Based on Article 30 of the Law on Classified Information (Official Gazette of the Republic of Macedonia, no. 9/2004), the Government of the Republic of Macedonia at its session held on 07.03.2005, passed the

DECREE ON INFORMATION SECURITY

(INFOSEC)

General Provisions

Article 1

This Decree regulates the measures and activities for information security (INFOSEC) concerning:

- certification of communication and information systems and processes;
- assessment for possible breech of security of the communication and information systems (CIS);
- definition of methods and security procedures for reception, processing, transmission, storing and archiving of electronic classified information;
- protection of the information during processing and storing of classified information in the CIS;
- production of crypto keys and other crypto material;
- cryptographic protection of communication, information and other electronic systems used for preparation, transmission, processing and archiving of classified information;
- determination of zones and rooms protected from compromising electro-magnetic emission; and
- installation of devices for safekeeping of classified information.

Certification of communication and information systems and processes

Article 2

The state organs and organizations (hereinafter referred to as “the institutions”) that plan to procure or install a CIS for classified information, shall submit a request to the Directorate for Security of Classified Information (hereinafter referred to as “the Directorate”) for security certification of the CIS (hereinafter referred to as “the system”).

Article 3

To the request from Article 2 of this Decree, the following documents shall be attached:

- risk assessment for the security of the system;

- security requirement statement for the system and
- security operating procedures for the system.

The documents in paragraph 1 of this Article shall be marked with the classification level commensurate to the highest level of classified information processed by the system.

Article 4

When the system includes a number of institutions, they shall enter into an agreement for connection of the systems.

The agreement from paragraph 1 of this Article shall be attached to the request for certification of the system.

Article 5

Security verification of the system shall be the final stage of the certification process of the system.

Article 6

The security verification of the system:

- determines whether the envisaged security measures, stipulated in the security requirement statement have been properly implemented;
- determines that security measures have been implemented and that the required security level has been achieved through appropriate security testing; and
- documents the results of the security implementation verification, as input to the certification process.

Article 7

The security testing of the system shall result in issuing of: a security certificate, a security certificate with limited duration and an interim security certificate.

Article 8

Security certificate shall be issued for a system where information classified CONFIDENTIAL and above is created, processed, stored or transmitted (hereinafter referred to as “processed”).

For the systems where information classified RESTRICTED is processed, which in line with the Law of Classified Information are not subject to certification, conditions shall be provided for maintaining the security objectives (confidentiality, integrity and availability) of information.

Assessment of possible breach of security of the CIS

Article 9

The assessment of possible breach of CIS security shall be conducted to determine the risk, the assessment of the residual risk, to evaluate the vulnerability and threats and to determine the consequences from the realization of certain threats.

Article 10

The risk assessment and the determination of appropriate measures for protection of the system shall be undertaken by authorized persons employed at the institution.

As appropriate, external experts may be included in the risk assessment.

Article 11

When a system is used in specific conditions (mobile, terrain and other), the risk assessment shall also include the risks related to the surrounding where the system is used.

Article 12

The system vulnerability assessment shall be accomplished in determined timelines and with vulnerability assessment proceedings envisaged in the system vulnerability assessment plan.

Determining of methods and security procedures for receiving, processing, transmitting, storing and archiving of electronic classified information

Article 13

The locations of the systems where classified information is processed shall be determined as security and administrative zones, in line with the regulation on physical security of classified information.

When the system is used in specific conditions (mobile, terrain and other), specific conditions for physical security shall be applied.

Article 14

Separate rooms shall be identified within the security zones for: electronic processing of information, system management, work with cryptographic devices and keys and for an archive of storage media holding classified information.

Article 15

When identifying authorized persons for system security management, particular attention shall be given all important security elements not to be controlled by one person alone.

Article 16

The systems processing classified information are required to have computer security particularly for:

- identification of persons having access to the system;
- control and maintaining records of the access to the facilities of the system based on the authorized access to a defined data base;
- up-to-date records of the condition of the system, related to its security (security records), the activity of the system, the parameter changes etc.;
- possibility for studying the security records and determining of the users' activity related to the system security;
- installing program applications in the system that will prevent unauthorized access of users;
- ensuring a security mode of operation for classification marking;
- identification of the user of the print, recorded, modified or copied document;
- up-to-date records of the modification, copying, re-recording and deleting of classified information according to the users; and
- protection of the important technical and program elements, system possibilities and its functionality.

Article 17

The systems processing classified information may operate in one of the following security modes of operation:

- "dedicated";
- "system high";
- "compartmented"; and
- "multi-level".

Article 18

Computer security of the systems in the security modes of operation "dedicated", "system high" and "compartmented" shall be ensured with the minimum requirements for computer security.

Computer security of the systems in the security mode of operation "multi-level" shall be accomplished with the security of the system in line with Article 16 of this Decree and the application of additional access control of the users to the program elements of the system.

Protection of information during processing and storage in CIS

Article 19

The institutions shall control and evaluate all the changes in the wider, closer and electronic environment affecting the security of the system and shall apply measures and actions for security and protection of the system.

Article 20

The following shall be undertaken to provide security and protection of the system during its use:

- periodical checking of the systems, devices and removable computer storage media from the aspect of quality and functionality;
- recording the system data and the classified information in separate removable computer storage media and their storing in a detached place corresponding to the highest classification level of the recorded data;
- installing software and configuration of the system by authorized person only;
- application of new technical and programming devices in the system only upon a previously received certificate;
- servicing and repair of devices from the system in a way that prevents breeching of its security and that is in line with the conditions for certification;
- replacement of cryptographic methods, devices and keys according to the provisions of the Decree on Crypto Protection or an international agreement;
- assessment and, as appropriate, protection from compromising electromagnetic emission of the devices having been serviced, repaired or renewed; and
- prohibition for bringing and using privately-owned computers, recording media and software in the security and administrative zones of the system.

Article 21

The portable computing devices may be included in a certified system only if they have been previously certified for processing information of an appropriate classification level and if they have been approved by the authorized person of the institution.

Article 22

Information classified TOP SECRET and SECRET shall not be processed in portable computing devices.

Article 23

The removable computer storage media that have once held information classified TOP SECRET and SECRET shall be destroyed after their declassification.

The computer storage media holding information classified CONFIDENTIAL and lower may be kept for further use after its declassification.

Article 24

The removable computer storage media holding classified information that have come to the end of their useful life or have been damaged shall be destroyed.

Article 25

The automatic computing devices that function without the presence of an operator, shall not process information classified CONFIDENTIAL and above.

Article 26

Privately-owned computing devices and removable computer storage media (personal computers, portable computers, floppy units, memory elements and similar) shall not be used for processing information classified RESTRICTED and above.

Article 27

Removable computer storage media that are used in the system shall be marked, registered and archived in a manner commensurate with the media holding the information.

Marking, control, archiving, periodical control and disposal of removable computer storage media holding classified information shall be done according to the Decree on Administrative Security of Classified Information.

Article 28

Removable computer storage media holding information and data that provide access to the system (specific codes, passwords, identification elements) shall be protected with measures corresponding to the measures for protection of the highest level of classified information held in the system.

The information and data from paragraph 1 of this Article shall be destroyed in line with the security operating procedures for the system and in a manner that prevents recovery of the records.

Article 29

Portable computing devices and removable computer storage media used for processing classified information shall be considered as documents that contain classified information.

Removing the devices stipulated in paragraph 1 of this Article out of the security zones shall be done in the same manner as the one applied for the other classified information.

Production of crypto keys and other crypto material

Article 30

Distribution and storage of crypto keys to systems used for international exchange of classified information shall be done within the Directorate.

Distribution and storage of crypto devices and keys to systems used for exchange of classified information with foreign states and international organizations shall be done in accordance with an international agreement.

Cryptographic protection of the systems for classified information

Article 31

Transmission of classified information between the Central Registry and the registries and the control points of the Directorate shall be carried out through a secure system for cryptographic protection.

Article 32

The systems for cryptographic protection shall ensure:

- safe and protected identification of the users;
- confirmation of the authenticity of the sender and the receiver of the information that needs to be done prior to the transmission of the information;
- confidentiality, integrity and availability of the information; and
- confirmation for the receipt of the information.

Article 33

Classified information shall not be transmitted through communication systems outside the security zones without application of cryptographic methods and devices.

Article 34

Cryptographic methods and devices for protection of information classified TOP SECRET and SECRET shall be used for the protection of the information during their storage.

Identification of zones and rooms protected from compromising electromagnetic emission

Article 35

The systems used for processing information classified CONFIDENTIAL and above shall be protected from compromising electromagnetic emission.

Installing devices for storage of classified information

Article 36

Classified information shall be stored in devices installed by competent and authorized persons of the institutions.

Final provision

Article 37

This Decree shall enter into force on the eight day from the day of its publication in the “Official Gazette of the Republic of Macedonia”.