Pursuant to Article 7 of the Information Security Act (Official Gazette 79/2007), the Government of the Republic of Croatia, at its session on _____ 2007, adopted the following

REGULATION

ON INFORMATION SECURITY MEASURES

I BASIC PROVISIONS

Article 1

This Regulation establishes the information security measures stipulated for handling classified and unclassified information.

This Regulation applies to state authorities, local and regional self-government bodies and legal persons with public authority who, in their respective scope of work, use classified and unclassified information.

This Regulation applies to natural and legal persons who gain access to or handle classified and unclassified information.

Article 2

Classified information shall need protection as long as being classified with one of the classification degrees, regardless of its shape, format or medium.

Article 3

Information classified with higher classification degrees (hereinafter: accountable information) are information classified as TOP SECRET, SECRET and CONFIDENTIAL.

Access to accountable information may be granted solely to the person who is briefed on the standards of classified information handling, who has need-to-know and who has the appropriate Personnel Security Clearance (hereinafter: Certificate).

Access to information classified as RESTRICTED may be granted to the person who is briefed on the standards of classified information handling and who has need-to-know.

Article 4

Authorization to access classified information shall be given by the head of authority or legal person where the person to access classified information is employed, or the persons appointed by the head in writing, for that purpose only, within their respective scope of work.

No person shall have the right to access classified information based solely on their rank, function or Certificate.

Article 5

Classified information may be delivered to other bodies only with the prior consent of the originator and in accordance with the requests referred to in Chapter VI of this Regulation and the Ordinance on information security standards.

Classified information originator has the right of control of classified information delivered to other authorities.

Article 6

Classified information may be forwarded only to the countries and international organizations that have signed the Security Agreement with the Republic of Croatia or have given the security guarantee for the protection of classified information to the Republic of Croatia, evidence of which shall be kept by the Office of the National Security Council.

Article 7

Classified information shall be protected by a group of security measures which include security vetting, physical protection, security of information and INFOSEC measures and they shall be applied to all persons who have classified information access, to all media where information are stored or transmitted, and to all facilities where classified information are handled, processed and stored.

Article 8

Unclassified information is used for official purposes and does not have the determined classification, may be without any classification marking or classified as UNCLASSIFIED, regardless of its shape, format or medium.

Unclassified information without any marking shall not have any restrictions in usage and access of persons.

Information classified as UNCLASSIFIED shall be used only for official purposes and may be made available only to the persons, bodies and organizations that have need-to-know.

Every information delivered to the Republic of Croatia by another country, international organization or institution that the Republic of Croatia cooperates with, and is UNCLASSIFIED, or classified with the equivalent foreign marking in accordance with the international agreement that the Republic of Croatia has signed, shall be used only for official purposes and may be made available only to the natural persons, bodies and legal persons that have the need-to-know.

II INFORMATION SECURITY MEASURES

Article 9

Bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation for the implementation of requirements referred to in this Regulation, Acts and Sub-Acts shall establish the appropriate information security programs which shall ensure the implementation of basic security principles and minimum criteria for the protection of classified and unclassified information, in order to guarantee the equal level of protection of all classified and unclassified information in the Republic of Croatia.

Article 10

For the protection of unclassified information legal and natural persons referred to in Article 1 paragraph 2 of this Regulation shall determine and implement the appropriate security measures with the purpose of ensuring the necessary confidentiality, integrity and availability of unclassified information, and in accordance with the international standards for information security management, which have been established in the Republic of Croatia as Croatian HRN ISO/IEC 27001 and HRN ISO/IEC 17799 standards.

III RESPONSIBILITIES IN THE INFORMATION SECURITY AREA

The Office of the National Security Council

Article 11

The Office of the National Security Council in the information security area, except for the responsibilities laid down by the law, is also responsible for:

- preparation and harmonization of bilateral and multilateral security agreements that the Republic of Croatia signs with other countries and international organizations;
- protection of national classified and unclassified information and classified and unclassified information of other countries and international organizations delivered to the Republic of Croatia, or respective state authorities of the Republic of Croatia;
- establishment and disestablishment of the registry system for the exchange of classified information with other countries and organizations, especially NATO and the EU;
- coordination of national measures of classified information handling in emergency situations by issuing the requirements to all bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation for making their own contingency plans
- coordination of behavior in case of destruction, unauthorized disclosure, compromise or possible compromise of classified information, with the originator of information in the Republic of Croatia or any other country or international organization, and with the competent authorities and institutions in the information security area and the investigative bodies in the Republic of Croatia;
- coordination and oversight of the information security measures and standards in the Industrial Security area

Information Systems Security Bureau

Article 12

The Information Systems Security Bureau in the information security area, except for the responsibilities laid down by the law, is also responsible for:

- control of cryptographic technical information related to the protection of national classified information and classified information exchanged with other countries and international organizations, especially with NATO and EU;
- managing cryptographic material for classified information systems and for the purpose of the exchange of classified information with other countries and international organizations, at the same time ensuring the implementation of the appropriate cryptographic procedures, secure handling, storage and distribution of all cryptographic material;
- defining the subjects in bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation who use cryptographic procedures in the exchange of classified information, responsible for the protection of necessary communication channels, systematic control of cryptographic communication and storage of information on all active communication channels;
- cooperation with the appropriate international bodies competent for security accreditation of classified systems and with bodies competent for cryptographic tasks, which shall be implemented in coordination with the Office of the National Security Council

National Authority for the Prevention and Protection from Computer Threats to Public Information Systems Security in the Republic of Croatia (National CERT)

Article 13

National CERT in the information security area, except for the responsibilities laid down by the law, is responsible for the harmonization of its work with the provisions stipulating the information security area

IV INFORMATION SECURITY MEASURES FOR PERSONNEL SECURITY

Personnel Security Measures

Article 14

Title IV of this Regulation stipulates the minimum information security measures for Personnel Security and Certificate issuance, which shall be implemented along with the minimum measures stipulated by this Regulation, Acts and Sub-Acts.

The standards for the implementation of measures referred to in paragraph 1 of this Article shall be stipulated by the Ordinance on personnel security standards.

Article 15

The Ordinance on personnel security standards shall stipulate the criteria for the evaluation of trustworthiness and reliability for the Certificate issuance, the requirements for security vetting procedure for the Certificate issuance for accountable information access, requirements for Certificate issuance for individuals, requirements for Certificate renewal, procedures related to negative information for persons who are Certificate holders, managing the registry of Certificates issued, the conditions for classified information access in emergency situations.

Security briefing

Article 16

All persons who have access to classified information within their scope of work shall periodically, and least once a year, undergo security briefing on stipulated information security measures and standards and shall sign the Statement on classified information handling.

Article 17

Security briefing of persons to access accountable information shall be performed by the authorized employees of the Office of the National Security Council, and they shall keep the appropriate records thereof.

Security briefing of persons to access information classified as RESTRICTED shall be performed by information security advisors in bodies and legal persons or other security coordinators appointed by the bodies and legal persons, and they shall keep the appropriate records thereof.

The Office of the National Security Council shall train the information security advisors and security coordinators referred to in paragraph 2 of this Article.

Managing Certificate Registry

Article 18

The Office of the National Security Council shall manage the national registry of all Certificates issued, decisions on Certificate denied and signed statements on classified information handling.

Article 19

Bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation, which handle accountable information, shall manage the registry of Certificates received and the registry of signed statements on handling information classified as RESTRICTED.

V INFORMATION SECURITY MEASURES FOR PHYSICAL SECURITY AREA

Article 20

Title V of this Regulation stipulates minimum information security measures for physical security area, which shall be implemented along with the minimum measures stipulated by this Regulation, Acts and Sub-Acts.

Standards for the implementation of measures referred to in paragraph 1 of this Article shall be stipulated by the Ordinance on physical security standards.

Minimum Physical Security Measures

Article 21

Each body and legal person referred to in Article 1, paragraph 2 of this Regulation which handle classified information shall implement the stipulated minimum physical security measures which shall ensure the equal degree of protection of all classified and unclassified information in the Republic of Croatia.

Article 22

All locations, buildings, offices, facilities and other areas where classified information are stored or handled shall be protected with the appropriate physical security measures.

Article 23

In determining physical security measures the classification degree should be taken into consideration, as well as the quantity and the form of classified information, the authorizations for classified information access and Certificate holders, security assessment of possible threats (espionage, sabotage, terrorism, subversive or any other criminal activities) and the manner of storage of classified information.

Article 24

Physical security measures shall be implemented in order to prevent unauthorized or violent entry of an intruder, deter, impede and detect actions by disloyal personnel, allow for segregation of personnel in accordance with the need-to-know principle and to detect and act upon all security breaches as soon as possible.

Article 25

Physical security measures are a form of protection that shall be implemented along with the security of information protection measures, INFOSEC measures and personnel security measures.

Security risk management shall include the establishment of efficient methods of countering threats, and securing the facilities where classified information are handled by the combination of protective measures from security areas referred to in paragraph 1 of this Article.

Article 26

Physical security measures shall be implemented on the basis of the “defence-in-depth” principle through:

- identifying the location that requires protection;
- creating layered security measures that provide “defence-in-depth” and delaying factors;
- establishing outermost physical security measures that define the protected area and deter unauthorized access;
- establishing measures that detect unauthorized or attempted access and alert the guard force;
- creating the innermost level of measures which sufficiently delays intruders until they can be detained by the guard force;
- creating interrelationship between the reaction time of the guard force and the physical security measures that are designed to delay intruders,

Article 27

Re-evaluation of the effectiveness of physical security measures and the complete security system shall be done periodically, in particular if there is a change in use of the protected location or elements of the security system.

Security Areas

Article 28

Areas where accountable information are handled or stored shall be structured as Class I Security Area (SA I) or Class II Security Area (SA II).

Class I Security Area (hereinafter: SA I) is an area where accountable information is handled and stored and shall have:

- a clearly defined and protected perimeter through which all entry and exit is controlled,
- an entry control system which admits only those persons appropriately cleared and specifically authorized to enter the area,
- specification of the classification level and the category of information held in the area.

Class II Security Area (hereinafter SA II) is an area where accountable information is handled and stored, in such a way that it can be protected from access by unauthorized persons by controls established internally, and it shall have:

- a clearly defined and protected perimeter through which all entry and exit is controlled,
- an entry control system which admits unescorted access only to those persons who are security cleared and specifically authorized to enter the area, while for all other individuals provision shall be made for escorts or equivalent controls , to prevent unauthorized access to classified information and uncontrolled entry to technically secure areas referred to in Article 36 of this Regulation.

Article 29

Security areas that are not occupied by duty personnel on a 24-hour basis shall be inspected immediately after normal working hours to ensure that classified information is properly secured.

Article 30

Permanently employed personnel shall be checked at the entrance to SA I and SA II by inspecting their official ID or pass, or by the appropriate personal recognition system.

The visitors shall, upon the inspection of personal information and the reason of entry, be authorized to enter only SA II if escorted.

Administrative Zones

Article 31

An Administrative Zone may be established around or leading up to SA I or SA II, and it shall have a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles.

Only UNCLASSIFIED information and information classified as RESTRICTED shall be handled and stored in Administrative Zones.

Special Physical Security Measures

Article 32

Elaborate shall be made for each facility or area that requires protection by physical security measures, and it shall determine the necessary physical security measures such as perimeter fence, Intrusion Detection System (hereinafter: IDS), access control, guards, Closed Circuit Television (hereinafter: CCTV) and security lightning.

Article 33

Bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation shall perform periodical entry and exit visitor controls unannounced in order to prevent entry of unwanted or unauthorized material or unauthorized exit of classified information form the facility or area.

Minimum Physical Security Measures for Classified Information Storage

Article 34

Information classified as TOP SECRET shall be stored within a SA I or SA II under the following conditions:

- in an IDS equipped security container under constant protection and periodical control, or
- in an IDS equipped open storage area that shall be organized in accordance with the provisions of the Ordinance on physical security standards

Information classified as SECRET shall be stored within a SA I or SA II under the following conditions:

- in the same way as information classified as TOP SECRET, or
- in a specially approved security container, or
- in an open storage area which is either IDS equipped or under constant protection and periodical control.

Information classified as CONFIDENTIAL shall be stored within a SA I or SA II in an appropriate security container or in the same way as the information classified as TOP SECRET or SECRET.

Information classified as RESTRICTED shall be stored in an appropriate locked office container.

Protection against Technical Attacks

Article 35

Facilities or areas where information classified as TOP SECRET or SECRET is handled shall be protected against passive and active eavesdropping attacks, by means of sound physical security measures and access control.

The Office of the National Security Council shall determine the risk of technical eavesdropping and the necessary physical security measures in coordination with the competent security and intelligence agency.

Technically Secure Areas

Article 36

Facilities or areas referred to in article 35 of this Regulation which require protection from eavesdropping shall be designated as technically secure areas and entry to them shall be specifically controlled.

Technically secure areas, when not used, shall be locked and guarded in accordance with physical security standards and any keys shall be treated as security keys, and such areas shall be subject to regular physical and technical inspection in accordance with the Ordinance on physical security.

Minimum Physical Security Measures for Communication and Information Systems

Article 37

Areas where accountable information are used, stored or transmitted using communication and information systems shall comply with the standards that ensure the confidentiality, integrity and availability of classified information and shall be constructed as SA I or SA II.

Facilities where providers, information systems communication and management equipment is located shall be SAI or SA II.

Areas where UNCLASSIFIED information and information classified as RESTRICTED are used, stored or transmitted using communication and information systems may be constructed as Administrative Zones.

Approved Equipment

Article 38

The Office of the National Security Council shall determine the list of approved equipment for the protection of classified information in different specific conditions and circumstances, based on the appropriate list of equipment and standards by international organizations, in accordance with national and international standards.

VI INFORMATION SECURITY MEASURES FOR THE SECURITY OF INFORMATION AREA

Article 39

Title VI of this Regulation stipulates the minimum information security measures for the security of information area, which shall be implemented along with the minimum measures stipulated by this Regulation, Acts and Sub-Acts.

Standards for the implementation of measures referred to in paragraph 1 of this Article shall be stipulated by the Ordinance on security of information standards.

Classification and Markings

Article 40

The classified information originator shall during classification explain in writing the classification degree. The originator shall do the same during periodical assessment of classification.

Article 41

The classified information originator is authorized to alter the classification or agree to declassification of classified information.

The originator of classified information shall during classification, when possible, indicate the earliest date or event when classification may be altered or information agreed for declassification.

Article 42

Security classification indicates the type of physical security measures which shall be applied when disseminated, transmitted, handled, stored or destructed.

In order to ensure the security and effectiveness classification shall be done in accordance with the actual requirements of classified information protection.

Article 43

In order to protect classified information the originator shall permanently review the classification in accordance with the law.

Periodical assessment shall not be done in case when the originator has predetermined that a specific classification shall be automatically downgraded after a designated period.

The originator shall inform in writing all the recipients on the changes in classification of information or its declassification.

Article 44

Individual pages, paragraphs, extracts, enclosures or annexes to classified information shall be, where possible, classified differently if they shall be used and distributed separately. The overall security classification of a document shall be at least as high as that of its most highly classified component.

Article 45

When classified information from various sources is collated, the product shall be reviewed for overall security classification since it may warrant a higher classification than its component parts.

The original security classification caveat of each part of classified document shall be retained when information is used to prepare composite documents.

In case parts of classified documents referred to in paragraph 2 of this article were originated by a foreign country or international organization the provisions of Article 121 of this Regulation shall apply.

Article 46

The originator may apply a Dissemination Limitation Marking, if deemed necessary; to further limit the dissemination of classified information.

Article 47

Classification and other markings on classified information may, for the purpose of the exchange of classified information with another country or international organization, be used in accordance with stipulated markings of another country or international organization with which the Republic of Croatia has signed the Security Agreement on mutual protection of classified information.

Objectives of Accountable Information Records

Article 48

All users shall keep accountable information records stipulated by the Ordinance on security of information standards.

Article 49

Accountable information records shall ensure enough data on classified information and persons who had access to it, so that in case of an investigation all facts related to the damage due to unauthorized usage, publishing or loss may be determined.

Accountable information records shall ensure, within the body or legal person referred to in Article 1, paragraph 2 of this Regulation, the following:

- maintaining an up-to-date record of access to classified information – all persons who are authorized to access, who might have had access, or who had access to classified information, or the persons who have attempted to access classified information;
- designated location of classified information at any given moment;
- maintaining an up-to-date record of all information held or circulating inside the body or towards other bodies and legal persons – information users from the outside.

Registry System

Article 50

Registry system for the exchange of classified information with other countries and international organizations, especially NATO and EU, is comprised of:

- the Central Registry at the Office of the National Security Council,
- sub-registries of the Central Registry in bodies that are the major users of classified documents, and
- registries within other bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation.

Article 51

Registries shall be formed in coordination with the Office of the National Security Council for the internal distribution of classified information within bodies referred to in Article 1, paragraph 2 of this Regulation and they shall be responsible for keeping records of classified information within the said bodies.

The Central Registry with sub-registries and registries within the bodies referred to in article 1, paragraph 2 of this Regulation shall know at any time where accountable information is located.

Registries shall not be formed for the purpose of occasional access to classified information under the condition that the measures and standards of classified information protection laid down by the law, this Regulation and the Ordinance on security of information standards are implemented and that such information is under
constant control of the registry system.

Article 52

Security accreditation of the Central Registry, sub-registries and registries in state bodies is the procedure whereby it is determined whether the facility is properly equipped and whether the personnel of the bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation who are supposed to work in the registry system and handle classified information is capable, and this shall be done by identifying the implemented information security measures and standards.

The Office of the National Security Council shall perform the security accreditation of the Central Registry, sub-registries, and registries within the state bodies, and shall issue the certificate which approves the work and designates the highest classification of the information that can be handled, depending on the format, shape and medium of the classified information.

The Office of the National Security Council shall periodically review the accreditation referred to in paragraph 2 of this Article, and at least every 2 years.

The Office of the National Security Council shall adopt the Instruction on information security measures and standards for the registry system in order to implement the stipulated information security measures and standards.

Article 53

Information classified as TOP SECRET shall be distributed within the registry system on the condition that the sub-registries and registries concerned are accredited for handling TOP SECRET information.

The bodies shall designate a Control Officer for handling TOP SECRET information. The duties and responsibilities of the Control Officer shall be stipulated by the Ordinance on security of information standards.

Article 54

The Information Systems Security Bureau shall be in charge of establishing a separate registry for recording, control and distribution of cryptographic material and the information that are transmitted in this way do not have to be recorded through the registry system.

Handling Classified Information in Emergency Situations

Article 55

Requirements for handling classified information in emergency situations in order to prevent unauthorized access, disclosure or loss of classified information shall be stipulated by the Ordinance on security of information standards.

In accordance with the requests referred to in paragraph 1 of this Article all bodies and legal persons which handle classified information shall make contingency plans for the protection, evacuation and destruction of classified information in emergency situations.

Security Breaches

Article 56

In case of destruction, disclosure or compromise of classified information the originator shall take all necessary measures in order to remove or reduce any damage, in order to initiate the legal proceedings and to inform the Office of the National Security Council.

In case the destruction, disclosure or compromise of classified information has occurred within a body which is the user of the information, the competent person within that body shall without any delay inform the originator who will then initiate the procedure referred to in paragraph 1 of this Article, in cooperation with the user and shall inform the Office of the National Security Council.

Classified information lost, even temporarily, inside a security area, including that which cannot be located at periodic inventories, shall be presumed compromised until investigation proves otherwise.

Article 57

Where security breach happened in relation to classified information originated by another country or international organization, the Office of the National Security Council shall inform the competent body of another country or international organization thereof.

Article 58

The Office of the National Security Council may, where deemed necessary, ask the originator and competent bodies to start further investigation and deliver reports thereof.

Article 59

The Information Systems Security Bureau shall stipulate the procedures, records and reports of security breaches and compromises of cryptographic material.

Dissemination of Classified Information to Another Country or International Organization

Article 60

The bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation may give the classified information from their competence to another country or international organization with which the Republic of Croatia has signed the Security Agreement on mutual classified information protection, under the following conditions:

- there is a mutually agreed cooperation program in the designated area between the bodies in the Republic of Croatia and other countries and international organizations, which include the exchange of classified information;
- within the framework of registry system for the exchange of classified document separate records shall be kept on exchanged classified information within the cooperation program referred to in indent 1 of this Regulation;
- bodies and legal persons shall periodically report to the Office of the National Security Council on every cooperation program referred to in indent 1 of this paragraph, and at least once a year.

VII INFORMATION SECURITY MEASURES FOR THE INFOSEC AREA

Article 61

Title VII of this Regulation stipulates minimum information security measures for the INFOSEC area, for the purpose of protection of classified and unclassified information and respective services and resources in information systems where classified information are processed, stored or transmitted, or where classified information are used, in accordance with this Regulation, Acts and sub-Acts.

The standards for the implementation of measures referred to in paragraph 1 of this Article shall be stipulated by the Ordinance on INFOSEC organization and management standards.

Security Objectives

Article 62

For the protection of classified information which are used in the information systems sound security measures shall be identified and implemented, which are stipulated by this Regulation concerning physical security, personnel security, security of information and INFOSEC areas, with the purpose of ensuring:

- confidentiality of classified information by the control of unauthorized access and disclosure, and by the additional information systems services and resources;
- integrity of classified information, and the additional information systems services and resources;
- availability of classified information and the additional information systems services and resources.

For the protection of unclassified information used in the information systems the following security standards HRN ISO/IEC 27001 and HRN ISO/IEC 17799 standards shall be identified and implemented, in accordance with Article 10 of this Regulation.

Article 63

The integrity and availability of classified information and the additional information systems services and resources shall be protected by the minimum measures and standards for classified information protection with the purpose of securing general protection from usual problems in information systems, regardless of being intentional or accidental, and which are known to affect all information systems and their additional services and resources.

In case when security risk assessment in certain environment has shown that classified information and/or additional services and resources are under increased risk of specific threats and vulnerabilities, additional protective measures and standards shall be taken.

Security Accreditation of Information Systems

Article 64

Security accreditation of information systems is the procedure whereby the capability of the bodies and legal persons referred to in Article 1 paragraph 2 of this Regulation is determined for managing information systems security, and it is done by identifying the implemented information security measures and standards.

The bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation shall by security requirements determine the security objectives which must be accomplished, and the necessary degree of the protection of classified information and the additional information systems services and resources.

The security accreditation process shall determine whether the necessary level of protection has been accomplished and whether it is permanently maintained.

Article 65

The Information Systems Security Bureau shall accredit all information systems where classified information is used, in order to determine the security objectives of confidentiality, integrity and availability.

The bodies which use information systems for unclassified information shall perform at least the internal assessment of such information system in order to determine security objectives of confidentiality, integrity and availability, which can be performed by the information security advisor in bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation.

Unclassified information system referred to in paragraph 2 of this Article may be used for information classified as RESTRICTED, only on the condition that it was prior certified in accordance with the international standards for information security management system, stipulated in the Republic of Croatia as HRN ISO/IEC 27001, and on the condition of implementation of the appropriate measures and standards stipulated by this Regulation and Ordinances.

The Information Systems Security Bureau shall determine the conditions for information classified as RESTRICTED referred to in paragraph 3 of this Article.

On the proposal of the Information Systems Security Bureau, and in accordance with other conditions set in the Title X of this Regulation, the Office of the National Security Council shall give their consent for the security accreditation of the information system referred to in paragraph 1 of this Article, and shall confirm the evaluation of conditions referred to in paragraph 4 of this Article.

Personnel Security

Article 66

Persons who are authorized access to additional information systems services and resources or who are in charge of their protection and maintenance, even if they are not authorized to access the information used in the system shall have the TOP SECRET Certificate or a level above of the highest classification of information that are processed, stored or transmitted in the information systems under their competence.

Security of Computer Storage Media

Article 67

All classified computer storage media shall be properly identified, stored and protected in accordance with the highest classification of the information stored on the said media.

Article 68

Classified information on computer storage media which can be re-used, shall be erased in accordance with the procedures stipulated by the Information Systems Security Bureau.

Information Systems Records

Article 69

Procedures shall be established within the information systems which shall ensure enough information for investigation on intentional or accidental compromise of confidentiality of accountable information, and commensurate with the resulting damage it shall provide enough information on intentional or accidental compromise of integrity and/or availability of classified information and all additional information systems services and resources

Security Measures in Information Systems

Article 70

The stipulated security measures shall be implemented for all information systems where classified information is used in order to meet the security objectives and protect the classified information and the additional information systems services and resources, and it shall include:

- measure for trustworthy identification and verification of integrity of the persons who have authorized access, whereby the information and equipment controlling the access to an information system are controlled and protected in accordance with the measures and standards stipulated for the classification of information to which access is enabled;
- measure for unauthorized access control and access to classified information and additional information systems and resources based on the need-to-know principle;
- measure for the identification of integrity and origin of classified information and the additional information systems and resources;
- measure for the maintenance of integrity of classified information and the additional information systems services and resources;
- measure for the maintenance of availability of classified information and the additional information systems services and resources;
- measure for the control over the connections of information systems which process classified information;
- measure for the evaluation of trust in the protective security mechanisms of information systems;
- measure for the evaluation and confirmation of the proper functioning of the protective security mechanisms of the information system during its life cycle;
- measure for the control and investigation of the activities of information system users.

Article 71

Measures of security in information systems shall be implemented in order to deter, prevent, detect and recover from the effects of incidents affecting the confidentiality, integrity and availability of classified information and the additional information system services and resources, and shall include reports on security incidents.

Security Risks Management

Article 72

Security verification and security risks management shall be performed in information systems where classified information is used, in accordance with the provisions of this Regulation and Ordinances.

Electromagnetic Transmission of Classified Information

Article 73

Special measures for the protection of confidentiality, integrity and availability of classified information shall be implemented during electromagnetic transmission of the said information.

Article 74

When cryptographic methods are necessary for the protection of confidentiality, integrity and availability of classified information, such methods and similar products shall be specially authorized.

Article 75

Confidentiality of all classified information shall be protected during the entire transmission period by cryptographic methods or products accredited by the Information Systems Security Bureau, unless otherwise provided by the international agreement between the Republic of Croatia and another country or international organization or unless a different procedure or a different body for the accreditation of cryptographic methods or products has been defined according to international standards.

Article 76

Integrity and availability shall be ensured during the transmission of the classified information in accordance with the communication system operative requests.

The Information Systems Security Bureau shall stipulate the evaluation of mandatory requests for the integrity and availability of cryptographic mechanisms along with the specifications of the said mechanisms in their operative conditions.

Article 77

In extraordinary circumstances information classified as SECRET, CONFIDENTIAL and RESTRICTED may be transmitted by open text, with the appropriate authorization.

Extraordinary circumstances may appear during actual or pending crisis, conflict or war, and when the speed of delivery is the most important factor, or when no cryptographic mechanism is available, and it is estimated that the sent information cannot, even in case it is discovered, be used to have negative effect on the operation in due time.

Security of Cryptographic Products, Equipment and Information

Article 78

The sensitive nature of cryptographic products, equipment and information which are used in order to protect the confidentiality, integrity and availability of classified information shall call for the implementation of special security measures.

Article 79

The protection of cryptographic methods, equipment and information shall be commensurate with the damage that might occur if the protection is not successful, therefore the way to evaluate the functioning of cryptographic products and equipment and the protection and control of cryptographic information shall be established.

Article 80

The Information Systems Security Bureau shall adopt special regulations for the purpose of managing the receipt, control and distribution of cryptographic information to authorized persons in bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation.

Article 81

The Information Systems Security Bureau shall adopt the Ordinance which will stipulate the procedures for the distribution of technical information, selection, production and procurement of cryptographic products and equipment.

Security from Unwanted Electromagnetic Transmission

Article 82

The measures for security from compromise of accountable information by unwanted electromagnetic transmission shall be commensurate with the risk from potential misuse of classified information and the classification of the said information.

VIII INDUSTRIAL SECURITY MEASURES

Article 83

Title VIII of this Regulation stipulates minimum information security measures for industrial security area, which shall be implemented along with the minimum measures stipulated by this Regulation, Acts and Sub-acts.

Standards for the implementation of measures referred to in paragraph 1 of this article shall be stipulated by the Ordinance on industrial security measures.

Article 84

The information security measures for industrial security shall be stipulated for negotiating and letting of classified contracts, security vetting for legal persons, security vetting of the facility employees, security requests for classified contracts, transportation of classified material, international visits and personnel on loan within projects or programs.

Negotiation and Letting of Classified Contracts

Article 85

Bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation during the negotiations for classified contracting shall compile the documentation for tender which shall contain only UNCLASSIFIED information or information classified as RESTRICTED.

Bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation shall sign the Agreement on mutual protection of classified information included in the bid process with the legal and natural persons referred to in Article 1, paragraph 3 of this Regulation.

Article 86

Legal and natural persons referred to in Article 1, paragraph 3 of this Regulation, which take part in classified contracts that include accountable information, shall have the appropriate Facility Security Clearance (hereinafter: FSC), and employees of the legal person who will have access to classified information shall have appropriate Certificate and shall be able to access only classified information that are a part of the classified contract and for which they have need-to-know.

FSC is not necessary for contracts classified as RESTRICTED, but employees of the legal person shall be security briefed and shall sign the Statement on handling classified information.

During the letting of contract classified as RESTRICTED the bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation shall sign an Agreement on mutual protection of classified information with the prime contractor, and its provisions shall apply to all sub-contractors, which is the responsibility of the main contractor.

Article 87

For the realization of the prime contract the prime contractor may negotiate sub-contracts with other legal and natural persons, and sub-contractors may negotiate sub-contracts with other legal and natural persons, in accordance with the provisions of Article 86 of this Regulation.

Facility Security Clearance

Article 88

Provisions of this Regulation shall apply for all prime contractors and sub-contractors of contracts which contain accountable information.

Article 89

The bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation are authorized to submit requests for the issuance of FSC for legal and natural persons for letting of contracts with accountable information. FSC shall include the security vetting of employees, facilities and business.

The request for the issuance of FSC shall be delivered to the Office of the National Security Council.

Article 90

Legal and natural persons referred to in article 1, paragraph 3 of this regulation, who take part in international business, are authorized to submit requests for the issuance of FSC, after the

issuance has been requested by the competent security authority of the country that is initiating the contract.

Article 91

The procedure of FSC issuance shall start with signing the Security Agreement between the Office of the National Security Council and the legal or natural person referred to in Article 1, paragraph 3 of this Regulation.

The Office of the National Security Council shall give the prime contractor or the sub-contractor the list of information security measures and standards which shall be implemented before the procedure is finished.

Article 92

The Office of the National Security Council shall determine whether every legal and natural person who will have access to accountable information has implemented the information security measures and standards mandatory for the FSC issuance.

The employees of legal persons or natural persons who need access to classified information shall have the Certificate and shall be security briefed before the issuance of FSC.

FSC shall be categorized depending on the classification, the number of classified information, the way of storage and transportation of classified information and the number of employees who should have classified information access for the realization of the contract.

Article 93

The assessment, which shall be made prior to FSC issuance, shall be in accordance with the security standards and criteria stipulated by the Ordinance on industrial security standards.

Personnel Security

Article 94

Issuance of Personnel Security Clearances (Certificate) for natural persons and employees of legal persons referred to in Article 1, paragraph 3 shall be done according to the provisions of Title IV of this Regulation and other Acts and Sub-Acts.

Article 95

The contractor or sub-contractor, who employs a foreign citizen on a position which requires classified information access, shall through the Office of the National Security Council ask for the delivery of the Certificate for the said person by the competent authority of the state whose citizen the said person is.

Security Requirements for Classified Contracts

Article 96

The main contractor and sub-contractors shall, according to the requirements of the security agreement and under the cancellation of the contract, implement all stipulated measures for classified information protection, as laid down by Article 91 of this Regulation, as provided by the contract or entrusted to the main contractor or embedded into products or services provided by the main contractor.

Article 97

During the letting of the main contract the bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation shall make, as an annex to contract, a Project Security Instruction (hereinafter: PSI) whose integral part is a Project Security Classification Guide.

All other classified contracts that are not related to main programs or projects, shall have the minimum of Security Aspect Letter, which may be a PSI reduced in scope.

Article 98

The classification of programs and projects related to the main contract and all sub-contracts shall be based on the Project Security Classification Guide.

Transportation of Classified Material

Article 99

During the transportation of classified material security shall be assured at all stages and under all circumstances, from the point of origin to the ultimate destination, and the classification of consignment shall be determined by the highest classification of the material contained in it.

Legal persons who transport accountable information shall have FSC, and the personnel handling consignments shall have valid PSC. Transportation shall be point-to-point to the extent possible, and shall be completed as quickly as circumstances permit.

Article 100

Transportation plans shall be made by the bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation, main contractor or sub-contractor who initiated the transportation of classified material.

The Office of the National Security Council shall approve the transportation plan and give its consent for the national and international transportation of classified material.

Transportation plans shall be made for each transportation separately, or for more transportations done in the short period, and shall contain measures for unauthorized access prevention.

Article 101

Security standards for the transportation of classified material shall be stipulated by the Ordinance on security of information standards, and detailed instructions for hand carriage, transportation by commercial carriers, guards and escorts and for the transportation of explosives, propellants or other dangerous substances shall be stipulated by the Ordinance on industrial security standards.

International Visit Procedures

Article 102

The Office of the National Security Council shall approve the visit of civil and military representatives of foreign countries and international organizations, as well as contractors and sub-contractors from foreign countries who take part in classified contracts, programs and projects, based on the information given by the competent authorities and the valid certificates delivered.

The bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation who are in charge of the program or projects which includes international visits, shall be in charge, along with their contractors and sub-contractors, for initiating the procedure with the Office of the National Security Council which shall include the information about the visit, and the exchange of valid certificates with the competent authority of the other country or international organization.

Article 103

The bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation, or the contractors and sub-contractors involved in programs and projects shall ensure that all provisions set in the Article 102 of this Regulation are met, shall enable visitors access to information related to the visit and shall keep the records of all international visitors.

Article 104

The bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation, or the contractors and sub-contractors who intend to send their employees on international visits, shall through the Office of the National Security Council apply to the competent authority of the country or international organization where the body or legal person they wish to visit is located in.

The request for international visit shall be in accordance with the provisions of the Ordinance on industrial security standards and shall contain the guarantee that all visitors have valid certificates.

Article 105

Visits, which are a part of RESTRICTED or UNCLASSIFIED programs or projects, may be agreed upon directly, without the intercession of the Office of the National Security Council.

Personnel on Loan within a Project or Program

Article 106

When a person who has been cleared to access classified information is to be loaned from one facility to another within the same program or project, but in a different country, the legal person referred to in Article 1, paragraph 3 of this Regulation where the person is employed, shall request the Office of the National Security Council to provide the Certificate to the competent security authority to the country where the person is to go.

The person referred to in paragraph 1 of this Article shall be briefed on the security standards during international visits, in accordance with the Ordinance on industrial security standards.

IX INFORMATION SECURITY RISK MANAGEMENT

Article 107

All bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation which handle classified information shall, along with the implementation of minimum security measures stipulated by this Regulation, Acts and Sub-Acts, perform the information security risk management procedures.

Risk management comprises of risk assessment, risk processing and current risk management activities.

Information Security Risk Assessment

Article 108

Information security risk assessment includes systematic risk analysis and risk evaluation process for classified information, and is comprised of identifying, qualifying and dividing risks by priority, by criteria for risk acceptance and security objectives.

The risk assessment results shall give the body or legal person indication of the appropriate risk protection measures, in accordance with the risk management priorities.

Risk assessment process and the choice of measures may be applied more times in order to encompass different organizational parts or separate information systems within the body or legal person.

Article 109

Risk assessment shall be done regularly in order to recognize the changes in security requests and risk circumstances in case of significant changes within the organization or environment, during which the risk assessment shall be done methodically in order for the results to be compared and processed.

Risk assessment shall have a clearly defined scope in order to be effective.

Risk Processing

Article 110

Before the risk processing the criteria for accepting risks shall be determined.

Article 111

For each risk recognized during the risk assessment the risk processing shall be defined:

- by the implementation of security measures for decreasing the risk to the level estimated acceptable,
- by conscious and objective risk acceptance, on the condition that the risk conforms to the information security principles and risk acceptance criteria,
- by avoiding the risk by avoiding the actions which would cause the risk,
- by transferring the risk to other sides, if possible, for example within the industrial security procedures.

Article 112

Security measures for decreasing risks to the acceptable level shall take into consideration the requests and restrictions of laws and international regulations, organizational objectives, operative requests and restrictions, implementation costs and security measures costs in relation to decreasing risks, while costs should be kept within the boundaries of organizational requests and restrictions, and the need to harmonize the investment into security measures application in relation to the potential damage which might occur as the result of failure.

Bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation shall continuously follow, evaluate and enhance the effectiveness of security measures in order to maintain the requested security requirements level.

Article 113

In case, after the risk processing, the remaining risk is deemed unacceptable, the decision on solving that situation shall be passed by additionally processing the remaining risk.

All remaining accepted risks shall be recorded and approved by the head of the body or legal person.

Current Risk Management Activities

Article 114

Results of risk assessment and risk management shall be regularly revised for internal and external changes and in accordance with the needs of the body or legal person.

The bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation shall keep risk assessment records which shall contain the date of the assessment, risk description, the assessment and probability of influence of each risk, security measures applied and the statement on necessary security measures with the designated person and the implementation deadline.

Article 115

After adopting the decision on risk processing the bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation shall make risk processing plan which shall determine and map out the implementation of the said decisions.

Article 116

The Office of the National Security Council shall adopt the Guidelines for information security risk management for bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation.

X INFORMATION SECURITY OVERSIGHT

Article 117

The Office of the National Security Council shall perform periodical oversight in all bodies and legal persons referred to in Article 1, paragraph 2 and 3 of this Regulation, which handle classified and unclassified information.

The oversight referred to in paragraph 1 of this Article shall be performed in bodies and legal persons that handle accountable information at least once every 18 months, and in bodies and legal persons which use RESTRICTED information at least once every 36 months.

Article 118

The oversight referred to in Article 117 of this Regulation shall be performed on multiple levels by:

- internal oversight performed by the information security advisor in bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation, and who will report to the Office of the National Security Council and the head of the body or legal person,
- classified information systems security accreditation performed by the Information Systems Security Bureau, who will report the results to the Office of the National Security Council,
- certifying information security system management or internal assessment of unclassified information systems performed by an independent authorized institution or information security advisor, who will report to the Office of the National Security Council,
- oversight directly performed by the information security advisors of the Office of the National Security Council in bodies and legal persons referred to in Article 1, paragraph 2 and 3 of this Regulation,
- oversight of cooperation programs referred to in Article 60 of this Regulation.

Article 119

The objective of the oversight referred to in Article 117 of this Regulation is to determine the implementation of stipulated information security measures and standards, especially the following:

- classification and declassification procedures,
- access to classified and unclassified information,
- measures for classified information access protection in all information security areas,
- information systems security accreditation,
- Personnel Security Clearance registry with their respective expiry dates and security briefing of personnel,
- implementation of provisions of international agreements on classified information protection of foreign countries and international organizations that the Republic of Croatia has signed, and especially for the protection of NATO and EU classified information.

Article 120

The report on the oversight shall be made by the Office of the National Security Council in writing and shall be delivered to the head of the body or legal person where the oversight was performed, or where the classified information registry is located.

The report referred to in paragraph 1 of this Article shall contain the instructions on the removal of defects and irregularities which the bodies and legal persons shall remove within the period set in the oversight report.

XI TRANSITIONAL AND FINAL PROVISIONS

Article 121

In case classified information handling, as stipulated by the Security Agreement on mutual protection of classified information with foreign country or international organization that the Republic of Croatia has signed, calls for the implementation of measures and standards that are more strict than the ones prescribed by Acts, Sub-Acts and this Regulation, the provisions of the Security Agreement shall apply.

Article 122

The bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation shall adopt the information security programme referred to in Article 9 of this Regulation, within 6 months from the day that this Regulation enters into force.

The bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation shall start implementing the provisions of this Regulation and the Ordinances referred to in Article 15 and 18 of the Information Security Act within 12 months from the date that this Regulation enters into force.

Article 123

Bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation may temporarily or permanently, for classified information storage or handling, use the facilities in accordance with the registry system measures and standards as laid down by the Article 50 to Article 54 of this Regulation and the Instruction on information security measures and standards for the registry system in state authorities which is adopted by the Office of the National Security Council.

The provisions of paragraph 1 of this Article may be permanently implemented for the bodies and legal persons who use a small number of classified information, while the same provisions may apply to other bodies and legal persons within the transitional period until the full enforcement of the provisions referred to in Article 122, paragraph 2 of this Regulation.

The Office of the National Security Council shall deliver the Instruction referred to in paragraph 1 of this Article and shall ensure the expert advice in the implementation of information security measures and standards, upon the written request of the user.

Article 124

The information systems in bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation may be used for classified information transmission only if they are properly security accredited.

The bodies and legal persons, who have, according to the provisions of the Act on Personal Data Protection (Official Gazette, 108/1996), set up their own information systems, shall within 24 months from the date that this Regulation enters into force security accredit the classified information systems in accordance with the provisions of this Regulation.

The bodies and legal persons referred to in paragraph 2 of this Article may, until the classified information systems are fully accredited, use the said systems only for the processing, transmission and storage of national classified information.

Article 125

The information systems in bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation may be used for unclassified information transmission in accordance with the provisions of Article 10 of this Regulation.

The provisions of paragraph 1 of this Article shall be implemented within 18 months form the date that this Regulation enters into force within the information security program referred to in Article 9 of this Regulation.

Article 126

The Ordinances referred to in Article 15 of the Information Security Act shall be UNCLASSIFED, shall not be published and shall be delivered upon the request of the bodies and legal persons referred to in Article 1, paragraph 2 of this Regulation.

The requests referred to in paragraph 1 of this Article, shall be delivered in writing to the Office of the National Security Council and shall contain the title of the Ordinance requested and the explanation of usage of the classified information within the body or the legal person.

Article 127

The Ordinance on organization standards and information systems security management referred to in Article 15 of the Information Security Act shall prescribe the content of the Ordinances for information systems security technical areas, and they shall be adopted by the Information Systems Security Bureau.

Article 128

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