On the basis of Article 33, paragraph 1 of the Law on Classified Information (*Official Gazette of the Republic of Serbia*, No.104/09) and Article 42, paragraph 1 of the Law on the Government (*Official Gazette of the Republic of Serbia*, No. 55/05, 71/05 - corrigendum, 101/07, 65/08 and 16/11),

The Government hereby passes the following

DECREE ON SPECIAL MEASURES FOR THE PROTECTION OF CLASSIFIED INFORMATION WITHIN INFORMATION AND TELECOMMUNICATION SYSTEMS

I. INTRODUCTORY PROVISION

Article 1

The Decree sets out special measures for the protection of classified information within information and telecommunication systems.

II SPECIAL MEASURES FOR THE PROTECTION OF CLASSIFIED INFORMATION WITHIN INFORMATION AND TELECOMMUNICATION SYSTEMS

Article 2

Special measures for the protection of classified information within information and telecommunication systems (hereinafter: the system) shall be technical and organizational actions undertaken to prevent accidental mistakes, irregular and unauthorized gathering, storage, processing, use, damage, destruction, falsification and abuse of classified information.

Special measures for the protection of classified information within the system shall refer to the following: the facility in which the system is located (equipment, documents, software support and network); the space, premises or security areas in which classified information is processed within the system; the authorized persons for the system security management; all participants in the operation of the system; the use of the system for the performance of activities with classified information; the mode of operation of the system; the protection of classified information during of its processing and storage within the system; the protection from the risk of compromising electromagnetic emanations, and the installation of devices for the storage of classified information.

Article 3

The technical measures set out in Article 2, paragraph 1 of this Decree shall in particular refer to the following:

1) physical protection of facilities, space, premises or security areas in which classified information is processed within the system, as well as resources and documents within the system;
2) fire protection;
3) safeguarding and protection of the equipment (choosing adequate and reliable equipment, safeguarding such equipment in the course of its operation, regular maintenance and supply of spare parts) and documents in the course of their use and storage;
4) software protection (from the design and development to the application stage of the software system);
5) network protection (in the course of its design and operation).

The organizational measures set out in Article 2, paragraph 1 of this Decree shall in particular refer to the following:

1) organization and methodology of activities performed within the system in the course of its design (drafting of a preliminary development study, determining the classification level of information to be processed within the system and the level of classification of the system itself, conceptual design, master design, contractor's design and introduction of designed solutions), and in the course of operative working of the system (planning activities and maintaining records of executing all procedures relevant for the functioning of the system and the flow of documents);
2) establishing contingency procedures;

3) other conditions for the successful functioning of the system (check-outs when engaging new employees, setting activities and assignments for participants in the work of the system, professional training of employees, etc.);

Article 4

The space, premises or security areas in which classified information is processed in the system shall be established in accordance with the regulation setting out special measures for the physical and technical protection of classified information.

Article 5

The public authority or the legal entity which provides services to the public authority based on the contractual relationship (hereinafter: the legal entity) shall each designate a person who shall be authorized for the management of the system security.

Such authorized person for the system security management within the public authority or the legal entity shall monitor and evaluate the security characteristics of the system.

When designating its authorized person for the system security management, the public authority or the legal entity shall ensure that a single individual does not control all relevant elements of the system security, as well as that such an individual holds an adequate security clearance certificate for access to classified information.

Article 6

The system shall meet the conditions for the following:

1) protection from unauthorized access, which implies identification and reliable authentication of the identity of individuals having access to the system;
2) control and maintenance of records of access to the system;
3) a continuing recording (automated, manual or combined) of the security status of the system (security log file), system activities and modifications of the current status of the system;

4) examination of security log files by the authorized persons;
5) defining users' authorizations relating to the security of the system;
6) defining users' authorizations relating to the usage of the system;
7) providing a secure method for marking classification levels;
8) identification of a user who modifies, prints, re-records or deletes classified information;
9) recording a modification, printing, re-recording or deletion of classified information by such a user;
10) protection of relevant technical and software elements, possibilities and functionalities of the system;
11) protection of the back-up archive of classified information in case of loss of the existing archives, as well as maintenance of records of access to such archives;

Article 7

The system shall operate in one of the following security modes:

1) NON-SELECTIVE
2) SELECTIVE
3) MULTI-LEVEL

The head of the public authority or the responsible person of the legal entity shall determine the security mode of the system operation in a specific document.

Article 8

With respect to the system operating in the NON-SELECTIVE security mode of operation, all individuals having access to that system shall have a security clearance certificate for access to information classified at the highest level processed within the system, as well as have access to all classified information processed within the system.

With respect to the system operating in the SELECTIVE security mode of operation, all individuals having access to that system shall have a security clearance certificate for access to information classified at the highest level processed within the system, and may have access to some classified information only.

With respect to the system operating in the MULTI-LEVEL security mode of operation, the individuals having access to that system do not need a security clearance certificate for access to information at the highest level of classification processed within that system, and shall have access only to some classified information processed within the system.

The selective approach to the system and the selective approach to classified information within the system shall be implemented by means of adequate hardware and software.

Article 9

Classified information may not be transmitted across the system beyond the security areas without applying the methods and tools of cryptographic protection.

Article 10

In order to maintain the system security during its use, the public authority or the legal entity shall carry out the following:

1. periodical verification of the system, all its components and media for the storage and transmission of classified information, as well as examination of the conditions created for ensuring confidentiality, availability, integrity and authenticity of classified information within the system;
2. storage of classified information relating to the system, as well as classified information processed within the system on separate documents along with the maintenance of mandatory back-up records and the implementation of protective measures envisaged for information classified at the highest level which is found within the system;
3. installation of hardware, software and configuration of the system by the authorized persons;
4. application of new technical and software resources to the system in accordance with adequate SRPS ISO/IEC 27001 and SRPS ISO/IEC 17799 technical standards;
5. maintenance and repair of the system resources in a manner that does not impair the system security;
6. testing of the system resources, which have undergone maintenance and repair outside the premises of the public authority or the legal entity

against the effects of compromising electromagnetic emanations exercised by specialists;
7. adequate procedure in case of an unauthorized disclosure of classified document or a loss of a document containing classified information;
8. adequate procedure in case of detecting an unauthorized intrusion into the system;
9. planning of security measures in case of contingency.

Article 11

Portable information and telecommunication resources and documents used within the system shall be regarded as classified information, which can be included into the system only on condition that specialists of the public authority or of the legal entity have previously tested the system against a possible compromise.

If the public authority or the legal entity does not have specialists to carry out the testing referred to in paragraph 1 of this Article, the above testing shall be carried out by mutual agreement on the premises of the public authority, which have such specialists in its employ.

Article 12

Documents used within the system and marked with different classification levels shall be assigned a higher classification level in accordance with the law.

Documents providing the access to the system (codes, passwords, identification elements, etc.) shall be safeguarded by measures envisaged for the protection of information marked with the highest classification level which is found in the system.

Article 13

Privately-owned information and telecommunication resources and portable documents (personal computers, portable computers, diskettes, memory modules, etc.) shall not be used for the processing of classified information.

Article 14

If information classified at the TOP SECRET or SECRET level is reclassified or declassified, the document on which such information has been recorded in the electronic form shall not be reclassified or declassified.

If information classified at the CONFIDENTIAL or RESTRICTED level is reclassified or declassified, the document on which such information has been recorded in the electronic form may be reclassified or declassified only in case such information is deleted in a manner which disables its reconstruction by software tools.

The documents referred to in paragraph 1 and 2 of this Article shall be destroyed upon the expiry of their period of use or upon the expiry of the period of use of the system within which they have been used in accordance with the regulation setting out special physical and technical measures for the protection of classified information.

Article 15

Technically outdated or damaged documents on which classified information have been stored shall be destroyed in accordance with the regulation setting out special physical and technical measures for the protection of classified information.

Article 16

The use of automated information and telecommunication resources functioning without the presence of an operator shall be based on the risk assessment of the system security carried out by the head of the public authority or the responsible person of the legal entity.

Article 17

All components of the system used for the processing of information classified at the TOP SECRET, SECRET or CONFIDENTIAL level shall be protected from compromising electromagnetic emanations by implementing technical or operative measures against the impact of such emanations in accordance with the risk assessment relating to compromising electromagnetic emanations.

Article 18

The installation of devices and software onto the system shall be carried out by the authorized person for the system security management of the public authority or the legal entity.

Article 19

If classified information is exchanged with a foreign country or an international organization, standards on the security of networks and transmission devices, system interconnections and crypto protection of classified information envisaged by the pertinent international agreement shall be implemented in addition to special measures envisaged by this decree.

III USE OF THE SYSTEM FOR THE PURPOSE OF WORKING ON CLASSIFIED INFORMATION

Article 20

The public authority, as well as the legal entity intending to use the system for the processing and storage of classified information shall previously assess a possible risk of compromising the security of classified information by an intrusion into the system, as well as assess a threat to the use and destruction of classified information which has been processed and stored within the system (hereinafter: the risk assessment of the system security).

The risk assessment of the system security shall relate to the risk identification, assessment of unavoidable risks, assessment of the system vulnerability, as well as threats and possible effects of their realization on the system, including risks relating to the environment in which the system is used.

The risk assessment of the system security shall be carried out periodically in accordance with the risk assessment plan for the system adopted by the head of the public authority or the responsible person of the legal entity.

If the public authority or the legal entity has a need for an interconnection between their respective systems, they shall conclude an agreement on the interconnection between these systems.

Article 22

Along with the system risk assessment, the head of the public authority or the responsible person of the legal entity shall adopt a document prescribing a security procedure for receiving, processing, transmitting, storing and archiving classified information in the electronic form, as well as safeguarding project documentation (preliminary studies on the system development, conceptual project, master project and the contractor's project).

Article 23

The risk assessment shall be carried out for the system in which information classified as the TOP SECRET, SECRET and CONFIDENTIAL is processed, transmitted and stored.

With respect to the system in which information classified as RESTRICTED is processed, the public authority or the legal entity shall provide the maintenance of the appropriate security level of classified information (confidentiality, integrity, authenticity or availability) in accordance with regulations governing information security.

The verification of the implementation of the security level referred to in paragraph 2 of this Article shall be carried out by the public authority or the legal entity that is its respective authorized person for the system security management.

IV SYSTEM SECURITY RISK MANAGEMENT

Article 24

The system security risk management shall comprise the permanent assessment and processing of risk in order to prevent destruction, alienation, loss or unauthorized access to classified information.

The public authority or the legal entity shall adopt a decision on the system security risk management.

Article 25

The processing of the system security risk shall be an activity in which the risk acceptability level shall be determined for every risk assessed with a view to its acceptance, reduction or avoidance.

A risk shall be considered acceptable if the damage arising from such a risk were lesser than the damage arising from the non-implementation of security measures.

The risk reduction shall be carried out by implementing security measures in order to prevent destruction, alienation, loss or unauthorized access to classifed information.

The risk avoidance shall mean undertaking security measures in order to avoid actions that could cause a risk.

Article 26

After taking a decision on risk processing, the public authority or the legal entity shall adopt a document on risk processing which shall set out the implementation of necessary security measures.

The results of risk assessment and processing shall be reviewed on a regular basis in accordance with the needs of the public authorities or legal entities on the basis of the internal or external modifications which have arisen in the system.

V FINAL PROVISION

Article 27

This Decree shall enter into force on the eighth day from its publication in the Official Gazette of the Republic of Serbia.

Ref. No.05

Done in Belgrade on 14 July 2011.

GOVERNMENT

Ivica Dačić

First Deputy Prime Minister