

339

REGULATION Of the National Security Authority

Of 10 May 2004

On the Security of Technical Devices

The National Security Authority (hereinafter referred to as “Authority”) stipulates, pursuant to Article 6 paragraph 10, Article 55 paragraph 9, Article 56 paragraph 7 and Article 58 paragraph 4 of Act No.215/2004 (Coll.) on the protection of classified information and on the amending and supplementing of certain laws (hereinafter referred to as “Act”), the following:

Article 1 Subject of Regulation

This regulations governs all details related to the security of technical devices, approval of technical devices into operation, their use and details related to the requirements placed on the technical devices on which classified information are created, processed, transferred, filed and archived, details about the procedure used in the certification of technical devices, as well as all details about the development of security projects for technical devices and about the issue and use of security standards.

Article 2 Security of Technical Devices

(1) Technical devices shall be secured pursuant to special regulations¹⁾ in such a way that this security corresponds to the level of security classification, for which technical devices are approved into operation.

(2) A managing person²⁾ shall, pursuant to paragraph 1, be responsible for the security of technical devices, which work with classified information.

(3) The technical devices determined for the creation, processing, transfer, filing and protection of classified information of the levels of security classification “Restricted” must provide at least for a clear identification of the user.

¹⁾ Regulation of the National Security Authority No. 331/2004 (Coll.) on personnel safety and the vetting of security employee.

Regulation of the National Security Authority No. 336/2004 (Coll.) on physical and building security,

Regulation of the National Security Authority No. 338/2004 (Coll.) on administrative security.

Regulation of the National Security Authority No. 340/2004 (Coll.) laying down details on cipher protection of information.

²⁾ Article 8 of Act No. 215/2004 (Coll.) on the protection of classified information and on the amending and supplementing of certain laws.

(4) The technical devices determined for the creation, processing, transfer, filing and protection of classified information of the levels of security classification “Top Secret”, “Secret” or “Confidential” must provide, as a minimum, for the following security functions:

- a) Clear identification and authentication of the user that precedes all of the other user’s activities upon the processing of classified information on the technical device;
- b) Alternative control of the access to objects (file, directory, peripheral device, service, etc.) on the basis of differentiation and administration of the user’s access rights, his identity or membership in a group of users;
- c) Continuous keeping of a control record by a technical device about its activity, with the possibility of monitoring, backward examination of the technical device, as well as the determination of the responsibility of a specific user for the activities performed by him; a person authorized with the execution of IS security administration (hereinafter referred to as “security administrator”) shall regularly check this record in intervals specified in the directive about the use of the technical device pursuant to Article 4;
- d) Removal of classified information, which are not necessary for further processing, archiving or manipulation (operating memory, temporary files and work files) from storage mediums after the completion of work with a technical device, so as to prevent any detection of their previous content or make it very difficult even if using special laboratory means and methods; it is necessary to carry out this removal always before the allocation of these devices to another subject;
- e) Protection of the confidentiality of data during its transfer in a network must be ensured in such a way as to protect classified material in the process of its transfer between the source and final destination, pursuant to a special regulation³).

(5) Technical devices used by state body upon the fulfilment of duties pursuant a special regulation,⁴) determined for the creation, processing, transfer, filing, protection and archiving of classified information of the level of security classification “Confidential” must ensure the security functions pursuant to paragraph 4 letter a), b), d) and e).

(6) The level of security classification of a carrier of classified information marked with the level of security classification “Confidential” or the level of security classification “Restricted” may only be decreased, if the removal of information representing the classified information was carried out in such a way that their recovery is not possible or is very difficult even if special laboratory means and methods are used.

(7) The level of security classification of a carrier of classified information marked with the level of security classification “Secret” or the level of security classification “Top Secret” cannot be decreased.

(8) Non-usable carriers of classified information shall be physically destroyed or by special software or hardware means, specifically in a commissional way, so that no information may be recovered from them by any means.

³) Regulation of the National Security Authority No. 340./2004 (Coll.).

⁴) Act of the National Council of the Slovak Republic No. 46/1993 (Coll.) on the Slovak Information Service, as amended by later regulations.

(9) Technical devices shall be secured against unfavourable electromagnetic radiation that could result in the revealing of classified information pursuant to security standard for the protection against unfavourable electromagnetic radiation.

(10) If the cost necessary for the provision of any security function of a technical device is unreasonable, a replacement may be carried out through the means or measures pursuant to special regulations¹⁾ or their appropriate combination, provided that the required level of security classification is maintained.

(11) Portable technical devices, such as notebook, laptop), mobile technical devices and technical devices situated outside of protected area have the character of data carriers. Classified information shall be protected pursuant to special regulations¹⁾ or their adequate combination, provided that the required level of security classification is maintained.

(12) In exceptional cases, technical devices accepted into operation may also be used for the lower level of security classification, as is the level of security of the classified information processed on them, on the basis of approval given by the Authority provided that the required level of security classification of classified information processed is maintained using devices or measures pursuant to a special regulation¹⁾ or their appropriate combination.

Article 3

Approval of Technical Devices into Operation

(1) A managing person may approve of a technical device into operation provided that

- a) The technical device is certified⁵⁾;
- b) Operational conditions of the technical device are in compliance with the approved security project⁶⁾ and work conditions of a certified device.

(2) Before the introduction of a technical device into operation, the managing person shall provide for the processing of:

- a) Protocol about the approval of a technical device into operation, specifying the period of permitted operation, conditions and methods of its use;
- b) Directive for the use of the technical device.

Article 4

Directive for the Use of Technical Devices

(1) The directive for the use of a technical device (hereinafter referred to as “directive”) shall specify the tasks and measures resulting from a security project.

(2) The directive shall contain:

- a) List of technical and system devices determined by a security project for work with classified information, stating the name and type of the technical device, identifier of the

⁵ Article 55 paragraph 4 Act No.215./2004 (Coll.)

⁶ Article 58 of Act No.215/2004 (Coll.)

- technical device, level of security classification for which the technical device may be used, as well as the location of the technical device;
- b) List of persons authorized for the use of technical and systemic devices, prepared in such a way that it is evident which person shall work with which technical device or technical devices, as well as the scope of authorizations, method of identification and authentication of a specific person, pursuant to Article 5, for each allocated technical device, scope and method of use of systemic means, services and application software; the lists of persons and scopes of authorizations may be defined in an independent annex to the directive;
 - c) Specification of a security administrator responsible for the administration of security functions;
 - d) Specification of an information system administrator responsible for the execution of control over the performance of security principles in terms of system functionality;
 - e) Form of control and the maximum time intervals between individual controls;
 - f) Form of securing the protection of classified information in the case of emergencies or failures of technical devices.
- (2) The applicant develops the directive especially for the security administrator, information system administrator and individual users or groups of users.

Article 5 Use of Technical Devices

(1) A security administrator specifies the scope of actions that may be carried out by an authorized person. The scope of actions is encoded through an identifier of the user in direct relation to a technical device on the basis of the knowledge of information only available to the user, by which he identifies himself to the technical device and the authentication of the user. The authentication of a user shall mean the verification of his identity according to a required rate of guarantee based on the principle of the comparison between the user's access identifier (e.g., password) and a value saved in the authenticated object.

(2) The user's identifier for a technical device used for the processing of classified information of the level of security classification "Restricted" is as follows:

- a) Knowledge of an information only available to the user;
- b) Access tool that definitely identifies the user;
- c) Combination of identifiers pursuant to letter a) and b).

(3) The user's identifier for a technical device used for the processing of classified information of the level of security classification "Top Secret", "Secret" or "Confidential" is as follows:

- a) Knowledge of an information only available to the user by which he identifies himself to a technical device and, at the same time, an access tool by which he confirms this identity,
- b) Access tool by which he identifies himself to a technical device and the simultaneous use of the technical device or part of it for the reading of one of the user's personal characteristic attributes which clearly confirms his identity;

c) Other combination of methods for identification and authentication pursuant to letter a) a b), whilst the user's identification and authentication cannot be separated.

(4) The user's identifier may contain the information specifying the scope of authorizations within a technical device.

(5) A user is obliged to ensure that no loss, revelation or abuse of his identifier occurs.

(6) Each technical device by which classified information are processed shall contain a controlling mechanism and a blocking mechanism that prevents the user from working with a technical device if his identifier does not authorize him for this work.

(7) A classified material that is an output from a technical device, must be marked with a relevant level of security classification in order to secure the performance of the conditions established by the law for the specified level of security classification related to a classified material upon its further manipulation.

(8) The provision of paragraph 7 does not refer to encrypted classified papers, which are intended for transfer by standard communication means.

(9) Technical devices shall be placed in protected areas, within which their protection against any unauthorized access by unauthorized persons, damage, unfavourable electromagnetic radiation or manipulation is secured in compliance with a security project. The form of protection of the technical devices must comply with the requirements for the security of the technical devices processing classified information of a relevant level of security classification.

(10) Technical devices shall be placed in such a way as to prevent any unauthorized persons viewing the classified information.

(11) All carriers of classified information shall be registered as administrative instruments⁷), if possible in regard to their character and purpose of use.

(12) The Authority shall specify the technical devices indented for interface between the Authority and central state administration bodies.¹⁾

Article 6

Certification of Technical Devices

(1) The types of certification of technical devices are as follows:

- a) Certification of the type of technical device (hereinafter referred to as "type certification");
- b) Certification of individual technical devices.

(2) The Authority, or an authorized person, shall recognise the test results issued by a foreign certification authority, if resulting from an international treaty or other type of agreement that the Slovak Republic is bound by.

⁷ Regulation of the National Security Authority No. 338/2004 (Coll.)

Article 7
Type Certification

(1) By type certification, the conformity of attributes of a type of technical device shall be verified and certified with the security requirements pursuant to Article 2 and 5. The execution of a type certification shall result in a certificate pursuant to Annex No. 2.

(2) A managing person shall file an application for the execution of a type certification to the Authority or authorized person pursuant to Annex No. 1.

Article 8
Certification of Individual Technical Devices

(1) The certification of individual technical devices is a kind of certification by which the conformity of attributes of the technical device is verified and certified with the security requirements defined in Article 2 and 5, if the Authority did not issue a type certificate.

(2) The certification of an individual technical device shall appropriately follow the provisions of Article 7.

Article 9
Use of Systemic Devices

(1) A recommended systemic device with the recommended security set-up for the level of security classification and under the conditions defined in the certificate of the technical devices may only be used for work with classified information. The list of recommended system devices shall be regularly published on the Internet website of the Authority.

(2) Each systemic device that process classified information shall contain a controlling mechanism and a blocking mechanism that prevents the user working with the relevant systemic device, if his identifier does not authorize him for this work.

(3) The Authority shall specify the system devices indented for interface between the Authority and central state administration bodies.

Article 10
Security of Information Systems

(1) The operator of an information system shall provide for its operation through the information system administrator and security administrator and is responsible for the security of its operation in compliance with the security project and directives. An information system shall mean one or more computers, their software, peripheral devices, processes or means that form an integral unit capable of carrying out the collection, generation, processing, filing, display and transfer of classified information.

(2) The duty of a security administrator shall contain the execution of the administration of an information system security, especially the allocation of access rights, administration of authentication and authorization functions, evaluation of control records about the activity of

the information system, development of reports on unauthorized manipulations with the information system and duties resulting from directives for the use of a technical device.

(3) An information system administrator shall execute the administration of a system and its resources.

(4) In an information system, the role of the security administrator shall be implemented separately from the role of the information system administrator.

(5) In information systems that process classified information of the level of security classification “Confidential”, “Secret” and “Top Secret”, the continuous keeping of a control record of the activity of the information system and parts thereof must be ensured, with the possibility of its monitoring, backward examination, as well as the determination of responsibility of specific users for the activity performed by them in the information system.

Article 11 Security Project for Technical Devices

(1) A security project for a technical device shall contain the following:

a) Basic information

1. Name, type, identification or specification of a technical device;
2. Level of security classification of the processed classified information;
3. Name, address and company registration number of the organisation;
4. Name of the executor (author or composite authors),
5. Imprint of a stamp of the organisation, date of approval and signature of the approver;

b) Security plan

1. Requirements for the security of a technical device for the required level of security classification of the technical devices;
2. Evaluation of the current status, specification of problems and insufficiencies in the security of the technical devices;
3. Specification of the key problems;

c) Description of a technical device

1. Specification of the environment in which a technical device is placed;
2. Specification of the information environment (hardware, software);
3. Conditions for the operation of a technical device;

d) Analysis of the protection of classified information

1. Classification of the main threats to classified information;
2. Classification of possible countermeasures to individual threats;

e) Specification of the security standards used and determination of other methods and devices for the protection of classified information used, which solve the issue concerning

the security of a technical device against loss of reliability, integrity and availability of classified information;

- f) Specification of threats secured by protective measures, which contains specific threats actually affecting the assets, as well as the implemented countermeasures;
- g) Specification of threats not secured by protective measures, which contains specific threats actually affecting the assets to which no adequate countermeasures are implemented;
- h) Directive for the emergency planning and renewal of activities of a technical device or system, which shall contain:
 - 1. Organisational measures used in extraordinary events;
 - 2. Means of control of these organisational measures.

(2) The control and update of a security project shall be carried out after every change that could affect its content, in the form of an annex. The security project and annex to it shall form a subject to approval proceedings by the Authority.

Article 12 Use of Security Standards

(1) The security standards represent a system of standards that specify the minimum criterion for the required level of protection of technical devices.

(2) The Authority shall issue a list of standards used for the determination of a security standard, whilst publishing the current list of them on its Internet website.

(3) The security standard of technical devices is determined pursuant to technical standards.⁸⁾

Article 13 Operation

This Regulation shall enter into force on 1 June 2004.

Aurel Ugor, by his own hand.

⁸ STN ISO / IEC 17799 Information Technologies. Code of the Information Security Management Practice; STN ISO / IEC TR 13335-1 Information Technologies. Instructions for IT Security Management. Section 1: IT Security Concepts and Models; STN ISO / IEC TR 13335-2 Information Technologies, Instructions for IT Security Management. Section 2: IT Security Planning and Management; STN ISO / IEC TR 13335-3 Information Technologies. Instructions for IT Security Management. Section 3: IT Security Management Techniques; STN ISO / IEC TR 13335-4 Information Technologies. Instructions for IT Security Management. Section 4: Selection of Security measures; STN ISO 7498-2 Information Process Systems. Open Systems Interface (OSI). Basic Reference Model. Section 2: Security Architecture; STN ISO / IEC 9796 Information Technology. Security Methods. Digital Signature Method giving Message Recovery; STN ISDO / IEC 9797 Information Technologies. Security Techniques. Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm; STN ISO / IEC 9798-1 Information technology. Security Methods. Entity Authentication Mechanisms. Section 1: General Model; STN ISO / IEC 9798-2 Information Technologies. Security Techniques, Entity Authentication Mechanism. Section 2: Mechanism with Symmetric Cipher Algorithm; STN ISO / IEC 9798-3 Information Technologies. Security Techniques, Entity Authentication Mechanism. Section 3: Entity Authentication through Registered Key Algorithm; ISO 8732, ISO 9564-1; ISO 9564-2; ISO / IEC 101664, TCSEC / Trusted Computer Evaluation Criteria, ITSEC International Trusted Evaluation Criteria.

Annex No. 1 to Regulation No. 339/2004 (Coll.)

APPLICATION

**for the execution of type certification/individual technical device certification
for the level of security classification**
pursuant to Article 56 of Act No. 215/2004 (Coll.) on the protection of classified information
and on the amending and supplementing of certain laws

1. Applicant

Name:.....
Address:
Company Reg. No.:
Tel.: Fax:
Responsible employee: Tel:

2. Producer/supplier

Name:.....
Address:.....
Company Reg. No.:
Tel.: Fax:

3. Technical device

Type:
Production No. (or other clearly identifying parameter):.....
.....
Identification, authentication instrument:
Specification (bds, BIOS, etc.).....
.....
.....
.....

4. Documentation accompanying the application

Security project	Annex No.
Technical documentation.....	Annex No.
Certificates issued (inc. foreign laboratories)	Annex No.....
.....	Annex No.
.....	Annex No.
.....	Annex No.

Inon.....

.....
Signature and imprint of the
applicant's stamp

Annex No.2 to Regulation No. 339/2004 (Coll.)

The National Security Authority, pursuant to Article 70 paragraph 1 letter a) item 8 of Act No215/2004 (Coll.) on the protection of classified information and on the amending and supplementing of certain laws, issues this

C E R T I F I C A T E
of technical device

No.: C – level of security classification/TD

Name of the technical device
(identification attributes)

Holder of certificate:

Seat:..... Company Reg. No.:

Producer/Supplier:

Seat: Company Reg. No.:

This certificate certifies the capability of the technical device for work with classified information up to the level of security classification (including) the

level of security classification

The technical device may be used for work with classified information up to the level of security classification (inclusive) only under the performance of conditions specified in the Annex to this certificate.

Date of the certificate issue:

Certificate validity by:

In Bratislava, on:

.....
Director, by his own hand