in the building or in the protected area,
- d) Records of visit data must be kept in logbooks (given name, family name, title, ID, service ID or travel document number); detailed rules shall be determined in the security documentation.

5. PHYSICAL PROTECTION AND ELECTRIC SECURING SYSTEMS

5.1. Physical protection

5.1.1. Physical protection – Type 5

SS₈ = 5 points

- a) Physical protection is carried out by members of armed security corps,
- b) Persons carrying out physical protection make rounds inside the building,
- c) During the rounds or during an intervention the permanent physical protection post must remain manned by at least one employee on physical protection duty.

5.1.2. Physical protection – Type 4

SS₈ = 4 points

- a) Physical protection is carried out by members of armed forces or by armed personnel permanently on duty,
- b) Persons carrying out physical protection shall make rounds inside the building,
- c) During the rounds or during an intervention the permanent physical protection post must remain manned by at least one employee on physical protection duty.

5.1.3. Physical protection – Type 3

SS₈ = 3 points

- a) Physical protection is carried out by members of armed forces, armed security corps or by armed personnel permanently on duty, employees of private security services or trained employees of the building operator, or appointed own employees,
- b) Persons carrying out physical protection make rounds outside of the building,
- c) The interval of rounds depends on the internal operating conditions of the building and on the estimated rate of risk,
- d) During the rounds or during an intervention the permanent physical protection post must remain manned by at least one employee on physical protection duty.

5.1.4. Physical protection – Type 2

SS₈ = 2 points

- a) Physical protection requires no rounds to be made since it is carried out by local protection using own employees permanently on duty,
- b) When required, the persons carrying out physical protection shall summon assistance, for example members of armed personnel, employees of private security services or trained employees of the building operator.

5.1.5. Physical protection – Type 1

SS₈ = 1 point

Physical protection is carried out by checking the envelope of the building mainly after office hours, and corresponds to the building protection by an electric securing system with its output signal terminating at a permanently manned physical protection post.

5.2. Electric securing systems

5.2.1. Technical level of ESS devices

The technical level of ESS devices is defined by the lowest category of technical devices, used in the ESS.

5.2.1.1. Technical level of ESS devices - Type 4

SS₉₁ = 4 points

ESS elements in the category Top Secret, meeting level-4 security requirements „High risk“ in accordance with the standard⁵.

5.2.1.2. Technical level of ESS devices - Type 3

SS₉₁ = 3 points

ESS elements in the category Secret, meeting level-3 security requirements „Medium to high risk“ in accordance with the standard⁵.

5.2.1.3. Technical level of ESS devices - Type 2

SS₉₁ = 2 points

ESS elements in the category Confidential, meeting level-2 security requirements „Low to medium risk“ in accordance with the standard⁵.

5.2.1.4. Technical level of ESS devices - Type 1

SS₉₁ = 1 point

ESS elements meeting level-1 security requirements „Low risk“ in accordance with the standard⁵.

5.2.2. Method of protection using ESS devices

Camera arrays operating in a closed-circuit television system used for securing a building or protected area (further referred to as “camera array”) must meet the requirements of the standard⁶. The output signal of the camera array shall terminate at a permanently manned physical protection post, and shall be recorded and archived.

The following camera array components are subject to certification:

- a) Cameras,
- b) Control units,
- c) Output units (monitors).

The camera array monitoring entry into the protected area serves as a supporting measure.

ESS installed in a protected area must be controllable independently on the control system in other protected areas or in other premises. The ESS output alarm signal shall terminate at a permanently manned physical protection post. The persons on physical protection duty shall have means available for summoning the rapid response unit with a

⁵ STN EN 50131-1, STN EN 50131-1 Amendment Z1, STN EN 50131-6, STN 33 4590-1, STN 33 4590-2, STN 33 4590-3, STN 33 4590-4, STN 33 4590-5, STN 33 4590-6, STN 33 4590-7, STN 33 4590-8 and related standards, or the testing procedures of authorised persons, approved by the Authority.

⁶ STN EN 50132-2-1, STN EN 50132-4-1, STN EN 50132-5, STN EN 50132-7 and related standards, or the testing procedures of authorised persons, approved by the Authority.

recommended maximum response time of 5 minutes. The response time of the rapid response unit shall be verified at least once in a year.

5.2.2.1. ESS - Type 4

SS₉₂ = 4 points

- a) The ESS ensures perimeter protection and full enclosure protection of the protected area,
- b) Distress system meeting the requirements specified in Section 5.2.3.,
- c) Provides protection of security lockers,
- d) Camera array monitoring the entry into the protected area installed,
- e) The ESS and camera array alarm output signals shall terminate at a permanently manned physical protection post; both systems must be mutually functionally independent.

5.2.2.2. ESS - Type 3

SS₉₂ = 3 points

- a) The ESS ensures perimeter protection and full enclosure protection of the protected area,
- b) Distress system meeting the requirements specified in Section 5.2.3.,
- c) When there is a camera array installed in the protected area, an ESS for ensuring full enclosure protection of the protected area is not required; the ESS and the camera array must be mutually functionally independent.

5.2.2.3. ESS - Type 2

SS₉₂ = 2 points

- a) The ESS ensures perimeter protection of the protected area, and enclosure protection of the protected area realised in the form of securing windows, doors and closures of openings to the protected area,
- b) Perimeter protection or enclosure protection referred to in indent a) is not required, when the bottom edge of the window or opening is higher than 5.5 m above the surrounding terrain and is not easily accessible from the roof, lightning conductor, eaves or other structural elements, unevenness of the terrain, trees or other structures, and when the building is adequately secured.

5.2.2.4. ESS - Type 1

SS₉₂ = 1 point

- a) The ESS ensures perimeter protection of the protected area,
- b) The ESS alarm output signals shall terminate at a permanently manned physical protection post, or use an acoustic alarm device, enabling signal detection from publicly accessible points.

5.2.3. Distress system

5.2.3. Distress system

No evaluation with points

The distress systems shall meet the requirements of the standard⁷. Distress systems need not be installed in protected areas simultaneously used as permanently manned physical protection posts.

⁷ STN EN 50134-1 and related standards, or the testing procedures of authorised persons, approved by the Authority.

6. EXTERNAL PROTECTION MEASURES

External protection of a building is carried out in the form of a comprehensive system of measures protecting the envelope of the building, its entries, fire escapes and closures of openings. Individual mechanical barrier devices and technical protection devices may be disabled during office hours, providing acceptance of measures preventing threat to the protection of classified information.

6.1. Barriers

Barriers along the entire building envelope are designed to prevent unchallenged access to the building.

6.1.1. Barrier - Type 4	SS₁₀ = 4 points
--------------------------------	-----------------------------------

- a) The height of the barrier is at least 2 150 mm,
- b) The barrier top ends in two-sided oblique struts protruding at least 400 mm toward both sides under a 45° angle, and is supplemented along the full length with steel-barbed wire,
- c) The barrier is supplemented with ground plates preventing burrowing, or with steel grids,
- d) The barrier is supplemented with a perimeter detection system and with a camera array operated in a closed-circuit television system,
- e) A 25 m wide free zone must be left around the building, maintained in clean conditions and without artificial obstacles.

6.1.2. Barrier – Type 3	SS₁₀ = 3 points
--------------------------------	-----------------------------------

- a) The height of the barrier is at least 2 150 mm, its top and bottom parts must be provided with means preventing climbing over or crawling under the barrier,
- b) A free zone must be left around the building, maintained in clean conditions and without artificial obstacles,
- c) The barrier is supplemented with a perimeter detection system and with a camera array operated in a closed-circuit television system.

6.1.3. Barrier – Type 2	SS₁₀ = 2 points
--------------------------------	-----------------------------------

- a) The height of the barrier is at least 1 800 mm, it must represent an obstacle against attempted climbing over, and against penetration by breakage,
- b) A free zone must be left around the building, maintained in clean conditions and without artificial obstacles.

6.1.4. Barrier – Type 1	SS₁₀ = 1 point
--------------------------------	----------------------------------

The barrier must designate the boundaries of the building.

6.2. Entry checks at barrier entries

6.2.1. Entry check realised at all entries**SS₁₁ = 1 point**

The entry check at barrier entries shall be realised in accordance with Section 4.1. The entry check method must be recorded in the security documentation of physical security and building security.

6.2.2. Entry check not realised at all entries**SS₁₁ = 0 points****6.3. Building perimeter detection system**

The building perimeter detection system is used to increase the external protection level; it may be concealed, or installed visibly as a deterrent element.

6.3.1. Building perimeter detection system realised**SS₁₃ = 1 point**

The output signal of the building perimeter detection system shall terminate at the permanently manned physical protection post. Since a building perimeter detection system is prone to false alarm conditions, it is recommended to supplement it with another control system, e.g. with a camera array operated in a closed-circuit television system, the evaluation points of which shall be separately calculated.

6.3.2. Building perimeter detection system not realised**SS₁₃ = 0 points****6.4. Security lighting****6.4.1. Security lighting realised****SS₁₄ = 1 point**

Security lighting is installed in support of external protection, as a deterrent against potential violators.

6.4.2. Security lighting not realised**SS₁₄ = 0 points****6.5. Camera array****6.5.1. Camera array realised****SS₁₅ = 1 point**

The camera array operated in a closed-circuit television system must meet the conditions of Section 5.2.2. Certification of the camera array operated in a closed-circuit television system is not required, when it is used for external protection of the building's perimeter, and the perimeter is not identical with the envelope of the protected area.

6.5.2. Camera array not realised**SS₁₅ = 0 points**

7. DEVICES FOR DETECTING SUBSTANCES AND THINGS

- a) Devices for detecting substances and things used to detect metals shall be installed at the entry of the building or of the protected area; they shall provide for differentiation of metallic objects, and for detecting those metallic objects which must not be brought into the protected area,
- b) Metal detectors shall be installed in a way enabling direct supervision or direct servicing thereof by persons carrying out physical protection,
- c) Metal detectors shall meet the conditions of testing procedures by authorised persons, approved by the Authority.

8. DEVICES FOR PHYSICAL DESTRUCTION OF INFORMATION CARRIERS

Physical destruction of magnetic information carriers, e.g. floppy disks, compact disks, magnetic tapes, memory storage chips and hard disks shall be carried out with use of certified devices, exclusively designated for destruction of such data carriers by their manufacturers.

8.1. Device for physical destruction of information carriers – Type 4	No evaluation with points
--	----------------------------------

- a) Device for physical destruction of information carriers, designed for destroying carriers of classified information at all security classification levels,
- b) Device for physical destruction of information carriers of the Top Secret category, meeting the requirements of security degree 5 in accordance with the standard⁸,
- c) Device for physical destruction of information carriers, designated to destroy carriers of classified information submitted to the Slovak Republic by a foreign power, at all security classification levels.

8.2. Device for physical destruction of information carriers – Type 3	No evaluation with points
--	----------------------------------

- a) Device for physical destruction of information carriers, designed for destroying carriers of classified information at the security classification level Secret or lower,
- b) Device for physical destruction of information carriers of the Secret category, meeting the requirements of security degree 4 in accordance with the standard⁸,
- c) The device for physical destruction of information carriers of the category Secret may be used to destroy magnetic information carriers, e.g. floppy disks, compact disks and similar mediums in the TS category,
- d) The device for physical destruction of information carriers may be used to destroy carriers of classified information submitted to the Slovak Republic by a foreign power, at all security classification levels.

8.3. Device for physical destruction of information carriers – Type 2	No evaluation with points
--	----------------------------------

- a) Device for physical destruction of information carriers, designed for destroying carriers of classified information at the security classification level Confidential or lower,
- b) Device for physical destruction of information carriers of the Confidential category, meeting the requirements of security degree 3 in accordance with the standard⁸,
- c) The device for physical destruction of information carriers must not be used to destroy carriers of classified information, submitted to the Slovak Republic by a foreign power.

⁸ STN 369510-1 and related standards or the testing procedures of authorised persons, approved by the Authority.

8.4. Device for physical destruction of information carriers – Type 1**No evaluation
with points**

- a) Device for physical destruction of information carriers, designed for destroying carriers of classified information at the security classification level Restricted,
- b) Device for physical destruction of information carriers of the Restricted category, meeting the requirements of security degree 2 in accordance with the standard⁸,
- c) The device for physical destruction of information carriers must not be used to destroy carriers of classified information submitted to the Slovak Republic by a foreign power.

9. PROTECTION OF CONFERENCE ROOMS AGAINST INTERCEPTION OF CLASSIFIED INFORMATION

Passive interception of classified information means leakage of classified information by direct eavesdropping and direct observation, accomplished through the envelope of the conference room or through technical openings established therein. Active interception of classified information means leakage of classified information by way of implanted devices.

The conference room used to regularly discuss classified information must be furnished with a minimum of furniture and equipment, which must be recorded (including their type and serial or inventory numbers). Any technical and communications equipment (telephone, fax, television sets, wireless sets, video recorders, computers, monitors, etc.) not inevitably needed in the course of work with classified information must be excluded from the conference room. The equipment inevitably needed in the course of work shall be subjected to measures in order to prevent unauthorised handling thereof. When not used, the conference rooms shall be locked and controlled.

9.1. Regime measures

Regime measures shall be established, determining the method and conditions of entry and movement of persons, as well as the purpose of their presence in the conference room, the method of checking and identifying persons entering the room, and the method of recording and archiving the aforesaid data. These measures are designed to ensure that only authorised persons would, without being accompanied, enter the conference room. All other persons, including cleaning and maintenance personnel shall be accompanied at all times while staying in the conference room.

9.2. Technical security inspections

Technical security inspections are designed to verify, whether or not there are interception devices implanted in the room and/or in its furnishings and equipment. Technical security inspections shall be carried out in regular intervals, as well as after all reconstructions of the room. Technical security inspections shall be carried out by legal entities who are holders of industrial security certificates⁹, or by specialised units of state authorities. The persons carrying out the technical security inspections shall be adequately cleared. The course of the technical security inspection shall be described in a report, comprising the results of measurements and the result (evaluation) of the technical security inspection; the report shall be attached to the security documentation of physical security and building security.

9.3. Mechanical barrier devices and technical protection devices

Mechanical barrier devices and technical protection devices are used to secure the windows, doors, outlets of openings used for airconditioning, heating, ventilation and other purposes that enable interception. The rooms shall be equipped mainly with an acoustic noise generator, piezoelectric transducers installed on windows, etc.

All cables entering the conference room shall be secured by marking all wire pairs, both used and unused. Unused pairs shall be earthed in a way excluding unauthorised use.

⁹ Article 50 of Act No. 215/2004 Coll.

10. PHYSICAL SECURITY AND BUILDING SECURITY OF BUILDINGS AND PROTECTED AREAS HOLDING TECHNICAL DEVICES AND CRYPTOGRAPHIC DEVICES AND SYSTEMS OF PROTECTING INFORMATION

The area holding control elements of communications and information systems of technical devices¹⁰ (servers, control elements of computer networks, communications control elements) and distribution elements of cryptographic systems of protecting information pursuant to separate legislation¹¹ (centre of records, handling and distribution of cipher materials) shall be/

- a) Designated Class 1 protected area pursuant to Article 3, paragraph 4,
- b) Checked after office hours by an appointed employee,
- c) Equipped with electric fire signalling devices, electric securing system, entry check system, air temperature and humidity measuring instruments, backup power source and flooding detectors.
- d) All code settings of the mechanical protecting devices and technical protection devices shall be changed at least once in 6 months.

When the stored information is encrypted, and when user identification and authentication is provided for, the aforesaid measures shall be considered equivalent to the security locker together with the lock of security locker.

The areas designed for installing technical devices and cryptographic devices and systems of protecting information shall be protected against leakage of classified information by electromagnetic radiation pursuant to separate legislation¹².

¹⁰ Article 2, indent i) of Act No. 215/2004 Coll.

¹¹ National Security Authority Regulation No. 340/2004 Coll., regulating the particulars of cipher protection of information.

¹² Article 70, paragraph 1, subparagraph c), point 15 of Act No. 215/2004 Coll.

11. EVALUATION OF PHYSICAL SECURITY AND BUILDING SECURITY ELEMENTS IN POINTS

11.1. Storage of classified information

Security lockers (see 1.1.)

Classification of security lockers	Evaluation in points - SS ₂	Security standards
Type 4	4 points	See 1.1.1.
Type 3	3 points	See 1.1.2.
Type 2	2 points	See 1.1.3.
Type 1	1 point	See 1.1.4.

Locks of security lockers (see 1.2.)

Classification of locks of security lockers	Evaluation in points - SS ₂	Security standards
Type 4	4 points	See 1.2.1.
Type 3	3 points	See 1.2.2.
Type 2	2 points	See 1.2.3.
Type 1	1 point	See 1.2.4.

Summary evaluation of the security locker and its lock:

$$S_1 = SS_1 \times SS_2$$

11.2. Protected area securing measures

Protected area (see 2.1.)

Classification of the protected area	Evaluation in points - SS ₃	Security standards
Type 4	4 points	See 2.1.1.
Type 3	3 points	See 2.1.2.
Type 2	2 points	See 2.1.3.
Type 1	1 point	See 2.1.4.

Lock systems designed to lock protected areas (See 2.2.)

Classification of lock systems	Evaluation in points - SS ₄	Security standards
Type 4	4 points	See 2.2.1.
Type 3	3 points	See 2.2.2.
Type 2	2 points	See 2.2.3.
Type 1	1 point	See 2.2.4.

Summary evaluation of securing protected areas: $S_2 = SS_3 + SS_4$

11.3. Building securing measures

Buildings (see Chapter 3)

Building classification	Evaluation in points - S_3	Security standards
Type 4	5 points	See 3.1.
Type 3	3 points	See 3.2.
Type 2	2 points	See 3.3.
Type 1	1 point	See 3.4.

Summary evaluation of the building: $S_3 = 5, 3, 2, \text{ or } 1$

11.4. Entry checks and regime of visits

Entry checks in protected areas or buildings (See 4.1.)

Classification of the security of entry of buildings and protected areas	Evaluation in points - SS_6	Security standards
Type 4	4 points	See 4.1.1.
Type 3	3 points	See 4.1.2.
Type 2	2 points	See 4.1.3.
Type 1	1 point	See 4.1.4.

Regime of visits in buildings (See 4.3.)

Classification of the regime of visits	Evaluation in points - SS_7	Security standards
Visitors accompanied	1 point	See 4.3.1.
Visitors unaccompanied	0 points	See 4.3.2.

Summary evaluation of entry checks and regime of visit:

$$S_4 = SS_6 + SS_7$$

11.5. Physical protection and electric securing systems

Physical protection (See 5.1.)

Classification of physical protection	Evaluation in points - SS_8	Security standards
Type 5	5 points	See 5.1.1.

Type 4	4 points	See 5.1.2.
Type 3	3 points	See 5.1.3.
Type 2	2 points	See 5.1.4.
Type 1	1 point	See 5.1.5.

Electric securing systems (See 5.2.)

Technical level of ESS devices (See 5.2.1.)

Classification of technical level of ESS devices	Evaluation in points - SS ₉₁	Security standards
Type 4	4 points	See 5.2.1.1.
Type 3	3 points	See 5.2.1.2.
Type 2	2 points	See 5.2.1.3.
Type 1	1 point	See 5.2.1.4.

Method of protection, using ESS devices (See 5.2.2.)

Classification of the method of protection, using ESS devices	Evaluation in points - SS ₉₂	Security standards
Type 4	4 points	See 5.2.2.1.
Type 3	3 points	See 5.2.2.2.
Type 2	2 points	See 5.2.2.3.
Type 1	1 point	See 5.2.2.4.

$$SS_9 = (SS_{91} + SS_{92}) \times K/2,$$

where K is a coefficient of installation, determined as follows:

$$K = SS_{92} / \text{CHP},$$

where CHP is the value in points, given by the category of the protected area as follows:

Category of the protected area	CHP value in points
„Top Secret“	4 points
„Secret“	3 points
„Confidential“	2 points
„Restricted“	1 point

The interim result (SS₉) shall be rounded up to the next integer number. SS₉ may assume the highest value of 4 points.

Summary evaluation of physical protection and of the electric securing system:

$$S_5 = SS_8 + SS_9$$

11.6. External protection measures

Barriers (See 6.1.)

Classification of the barrier	Evaluation in points - SS ₁₀	Security standards
Type 4	4 points	See 6.1.1.
Type 3	3 points	See 6.1.2.
Type 2	2 points	See 6.1.3.
Type 1	1 point	See 6.1.4.

Entry check at the barrier access points (See 6.2.)

Classification of entry check at the barrier access points	Evaluation in points - SS ₁₁	Security standards
Realised	1 point	See 6.2.1.
Not realised	0 points	See 6.2.2.

Random incoming and outgoing inspections (See 4.2.)

Classification of random inspections	Evaluation in points - SS ₁₂	Security standards
Realised	1 point	See 4.2.1.
Not realised	0 points	See 4.2.2.

Building perimeter detection system (See 6.3.)

Classification of the building perimeter detection system	Evaluation in points - SS ₁₃	Security standards
Realised	1 point	See 6.3.1.
Not realised	0 points	See 6.3.2.

Security lighting (See 6.4.)

Classification of the security lighting	Evaluation in points - SS ₁₄	Security standards
Realised	1 point	See 6.4.1.
Not realised	0 points	See 6.4.2.

Camera array (See 6.5.)

Classification of the camera array	Evaluation in points - SS ₁₅	Security standards
Realised	1 point	See 6.5.1.
Not realised	0 points	See 6.5.2.

Summary evaluation of the external protection measures:

$$S_6 = (SS_{10} \times SS_{11}) + SS_{15}$$

$$S_7 = SS_{12} + SS_{13} + SS_{14}$$

12. MINIMUM REQUIRED VALUES IN THE EVALUATION OF PHYSICAL SECURITY AND BUILDING SECURITY

12.1. Minimum required values in the evaluation of physical security and building security of areas designed for storage of classified information

Area designed for storage of classified information of the „TS“ category	Rate of risk		
	Low	Medium	High
Obligatory: (S1) + (S2) + (S3)	10	11	13
Obligatory: (S4) + (S5) *	6	7	7
Obligatory: (S6) **	2	2	2
Non-obligatory: (S7 and increase of measures S1 - S6)	4	5	5
Total result	22	25	27

Area designed for storage of classified information of the „S“ category	Rate of risk		
	Low	Medium	High
Obligatory: (S1) + (S2) + (S3)	8	9	10
Obligatory: (S4) + (S5) ***	4	5	5
Obligatory: (S6) **	2	2	2
Non-obligatory: (S7 and increase of measures S1 - S6)	4	5	5
Total result	18	21	22

Area designed for storage of classified information of the „C“ category	Rate of risk		
	Low	Medium	High
Obligatory: (S1) + (S2) + (S3)	7	9	10
Obligatory: (S4) + (S5)	3	4	4
Non-obligatory: (S6 + S7 and increase of measures S1 - S5)	3	3	4
Total result	13	16	18

Area designed for storage of classified information of the „R category	Rate of risk		
	Low	Medium	High
Obligatory: (S1) + (S2) + (S3)	3	3	3
Non-obligatory: (S4 + S5 + S6 + S7 and increase of measures S1 - S3)	0	1	2
Total result	3	4	5

Notes:

- * S5 must reach at least 5 points,
- ** When a barrier pursuant to Section 6.1 could not be erected and the values $SS_{10} = 0$ points and $SS_{15} = 1$ point, the required point value of S6 may be reached by increasing the level of non-obligatory measures by 1 point,
- *** S5 must reach at least 4 points,
- Only one of the values S1, S2 or S3 may equal to zero,
- The “Low” rate of risk shall be applied to protected areas designed for short-term storage of classified information

12.2. Minimum required point values in the evaluation of physical security and building security of areas designed for storage of classified information submitted to the Slovak Republic by a foreign power

Security measures	Evaluation points of measures for the individual security classification levels		
	“TS”	“S”	“C”
Obligatory value S1	16	9	6
Obligatory value S2	7	6	4
Obligatory: (S1) + (S2) + (S3)	24	16	11
Obligatory value S4	4	3	2
Obligatory value SS91	4	3	2
Obligatory value S5	7	5	45
Obligatory: (S4) + (S5)	11	8	7
Obligatory value S6	2	2	-
Non-obligatory: (S7 and increase of measures S1 - S6)	3	3	4*
Total result	40	29	22

Note:

* Non-obligatory (S6 + S7 and increase of measures S1 - S5).

12.3. Minimum required point values in the evaluation of physical security and building security of protected areas designed for handling of classified information and for their storage in technical devices

Protected area of the „TS“ category	Rate of risk		
	Low	Medium	High
Obligatory: (S2) + (S3)	6	6	7
Obligatory: (S4) + (S5) *	6	7	7
Non-obligatory: (S6 + S7 and increase of measures S2 - S5)	4	5	5
Total result	16	18	19

Protected area of the „S“ category	Rate of risk		
	Low	Medium	High
Obligatory: (S2) + (S3)	5	5	6
Obligatory: (S4) + (S5) **	4	5	5
Non-obligatory: (S6 + S7 and increase of measures S2 - S5)	4	5	5
Total result	13	15	16

Protected area of the „C“ category	Rate of risk		
	Low	Medium	High
Obligatory: (S2) + (S3)	4	4	5
Obligatory: (S4) + (S5)	2	3	3
Non-obligatory: (S6 + S7 and increase of measures S2 - S5)	3	4	4
Total result	9	11	12

Protected area of the „R“ category	Rate of risk		
	Low	Medium	High
Obligatory: (S2) + (S3)	3	3	3
Non-obligatory: (S4 + S5 + S6 + S7 and increase of measures S2 and S3)	0	1	2
Total result	3	4	5

Notes:

* S5 must reach at least 5 points,

** S5 must reach at least 4 points,

- The value of S3 must not be a zero,

- The “High” rate of risk shall be applied to protected areas designed for generating, displaying, transferring in technical devices and recording classified information at the security classification levels Secret and Top Secret, submitted to the Slovak Republic by a foreign power.

13. TABLE OF EVALUATION OF SECURITY MEASURES BY POINTS IN THE PROTECTED AREA

Complete the Table by evaluating the individual specific security measures in points in accordance with their descriptions in Chapters 1 through 11 of the security standard. When the individual measures are not evaluated by points, show them separately in an annex to the Table. Complete a separate Table for each protected area.

The headline of the Table must show the following data:

- Designation of the protected area,
- Category and class of the protected area,
- Purpose of use of the protected area (storage, conference room, etc.).

SECURITY MEASURE	TYPE	EVALUATION IN POINTS
Security lockers (See 1.1.)	T. 4 – 4 points T. 3 – 3 points T. 2 – 2 points T. 1 – 1 point	SS1 =
Locks of security lockers (See 1.2.)	T. 4 – 4 points T. 3 – 3 points T. 2 – 2 points T. 1 – 1 point	SS2 =
Total evaluation of the security locker and its lock (See 11.1.)	S1 = SS1 x SS2	S1 =
Protected area (See 2.1.)	T. 4 – 4 points T. 3 – 3 points T. 2 – 2 points T. 1 – 1 point	SS3 =
Lock systems, designed to lock protected areas (See 2.2.)	T. 4 – 4 points T. 3 – 3 points T. 2 – 2 points T. 1 – 1 point	SS4 =
Total evaluation of securing the protected area (See 11.2.)	S2 = SS3 + SS4	S2 =
Building (See Chapter 3.)	T. 4 – 5 points T. 3 – 3 points T. 2 – 2 points T. 1 – 1 point	S3 =
Obligatory (S1) + (S2) + (S3)	(S1) + (S2) + (S3)	
Entry checks (See 4.1.)	T. 4 – 4 points T. 3 – 3 points T. 2 – 2 points T. 1 – 1 point	SS6 =
Regime of visits in the building (See 4.3.) a) Accompanied visitors b) Unaccompanied visitors	ad a) – 1 point ad b) – 0 points	SS7 =
Total evaluation of entry checks and regime of visits (See 11.4.)	S4 = SS6 + SS7	S4 =
Physical protection (See 5.1.)	T. 5 – 5 points	SS8 =

	T. 4 – 4 points T. 3 – 3 points T. 2 – 2 points T. 1 – 1 point	
Technical level of ESS devices (See 5.2.1.)	T. 4 – 4 points T. 3 – 3 points T. 2 – 2 points T. 1 – 1 point	SS91 =
Method of protection, using ESS devices (See 5.2.2.)	T. 4 – 4 points T. 3 – 3 points T. 2 – 2 points T. 1 – 1 point	SS92 =
Interim result (SS 9) - calculation (see 11.5.)		SS9 =
Total evaluation of physical protection and of ESS (See 11.5.)	S5 = SS8 + SS9	S5 =
Obligatory (S4) + (S5)	(S4) + (S5)	
Barriers (See 6.1.)	S. 4 – 4 points S. 3 – 3 points S. 2 – 2 points S. 1 – 1 point	SS10 =
Entry checks at barrier entries (See 6.2.) a) Checks realised b) Checks not realised	ad a) – 1 point ad b) – 0 points	SS11 =
Random incoming and outgoing inspections (See 4.2.) a) Inspections realised b) Inspections not realised	ad a) – 1 point ad b) – 0 points	SS12 =
Detection system of building envelopes (See 6.3.) a) Realised b) Not realised	ad a) – 2 points ad c) – 0 points	SS13 =
Security lighting (See 6.4.) a) Security lighting realised b) Security lighting not realised	ad a) – 2 points ad b) – 0 points	SS14 =
Camera array (See 6.5.) a) Realised b) Not realised	ad a) – 2 points ad b) – 0 points	SS15 =
Total evaluation of external protection measures (See 11.6)	S6 = (SS10 x SS11) + + SS15	S6 =
Total evaluation of external protection measures (See 11.6)	S7 = SS12 + SS13 + SS14	S7 =

The values of variables S1 through S7, obtained by completing the Table of evaluation of security measures by points in the protected area, shall be compared with the Table of minimum values in accordance with Chapter 12. Determine, based on this comparison, whether or not the accepted security measures are sufficient for the given rate of risk and the protected area category.