THE CROATIAN PARLIAMENT

Pursuant to Article 88 of the Constitution of the Republic of Croatia, I hereby issue the

DECISION
ON PROMULGATING THE INFORMATION SECURITY ACT

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

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

The President of the Republic of Croatia
Stjepan Mesić, m.p.

INFORMATION SECURITY ACT

I BASIC PROVISIONS

Article 1

(1) This Act establishes the notion of information security, information security measures and standards, information security areas and competent authorities for the adoption, implementation and oversight of information security measures and standards.

(2) This Act applies to state authorities, local and regional self-government bodies and legal persons with public authority who, within their scope of work, use classified and unclassified data.

(3) This Act also applies to legal and natural persons who gain access to or handle classified and unclassified data.

Article 2

Particular notions within the meaning of this Act shall have the following meaning:
- **information security** is the state of confidentiality, integrity and availability of information, which is achieved by implementation of stipulated information security measures and standards and by organisational support for jobs of planning, implementation, assessment and update of measures and standards.
- **information security measures** are general rules of data protection which are realized on the physical, technical and organisational level.
- **information security standards** are organisational and technical procedures and solutions intended for systematic and standardized implementation of stipulated information security measures.
- **information security areas** represent a division of information security field into five areas with the goal of systematic and effective realization of adoption, implementation and oversight of information security measures and standards.

- **security accreditation of information systems** is the procedure within which the degree of competence is determined for bodies and legal persons referred to in Article 1, paragraph 2 of this Act for managing information system security, and is performed by determining implemented information security measures and standards .
- **information system** is communicational, computer or other type of electronic system within which information are processed, stored or transmitted in such a way that they are available and applicable for authorised users.

II INFORMATION SECURITY MEASURES AND STANDARDS

Article 3

Information security measures and standards shall be used to determine minimum criteria for the protection of classified and unclassified data in bodies and legal persons referred to in Article 1, paragraphs 2 and 3 of this Act.

Article 4

(1) Information security measures and standards shall be determined for both classified and unclassified data.

(2) Information security measures and standards shall be determined in accordance with the degree of secrecy, number, type and threat to classified and unclassified data at a particular location.

(3) For CONFIDENTIAL, SECRET and TOP SECRET classified data security threat assessment shall be permanently performed.

Article 5

Information security measures and standards shall encompass as follows:
- oversight of access to and handling of classified data
- procedure during unauthorised disclosure and loss of classified data
- planning of measures during emergency situations
- founding of separate data bases for data classified in the Republic of Croatia and for classified data delivered by another country, international organization or institution that the Republic of Croatia cooperates with.

Article 6

(1) Information security measures and standards for unclassified data protection shall be determined in accordance with measures and standards for the personal data protection as stipulated by law.

(2) Information security measures and standards for the protection of RESTRICTED degree of secrecy shall be determined in accordance with paragraph 1 of this Article, with the addition of:
- prior verification of the implementation of stipulated measures and standards for unclassified data
- implementation of measures and standards stipulated for RESTRICTED degree of secrecy

Article 7

Information security measures shall be stipulated by the Regulation adopted by the Government of the Republic of Croatia and standards for the implementation of measures shall be stipulated by Ordinances adopted by the Heads of National Security Authority (NSA) and National Communications Security Authority (NCSA).

III INFORMATION SECURITY AREAS

Article 8

Information security areas for which information security measures and standards are stipulated, are as follows:

- Personnel Security
- Physical Security
- Security of Information
- INFOSEC
- Industrial Security

Personnel Security

Article 9

(1) Personnel Security is the information security area within which information security measures and standards are determined that are applied on persons who have classified data access.

(2) Persons referred to in paragraph 1 of this Article shall obtain Personnel Security Clearance (Certificate).

(3) Bodies and legal persons referred to in Article 1, paragraph 2 of this Act, who use classified data of CONFIDENTIAL, SECRET and TOP SECRET degree of secrecy, shall establish as follows:

- the list of persons with classified data access
- the registry of Certificates issued with their respective expiry dates

Physical Security

Article 10

(1) Physical security is the information security area which determines information security measures and standards for the protection of objects, facilities and equipment where classified data are stored.

(2) Bodies and legal persons referred to in Article 1, paragraph 2 of this Act, who use data of CONFIDENTIAL, SECRET and TOP SECRET degree of secrecy, shall perform the categorization of objects and facilities to security zones that are stipulated by information security measures and standards.

Security of Information

Article 11

(1) Security of information is the information security area for which determined are implemented as general measures of protection for prevention, detection and removal of damage caused by loss or unauthorised disclosure of classified and unclassified data.

(2) Bodies and legal persons referred to in Article 1, paragraph 2 of this Act, who use classified and unclassified data within their scope of work, shall implement the procedures on handling classified and unclassified data, on content and management of the records of classified data access and oversight of information security and stipulated information security measures and standards.

INFOSEC

Article 12

(1) INFOSEC is the information security area within which information security measures and standards are determined for classified and unclassified data that are processed, stored or transmitted within the information system and the protection of integrity and availability of the information system in the process of planning, designing, making, using and cease of work of the information system.

(2) Security accreditation of the information system shall be performed for the information system where classified data of CONFIDENTIAL, SECRET and TOP SECRET degree of secrecy are used.

(3) Persons who take part in the process referred to in paragraph 1 of this Article shall have the Certificate with the TOP SECRET degree of secrecy or one degree of secrecy higher than the highest degree of secrecy of classified data that are processed, stored or transmitted in the information systems under their competence.

(4) Measures of physical protection of facilities where information systems are located shall be taken in accordance with the highest degree of secrecy of classified data that are processed, stored or transmitted in the said facilities.

(5) NSA and NCSA shall form the registry of certified equipment and machines used in the information system of the CONFIDENTIAL, SECRET and TOP SECRET degree of secrecy. Registry of certified equipment and machines shall be formed on the basis of taking over the appropriate registers of international organizations or by own certifying process in accordance with relevant international norms.

Industrial Security

Article 13

(1) Industrial security is the information security area where stipulated information security measures and standards are applied for tenders or contracts with classified documentation which are binding for legal and natural persons referred to in Article 1, paragraph 3 of this Act.

(2) Legal and natural persons that take part in the tender or contract referred to in paragraph 1 of this Article shall obtain the Industrial Security Clearance (Certificate).

(3) Legal and natural persons referred to in paragraph 1 of this Article shall apply determined information security measures and standards for designated classified data degree of secrecy for their personnel, objects and facilities.

(4) Bodies and legal persons referred to in Article 1, paragraph 2 of this Act are authorised to submit requests for the issuance of Industrial Security Certificates for legal and natural persons whom they deliver classified data of CONFIDENTIAL, SECRET and TOP SECRET degree of secrecy.

(5) Legal and natural persons who take part in international jobs which require the Industrial Security Certificate are authorised to submit requests for the Certificate issuance.

(6) NSA is Designated Security Authority (DSA) which shall issue Industrial Security Certificate.

IV NATIONAL SECURITY AUTHORITY AND NATIONAL COMMUNICATIONS SECURITY AUTHORITY

Office of the National Security Council

Article 14

The Office of the National Security Council is the National Security Authority (NSA) that coordinates and harmonizes adoption and implementation of information security measures and standards in the Republic of Croatia and in exchange of classified and unclassified data between the Republic of Croatia and foreign countries and organizations.

Article 15

(1) The Office of the National Security Council shall adopt the Ordinance on Personnel Security standards, Ordinance on Physical Security standards, Ordinance on standards of Security of Information, Ordinance on INFOSEC organisation and management standards and Ordinance on Industrial Security standards.

(2) The Office of the National Security Council shall permanently harmonize stipulated information security measures and standards in the Republic of Croatia with international information security standards and recommendations and shall take part in the national standardization of the information security area.

Article 16

(1) The Office of the National Security Council shall coordinate and harmonize the work of bodies and legal persons referred to in Articles 17, 20, 23 and 25 of this Act.

(2) The Office of the National Security Council shall cooperate with competent foreign institutions and organizations in the information security area and shall coordinate the international cooperation of other bodies and legal persons referred to in paragraph 1 of this Article.

The Information Systems Security Bureau

Article 17

(1) The Information Systems Security Bureau is the NCSA for bodies and legal persons referred to in Article 1, paragraph 2 of this Act.

(2) Technical areas of information systems security are as follows:
- information systems security standards
- information systems security accreditations
- managing crypto materials used in the exchange of classified data
- coordination of prevention and response to security threats to information systems security

Article 18

(1) Information Systems Security Bureau shall use Ordinance to regulate standards for technical areas of information systems security referred to in Article 17, paragraph 2 of this Act.

(2) Information Systems Security Bureau shall permanently coordinate standards for technical areas of information systems security in the Republic of Croatia with international standards and recommendations and shall take part in the national standardization of information systems security areas.

Article 19

Information Systems Security Bureau shall do the work of security accreditation of information systems in cooperation with the Office of the National Security Council.

V NATIONAL CERT

Article 20

(1) CERT is the national authority competent for prevention and protection from computer threats to public information systems in the Republic of Croatia.

(2) CERT is a separate organizational unit that shall be established within the Croatian Academic and Research Network (hereinafter: CARNet).

(3) CERT shall harmonize procedures in case of security computer incidents in public information systems occurring in the Republic of Croatia or in other countries and organizations when they are related to the Republic of Croatia.

(4) CERT shall harmonize the work of the bodies that are working on the prevention and protection from computer threats to public information systems security in the Republic of Croatia and shall determine the rules and modes of joint performance.

Article 21

CERT and the Information Systems Security Bureau shall cooperate on the prevention and protection from computer threats to information systems security and shall take part in the making of information systems security recommendations and standards in the Republic of Croatia.

Article 22

The Director of CARNet shall appoint the Assistant competent for managing CERT.

VI INFORMATION SECURITY IMPLEMENTATION

Article 23

(1) Bodies and legal persons referred to in Article 1, paragraph 2 of this Act shall apply the information security measures and standards referred to in Article 7 of this Act.

(2) In bodies and legal persons who do not have the appropriate computer and technical means the measures and standards referred to in paragraph 1 of this Article shall be applied by the central state administration authority competent for information systems development (Communication and information systems Planning and Implementation Authority).

(3) Within the educational and academic sector the measures and standards referred to in paragraph 1 of this Article shall be applied by the central state authority competent for science and education (Communication and Information Systems Planning and Implementation Authority).

Article 24

(1) Bodies and legal persons referred to in Article 1, paragraph 2 of this Act shall determine the implementation of information security measures and standards by Ordinance.

(2) Central state administration authorities referred to in Article 23, paragraphs 2 and 3 of this Act shall determine the way of implementing information security measures and standards in other bodies by Ordinance.

VII INFORMATION SECURITY OVERSIGHT

Article 25

(1) The works of information security oversight are the works of oversight of organization, implementation and effectiveness of stipulated information security measures and standards in bodies and legal persons referred to in Article 1, paragraph 2 of this Act.

(2) The works of oversight referred to in paragraph 1 of this Article shall be implemented by information security advisors.

(3) The Office of the National Security Council shall adopt the Ordinance to stipulate criteria for forming the positions of information security advisors referred to in paragraph 2 of this Article

Article 26

(1) Information security advisor shall submit their report on the results of implemented oversight to the Head of body or legal person and to the NSA.

(2) NSA, based on the report referred to in paragraph 1 of this Article, is authorised to:
- give instructions for the purpose of eliminating determined defects and irregularities that the bodies and legal persons under oversight must eliminate within the designated period of time
- implement the procedure of assessment of the further validity of information systems security accreditation
- implement the procedure of determining responsibility
- take other measures and actions for which it has authorisation by separate provisions.

(3) The Head of the body or legal person shall take measures for eliminating defects determined during the oversight implementation

VIII TRANSITIONAL AND FINAL PROVISIONS

Article 27

The Regulation referred to in Article 7 of this Act shall be adopted by the Government of the Republic of Croatia within 3 months from the date when this Act enters into force.

Article 28

(1) The Ordinances referred to in Article 15, paragraph 1 of this Act shall be adopted by the Office of the National Security Council within 6 months from the date when this Act enters into force.

(2) The Ordinance referred to in Article 25, paragraph 3 of this Act shall be adopted by the Office of the National Security Council within 6 months from the date when this Act enters into force.

(3) The Ordinance referred to in Article 18, paragraph 1 of this Act shall be adopted by the Information Systems Security Bureau within 30 days from the day when the Ordinance referred to in paragraph 1 of this Article enters into force.

Article 29

(1) CARNet shall harmonize its Statute and deliver it to the Office of the National Security Council for approval within 3 months from the date when this Act enters into force.

(2) The Ordinances referred to in Article 24, paragraphs 1 and 2 of this Act shall be adopted within 9 months from the date when this Act enters into force.

Article 30

This Act shall enter into force 8 days following its publication in the Official Gazette.

Class: 650-05/07-01/01
Zagreb, 13 July, 2007

THE CROATIAN PARLIAMENT

The President of the Croatian Parliament

Vladimir Šeks, m.p.