PARLIAMENT OF CROATIA

1912

Pursuant to article 88 of the Constitution of the Republic of Croatia I hereby issue the

DECISION

PROMULGATING THE INFORMATION SECURITY ACT

I hereby promulgate the Information Security Act of the Republic of Croatia, passed by the Croatian Parliament at its session on 13 July 2007.

Class: 011-01/07-01/98
No.: 71-05-03/1-07-2
Zagreb, 18 July 2007.

President of the Republic of Croatia
(Sgd.) **Stjepan Mesić**

ACT

ON INFORMATION SECURITY

I. BASIC PROVISIONS

Article 1.

(1) This Act defines the concept of information security, the measures and standards of information security, the area of information security and the authorised bodies for establishing, implementing and supervising measures and standards of information security.
(2) This Act is implemented within government bodies, bodies of local and regional government, as well as legal persons with public authority, which use classified and unclassified information within their sphere of activities.
(3) This Act applies to legal and private persons which access or handle classified and unclassified information.

Article 2.

Terms in this Act have the following meanings:

– "Information security" is a state of information confidentiality, integrity and availability, which is achieved by implementing defined measures and standards of information security,

as well as organisational support for activities regarding planning, implementing, reviewing and revising measures and standards.

– "Information security measures" are general rules for protecting information which are conducted on a physical, technical and organisational level.
– "Information security standards" are organisational and technical procedures, as well as solutions, intended for the systematic and balanced implementation of defined information security measures.
– The "area of information security" is represented by the grouping of information security into five areas with the goal of systematically and efficiently defining, implementing and supervising measures and standards of information security.

– "Security accreditation of information systems" is a procedure for determining the competence of bodies and legal persons for managing security information systems mentioned under article 1, paragraph 2 of this Act and is conducted by determining implemented measures and standards of information security.

– "Information systems" are communication, computer and other electronic systems in which data is processed, stored and transmitted so that it may be available and usable for authorised users.

II. INFORMATION SECURITY MEASURES AND STANDARDS

Article 3.

Information security measures and standards determine the minimal criteria for protecting classified and unclassified information within bodies and legal persons mentioned under article 1, paragraph 2 and 3 of this Act.

Article 4.

(1) Measures and standards of information security are determined for classified and unclassified information.

(2) Measures and standards of information security are determined in accordance with the level of confidentiality, amount and type of threats to classified and unclassified information within a certain location.

(3) A constant security threat assessment is conducted for classified information with the "Confidential", "Secret" and "Top Secret" level of confidentiality.

Article 5.

Information security measures and standards include:

– supervision of access and handling of classified information,

– procedures conducted upon unauthorised disclosure and loss of classified information,

– planning measures for emergency situations,

– organising special data bases for classified information within the Republic of Croatia, as well as for classified information which is transmitted from other countries, international organisations or institutions with which the Republic of Croatia co-operates.

Article 6.

(1) Information security measures and standards for the protection of unclassified information

are determined in accordance with the measures and standards defined by legislation on the protection of personal citizen information.

(2) Information security measures and standards for the confidentiality level "Limited" is determined in accordance with paragraph 1 of this article along with:

– a prior review of the implementation of defined measures and standards for unclassified information,

– application of measures and standards defined for the "Limited" confidentiality level.

Article 7.

Information security measures shall be defined by a decree which shall be issued by the Government of the Republic of Croatia, and standards for implementing measures shall be defined by a code of rules which shall be issued by the heads of central state bodies for information security.

III. THE AREAS OF INFORMATION SECURITY

Article 8.

Information security measures and standards are defined for the following areas of information security:

– security checks,

– physical security,

– information security,

– information systems security,

– operational co-operation security.

Security Checks

Article 9.

(1) Security checks are an area of information security within which framework security information security measures and standards are determined and applied to individuals with access to classified information.

(2) Individuals mentioned under paragraph 1 of this article are obliged to present evidence of an individual security check (a certificate).

(3) Bodies and legal persons mentioned under article 1, paragraph 2 of this Act, which use classified information with a confidentiality level of "Confidential", "Secret" or "Top Secret" are obliged to draft:

– a list of individuals with access to classified information,

– a register of received certificates along with certificate validity dates.

Physical Security

Article 10.

(1) Physical security is an area of information security within which framework information security measures and standards are determined for the protection of facilities and devices which contain classified information.

(2) Bodies and legal persons mentioned under article 1, paragraph 2 of this Act, which use classified information with a confidentiality level of "Confidential", "Secret" and "Top Secret" shall categorise facilities into security zones defined by information security measures and standards.

Information Security

Article 11.

(1) Information security is an area of information security for which information security measures and standards are determined and which are implemented as general security measures for preventing, detecting and eliminating damages caused by the loss or unauthorised disclosure of classified or unclassified information.

(2) Bodies and legal persons mentioned under article 1, paragraph 2 of this Act, which use classified and unclassified information within their sphere of activities, are obliged to apply procedures for handling classified and unclassified information when determining the content and method of recording granted access to classified information, as well as to the supervision of security information defined by information security measures and standards.

Information Systems Security

Article 12.

(1) Information systems security is an area of information security within which framework information security measures and standards are determined for classified and unclassified information which is processed, stored or transferred within an information system, as well as the protection of the integrity and availability of information systems for the processes of planning, drafting, building, applying, maintaining and terminating information systems.

(2) Security accreditation of information systems is conducted for information systems which use classified information of a confidentiality level of "Confidential", "Secret" or "Top Secret".

(3) Individuals which participate in processes mentioned under paragraph 1 of this article must possess a "Top Secret" level certificate or one of a level higher than the highest level of confidentiality of the classified information which is being processed, stored or transferred within security systems under their authority.

(4) Measures for the physical protection of facilities in which information systems are located shall be conducted in accordance with the highest level of confidentiality of the classified information which is being processed, stored and transferred within them.

(5) The central government bodies for information security shall draft a register of certified equipment and devices used for classified information systems of a "Confidential", "Secret" or "Top Secret" level.
The register of certified equipment and devices is drafted based on relevant registers of international organisations or their own certification in accordance with correlating international standards.

Operational Co-operation Security

Article 13.

(1) Operational co-operation security is an area of information security in which defined

security information measures and standards are implemented for conducting tenders or contracts using classified documentation which applies to legal and physical persons mentioned under article 1, paragraph 3 of this Act.

(2) Legal and physical persons that approach conducting tenders or contracts mentioned under paragraph 1 of this article, are obliged to present evidence of a security check for legal persons (an operational security certificate).

(3) Legal and physical persons mentioned under paragraph 1 of this article are obliged to apply determined information security measures and standards for the specific confidentiality level of classified information to staff and facilities.

(4) Bodies and legal persons mentioned under article 1, paragraph 2 of this Act are authorised to issue requests for providing operational security certificates to legal and physical persons to whom they supply classified information of a confidentiality level of "Confidential", "Secret" or "Top Secret".

(5) Legal and private persons which participate in international operations which require an operational security certificate are authorised to issue requests for providing certificates.

(6) Operational security certificates are issued by central state bodies for information security.

IV. CENTRAL STATE BODIES FOR INFORMATION SECURITY

Office of the National Security Council

Article 14.

The Office of the National Security Council is the central government body which co-ordinates and adjusts the issuance and implementation of information security measures and standards within the Republic of Croatia and the exchange of classified and unclassified information between the Republic of Croatia and foreign countries and organisations.

Article 15.

(1) The Office of the National Security Council issues a Code for Security Check Standards, a Code for Physical Security Standards, a Code for Security Information Standards, a Code for Organisational and Management Standards within the Area of Security Information and a Code for Operational Co-operation Security Standards.

(2) The Office of the National Security Council constantly adjusts defined information security measures and standards within the Republic of Croatia to international standards and recommendations for information security, and also participates in the national standardisation of the information security area.

Article 16.

(1) The Office of the National Security Council co-ordinates the activities of the bodies and legal persons mentioned under articles 17, 20, 23 and 25 of this Act.
(2) The Office of the National Security Council co-operates with the authorised institutions of foreign states and organisations within the information security area and it also co-ordinates international co-operation with other bodies and legal persons mentioned under paragraph 1 of this article.

The Department of Information Systems Security

Article 17.

(1) The Department of Information Systems Security is the central state body for the technical area of information system security for bodies and legal persons mentioned under article 1, paragraph 2 of this Act.

(2) The technical areas of information systems security are:

– information systems security standards,

– security accreditation of information systems,

– management of encoded material used for exchanging classified information,

– co-ordination of prevention and solutions for computer threats to information system security.

Article 18.

(1) The Department of Information Systems Security regulates the standards of the technical areas of information systems mentioned under article 17, paragraph 2 of this Act with a code of rules.

(2) The Department of Information Systems Security continually correlates the standards of the technical area of information systems security in the Republic of Croatia with international standards and recommendations and also participates in the national standardisation of information systems security.

Article 19.

The Department of Information Systems Security conducts the security accrediting activities of information systems in co-operation with the Office of the National Security Council.

V. THE NATIONAL CERT

Article 20.

(1) CERT is a national body for preventing and defending against computer threats to the security of public information systems in the Republic of Croatia.

(2) CERT is a separate organisational unit which is organised within the Croatian Academic and Research Network (hereinafter: CARNet).

(3) CERT correlates procedures for security computer incidents within public information systems which occur in the Republic of Croatia or in other countries and organisations when they relate to the Republic of Croatia.

(4) CERT correlates the activities of bodies which operate to prevent and defend against computer threats to the security of public information systems in the Republic of Croatia and also determines the rules and methods of joint operations.

Article 21.

CERT and The Department of Information Systems Security co-operate in the prevention and defence against computer threats to information systems security and also co-operate in drafting recommendations and norms in the Republic of Croatia within the area of information systems security.

Article 22.

The director of CARNet-a appoints an assistant who is responsible for managing CERT.

VI. IMPLEMENTATION OF INFORMATION SECURITY

Article 23.

(1) Bodies and legal persons mentioned under article 1, paragraph 2 of this Act are obliged to implement information security measures and standards mentioned under article 7 of this Act.

(2) The central body of the government administration in charge of information system development shall apply measures and standards mentioned under paragraph 1 of this article to the bodies and legal persons which do not have appropriate IT or technical capabilities.

(3) Measures and standards mentioned under paragraph 1 of this article shall be applied within the area of the education and academic sector by the central body of the government administration in charge of science and education.

Article 24.

(1) Bodies and legal persons mentioned under article 1, paragraph 2 of this Act shall determine the implementation of information security measures and standards with a code of rules.

(2) Central bodies of government administration mentioned under article 23, paragraphs 2 and 3 of this Act shall determine the method of implementing security information measures and standards in other bodies with a code of rules.

VII. SUPERVISION OF INFORMATION SECURITY

Article 25.

(1) The activities of information security supervision are the activities of supervising the organisation, implementation and efficiency of defined information security measures and standards in bodies and legal persons mentioned under article 1, paragraph 2 of this Act.

(2) The supervision activities mentioned under paragraph 1 of this article are conducted by advisors for information security.

(3) The Office of the National Security Council shall determine the criteria for organising the jobs of advisors for information security mentioned under paragraph 2 of this article with a code of rules.

Article 26.

(1) An advisor for information security issues a report on the results of implemented supervision to the head of the body or legal person as well as to the central body of information security.

(2) Based on the report mentioned under paragraph 1 of this article, the central state body for information security is authorised to:

– issue instructions with the aim of eliminating determined faults and errors, which supervised bodies and legal persons are obliged to eliminate within a specific period,

– conduct the procedure of reviewing further validity of security accreditation of information systems,

– initiate the process of determining responsibility,

– conduct other measures and activities which they are authorised for under special regulations.

(3) The head of a body or legal person is obliged to conduct measures for eliminating determined faults in the implementation of supervision.

VIII. TRANSITIONAL AND FINAL PROVISIONS

Article 27.

The decree mentioned under article 7 of this act shall be issued by the Government of the Republic of Croatia within a period of three months from the date of entry into force of this Act.

Article 28.

(1) The codes of rules mentioned under article 15, paragraph 1 of this Act shall be issued by the Office of the National Security Council within a period of six months from the date of entry into force of this Act.

(2) The code of rules mentioned under article 25, paragraph 3 of this Act shall be issued by the Office of the National Security Council within a period of six months from the date of entry into force of this Act.

(3) The code of rules mentioned under article 18, paragraph 1 of this Act shall be issued by the Department of Information System Security within a period of 30 days from the date of entry into force of the rule book mentioned under paragraph 1 of this article.

Article 29.

(1) CARNet is obliged to correlate its statute to the Office of National Security and to obtain the approval of the latter within a period of three months from the date of entry into force of this Act.

(2) The code of rules mentioned under article 24, paragraph 1 and 2 of this Act shall be issued within a period of nine months from the date of entry into force of this Act.

Article 30.

This Act shall enter into force 8 days from the date of publication in the Official Gazette.

Class: 650-05/07-01/01

Zagreb, 13 July 2007.

THE PARLIAMENT OF THE REPUBLIC OF CROATIA

Speaker

Parliament of the Republic of Croatia

(Sgd.) **Vladimir Šeks**