THE GOVERNMENT OF THE REPUBLIC OF CROATIA

Pursuant to Article 7 of the Information Security Act (Official Gazette 79/2007), the Government of the Republic of Croatia, at its session on 18 April 2008, adopted the following

REGULATION

ON INFORMATION SECURITY MEASURES

I BASIC PROVISIONS

Article 1

(1) This Regulation establishes information security measures for handling classified and unclassified information.

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

(3) This Regulation applies to legal entities and persons that gain access to or handle classified and unclassified information.

Article 2

The terms in this Regulation have the following meaning:

- ***Hardware*** - physical component of a computer system
- ***Classified contract -*** contract the execution of which includes the exchange of classified information between the bodies and legal entities referred to in Article 1 paragraph 2 and the legal entities and persons referred to in Article 1 paragraph 3;
- ***Crypto materials*** - cryptographic products and information, that is, program solutions or equipment for information protection, technical documentation for such solutions and equipment, and the appropriate crypto keys;
- ***Data storage media*** - any medium on which data can be stored in electronic form;
- ***General protection level*** - set of measures and standards in information security areas stipulated for particular security classification levels;
- ***Security accreditation of a registry system*** - procedure whereby it is determined whether information security measures and standards stipulated for the organization of work, personnel, facilities, information systems and classified information are implemented in facilities where receipt, usage, storage and further distribution of classified information is organized;
- ***Security container*** - safe, vault and other anti-burglary equipped facilities for classified information storage;
- ***Software*** - all operating systems, programs, user and service applications;
- ***Threat*** - potential cause that may damage classified information or information system in which classified information is used;
- ***Information security risk management*** - systematic approach that includes planning, organizing and directing activities, with the aim of ensuring that the risks to classified

information are maintained within the framework established by law and deemed acceptable.

Article 3

(1) Classified information shall be protected by measures and standards stipulated for classified information protection, which ensure a general protection level for as long as it is classified with one of the security classification levels.

(2) When it is determined by means of security risk assessment that classified information is under increased risk, the bodies and legal entities shall implement the required additional measures and standards for the protection of that information pursuant to Article 96 of this Regulation.

Article 4

(1) Access to information classified as TOP SECRET, SECRET and CONFIDENTIAL may be granted only to a person holding an appropriate Certificate that has been security briefed and has a Need-to-Know based on list of duties and jobs for which a Certificate is required.

(2) Access to information classified as RESTRICTED may be granted to a person who has been security briefed and has a Need-to-Know based on the authorization for access to classified information by the head of the body or legal entity.

Article 5

Classified information may be delivered to other bodies and legal entities only with the prior consent of the originator and in accordance with the provisions of this Regulation and the ordinances adopted in accordance with law.

Article 6

(1) Classified information may be exchanged only with the states and international organizations that have signed agreements on mutual protection of classified information with the Republic of Croatia.

(2) By way of derogation from paragraph 1 of this Article, classified information may be exchanged with states and international organizations in the framework of international cooperation which includes the exchange of classified information.

(3) The records of the agreements referred to in paragraph 1 of this Article shall be kept by the Office of the National Security Council.

Article 7

(1) Information without any classification, when used for official purposes, may be either without classification marking or marked as UNCLASSIFIED.

(2) Information without any classification has no restrictions as to usage or access. Information marked as UNCLASSIFIED is used only for official purposes and may be available

only to those persons, bodies and legal entities that have a need to use such information for official purposes and have a Need-to-Know.

(3) Any information released to the Republic of Croatia by another country, international organization or institution with which the Republic of Croatia cooperates, that is UNCLASSIFIED or classified with the equivalent foreign classification in accordance with the international agreement signed by the Republic of Croatia, shall be used only for official purposes and may be made available only to persons, bodies and legal entities that have a need to use such information for official purposes and have a Need-to-Know.

Article 8

(1) Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall establish and implement an appropriate set of information security measures for the protection of unclassified information in accordance with the standards for information security management HRN ISO/IEC 27001 and HRN ISO/IEC 17799.

(2) In addition to the standards referred to in paragraph 1 of this Article, other measures stipulated by this Regulation, other regulations or international agreements shall be implemented for the protection of information classified as RESTRICTED.

(3) In addition to monitoring the implementation of the standards and measures referred to in paragraphs 1 and 2 of this Article, the Security Officer at the bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation, shall check on a regular basis whether the information system using unclassified information and information classified as RESTRICTED is harmonized with the stipulated norms, measures and information security standards.

Article 9

Bodies and legal entities handling classified and unclassified information shall implement the stipulated information security measures in order to ensure an equal level of protection for any classified or unclassified information in the Republic of Croatia.

Article 10

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.

II INFORMATION SECURITY MEASURES FOR THE AREA OF PERSONNEL SECURITY

Article 11

Information security measures for the area of Personnel Security are as follows:

- List of duties and jobs for which a Personnel Security Clearance (hereinafter: Certificate) is required;
- Procedure for Certificate issuance;
- Security Vetting Questionnaire;
- Written consent of the person undergoing the security vetting;
- Certificate issuance;
- Security briefing;
- National registry of the issued Certificates, decisions on the denied Certificates, and signed statements on classified information handling;
- Registry of the received Certificates and signed statements on classified information handling.

Article 12

All persons who have access to classified information shall be security briefed, at least once a year, on the stipulated information security measures and standards and shall sign a statement on classified information handling.

Article 13

(1) Security briefing of persons to access information classified as TOP SECRET, SECRET and CONFIDENTIAL shall be performed by the authorized persons from the Office of the National Security Council.

(2) The Office of the National Security Council may, for the jobs referred to in paragraph 1 of this Article, train the persons working in the registry system, security officers in bodies and legal entities, or other security coordinators designated by the bodies and legal entities.

(3) Security briefing of persons to access information classified as RESTRICTED shall be performed by security officers in bodies and legal entities or other security coordinators designated by the bodies and legal entities.

Article 14

(1) Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation handling information classified as TOP SECRET, SECRET and CONFIDENTIAL shall manage a registry of received Certificates and signed statements on classified information handling.

(2) Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation handling information classified as RESTRICTED shall manage a registry of signed statements on classified information handling.

III INFORMATION SECURITY MEASURES FOR THE AREA OF PHYSICAL SECURITY

Article 15

Information security measures for the area of Physical Security are as follows:
- Defense-in-Depth,
- Security Areas;
- Administrative Zones;
- Physical security plan;
- Assessment of physical security measures effectiveness;
- Control of persons;
- Storage of classified and unclassified information;
- Technically secure areas;
- Physical security of information systems;
- Equipment for the physical protection of classified information.

Article 16

Locations, buildings, offices, facilities and other areas where classified information is handled or stored shall be protected by the appropriate physical security measures.

Article 17

Physical security measures shall be implemented in order to:
- Prevent unauthorized or violent entry of an intruder;
- Deter, impede and detect misuse by personnel;
- Divide the personnel in accordance with their authorization for classified information access;
- Detect and respond to all security threats.

Article 18

Physical security measures shall be defined with regard to the classification, number, shape and means of storage of classified information, authorization for classified information access and security assessment of possible threats.

Article 19

Physical security measures shall be implemented together with the security of information measures, INFOSEC measures and personnel security measures.

Defense-in-Depth

Article 20

Physical security measures shall be implemented through Defense-in-Depth by means of:

- Identifying the location that requires protection;
- Establishing security measures for protection from and delaying unauthorized entry;
- Defining outer physical security measures;
- Establishing measures to detect unauthorized access attempts;
- Defining physical security measures in order to delay unauthorized access;
- Coordinating the time of response force arrival with the time of delaying unauthorized access.

Security Areas

Article 21

(1) Facilities where information classified as TOP SECRET, SECRET and CONFIDENTIAL is stored or handled shall be organized as Class I Security Area or Class II Security Area.

(2) Class I Security Area is a clearly marked and protected area with access controls and defined classification of information and categories of information held in that area.

(3) Access to Class I Security Area shall be allowed only to persons holding a Certificate and authorized to access that area.

(4) Class II Security Area shall be defined in the same way that is stipulated for Class I Security Area.

(5) Access to Class II Security Area shall be allowed, apart from persons holding a Certificate and authorized for access to such an area, to other persons as well, but only if they are escorted or appropriately controlled, and if they have a justified reason for entry.

Article 22

Control of access to Security Areas shall be performed by checking the identity of visitors and by checking the appropriate official ID or pass of employees, or by the appropriate automatic access control system.

Article 23

For the protection of classified information, authorized persons in bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall organize the control of Security Areas at the end of working hours.

Administrative Zones

Article 24

Administrative Zone shall be established for the use of unclassified information and information classified as RESTRICTED in a controlled, clearly marked perimeter within which it is possible to control the access of people and vehicles.

Administrative Zone shall be established in the area leading up to the Security Area for the purpose of access control.

Physical Security Plan

Article 25

Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation, for facilities or areas where classified and unclassified information is used, shall make a plan of requirements, implementation and organization for the application of physical security measures.

Assessment of Physical Security Measures Effectiveness

Article 26

Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall assess the effectiveness of physical security measures and the entire security system at least once a year, and the assessment shall be mandatory when there is a change in the purpose of the protected location or elements of the security system.

Control of Persons

Article 27

Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall perform occasional controls of persons at entrance and exit points to facilities and areas in order to prevent unauthorized disclosure of classified information or to prevent forbidden items from being taken inside.

Classified Information Storage

Article 28

(1) Information classified as TOP SECRET shall be stored within Security Areas:

- In an appropriate security container equipped with unauthorized access detection system, with constant protection and periodic control, or
- In an open storage area equipped with unauthorized access detection system.

(2) Information classified as SECRET shall be stored within Security Areas:

- In an appropriate security container, or
- In an open storage area equipped with unauthorized access detection system or under constant protection and periodical control.

(3) Information classified as CONFIDENTIAL shall be stored within Security Areas in an appropriate security container.

(4) Information classified as RESTRICTED and UNCLASSIFIED shall be stored in locked office furniture.

Technically Secure Areas

Article 29

(1) Technically secure areas are facilities or areas within Security Areas where information classified as TOP SECRET or SECRET is handled, the entrance to which is separately controlled and which have anti-eavesdropping protection.

(2) Technically secure areas, when not used, shall be locked and secured in accordance with physical protection standards.

Physical Security of Information Systems

Article 30

(1) Information systems where information classified as TOP SECRET, SECRET and CONFIDENTIAL is processed, stored or transmitted shall be installed within Security Areas.

(2) Areas where servers, communication and management equipment of information systems is housed, for the use of information classified as RESTRICTED, shall be organized as Security Areas.

(3) Areas where unclassified information or information classified as RESTRICTED is used through communication and information systems shall be organized as Administrative Zones.

Equipment for Physical Protection of Classified Information

Article 31

Equipment for physical protection of classified information shall be in accordance with information security standards for the area of physical security i.e. the appropriate national or international standards.

IV INFORMATION SECURITY MEASURES FOR THE AREA OF SECURITY OF INFORMATION

Article 32

Information security measures for the area of security of information are as follows:
- Classification and declassification of information;
- Marking of information;
- Access to information;
- Information protection;
- Registry system
- Records of classified information usage;
- Handling of classified information in emergency situations;
- Release of classified information to another state or international organization.

Article 33

(1) The originator of classified information may issue an internal instruction on the manner of explaining the chosen classification to each piece or set of classified information for the purpose of subsequent periodic control.

(2) In the course of classified information generation, the originator of classified information may, when possible, determine the timeframe within which the classification level may be altered or within which classified information may be declassified.

Article 34

(1) When the originator of information uses classified information from different sources to generate new classified information, its classification shall be assessed for the purpose of determining the classification for the new classified information.

(2) Parts of classified information, pages, paragraphs, extracts, annexes and attachments, when used or distributed, shall be marked with the original classification.

(3) If additional documents used to deliver classified information are separated from the classified document and do not contain classified information, they shall be classified as UNCLASSIFIED – SEPARATED FROM THE ATTACHMENT.

Registry System

Article 35

Registry system for the exchange of classified information with other states and international organizations consists of:

- Central Registry at the Office of the National Security Council;
- Sub-registries of the Central Registry;
- Registries in other bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation.

Article 36

(1) Registries referred to in Article 35 indent 3 shall be established in bodies and legal entities for internal distribution of classified information, in coordination with the Office of the National Security Council.

(2) Occasional access to classified information shall not require the establishment of a registry provided the stipulated measures and standards for the protection of classified information are implemented and provided there are records of the end users of information.

Article 37

(1) The Office of the National Security Council shall perform security accreditation of the registry system and shall issue a Certificate authorizing its operation and identifying the highest classification of classified information it may handle.

(2) The Office of the National Security Council shall determine the validity of the accreditation referred to in paragraph 1 of this Article at least once in two years.

Article 38

The Central Registry, sub-registries of the Central Registry and registries, when handling information classified as TOP SECRET, shall designate a Control Officer.

Article 39

Registry for the records, control and distribution of crypto material shall be a constituent part of the Information Systems Security Bureau, and the information transferred in this way shall not be recorded through the registry system.

Records of Classified Information Usage

Article 40

Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation, when using information classified as TOP SECRET, SECRET and CONFIDENTIAL, shall keep the records of its usage stipulated by Article 96 of this Regulation.

Handling of Classified Information in Emergency Situations

Article 41

Bodies and legal entities handling classified information shall make contingency plans for classified information.

Article 42

(1) When classified information has been lost or misplaced within the Security Areas or Administrative Zones provisions of the act related to destruction, alienation or availability of classified information to unauthorized persons shall apply.

(2) Based on the information about the destruction, alienation or availability of classified information to unauthorized persons, the Office of the National Security Council shall inform the competent security and intelligence agency and other competent authorities.

Article 43

In case of destruction, alienation or availability of classified information of another state or international organization to unauthorized persons, the Office of the National Security Council shall inform the competent authority of the other state or international organization.

Release of Classified Information to another State or International Organization

Article 44

(1) In case when an international agreement on the exchange and mutual protection of classified information has been signed, the bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation establish cooperation in a certain area that includes the exchange of classified information and keep separate records of the exchanged classified information.

(2) Bodies and legal entities shall inform the Office of the National Security Council at least once a year about the established cooperation and the implementation of the provisions of the international agreement referred to in paragraph 1 of this Article.

V INFORMATION SECURITY MEASURES FOR THE AREA OF INFOSEC

Article 45

Information security measures for the area of INFOSEC are as follows:
- Measures for INFOSEC protection;
- Security awareness management, and
- Plan of action in case of emergency.

Measures for the protection of information systems

Article 46

Measures for the protection of information systems are as follows:
- Protection of hardware, software and data storage media;
- Management of configuration and user access system;
- Control of connections and use of information systems;
- Protection from the risk of electromagnetic radiation;
- Application of cryptographic protection.

Protection of Hardware, Software and Data Storage Media

Article 47

Hardware and data storage media shall be protected and stored in accordance with the procedures defined for the protection of the highest classification level of the information processed or stored in the hardware and media concerned.

Article 48

Reparation, removal from inventory of worn-out or inoperable hardware, as well as maintenance, procedures related to deletion, reparation and destruction of data storage media, shall be carried out in accordance with the stipulated procedures.

Article 49

Use of software is mandatory for the purpose of maintaining the integrity, availability and accessibility of classified information and software referred to in Article 2 indent 7 of this Regulation.

Article 50

Systems for processing classified information shall be installed in such a manner as to entail the exclusion of any unnecessary servicing, removal of all programmes that are not necessary for the functioning of the users' work process, and the installation of the current security programme/software patches.

User Access Configuration and System Management

Article 51

Configuration management while planning, designing, building, using, maintaining and cessation of operation of an information system must ensure compliance with operational and security requirements.

Article 52

User access system management implies the development, application and maintenance of the system in such a manner as to enable unambiguous user identification, authentication and authorization.

Information System Connection and Use Control

Article 53

Information system connection control includes the definition of conditions for interconnection of information systems and records and control thereof.

Article 54

(1) Information system use control implies keeping records of the information system users' activities.

(2) Along with the activities referred to in paragraph 1 of this Article, measures shall be taken to prevent misuse of information systems through installation of systems for detecting unauthorized network intrusion, definition, review and analysis of system operation log and analyses of information system vulnerability.

Protection from the Risk of Electromagnetic Emissions

Article 55

All equipment used to process information classified as TOP SECRET, SECRET and CONFIDENTIAL shall be secured with TEMPEST countermeasures, in accordance with the assessment of the risk of unwanted electromagnetic emissions.

Application of Cryptographic Protection

Article 56

(1) Confidentiality, integrity, authenticity and non-repudiation of classified information shall be ensured by using approved cryptographic methods by the competent authority.

(2) During transmission, classified information shall be protected by the methods referred to in paragraph 1 of this Article, except when stipulated otherwise in an international agreement on mutual protection of classified information signed between the Republic of Croatia and a certain State or international organization.

Article 57

(1) If exceptional circumstances exist that may bring into question the transmission of classified information by prescribed methods, information classified as SECRET, CONFIDENTIAL and RESTRICTED may be transmitted without encryption, with written authorization.

(2) Authorization referred to in paragraph 1 of this Article shall be granted by the head of the body or legal entity or by a person authorized to do so by the head of the body or legal entity, based on the assessment that the possible detrimental consequences as a result of the classified information transmission that is not in accordance with the prescribed methods shall be less severe than the consequences that would arise without such transmission.

Article 58

Facilities and legal entities referred to in Article 1 paragraph 2 of this Regulation that use cryptographic equipment and documents for the protection of classified information shall apply security measures in accordance with prescribed procedures.

Security Awareness Management

Article 59

Security awareness management shall include:

- Establishment of security rules for employees,
- Security-related education and training.

Establishment of Security Rules for Employees

Article 60

All users of the information system shall be made aware of the security rules and consequences of the failure to comply with them.

Security-Related Education and Training

Article 61

All users of the information system, depending on their own duties and responsibilities, shall be educated, in a regular and timely manner, on security-related aspects of using the information system.

Planning of Actions in Exceptional Circumstances

Article 62

Planning of actions in exceptional circumstances shall include:

- Drafting of operation procedures in case of an incident,
- Drafting of a plan for uninterrupted operation.

Drafting of a Plan for Uninterrupted Operation

Article 63

Planning of actions in exceptional circumstances includes determination and analysis of potential problems in system operation, as well as definition of procedures for solving those problems and definition of other methods of use, in case the resources of the information system are unavailable, in order to maintain the continuity of operation.

Article 64

Continuity of operation also includes the establishment and testing of an adequate procedure of the security storage of information in order to recover the system and information to the pre-incident state (system breakdown, natural disasters and computer viruses).

Drafting of Operation Procedures In Case of an Incident

Article 65

Drafting of operating procedures in case of an incident includes planning and definition of activities to divert, prevent, detect and recover from the effects of the incident which affect the confidentiality, integrity and availability of the information or information system, including reporting on security incidents.

Article 66

Efficiency of measures referred to in Article 45 of this Regulation shall be ensured by a systematic approach that includes:

- Consideration of security aspects in all phases of the information system’s life cycle,
- Definition of responsibility for the implementation of each measure,
- Regular control of the established security rules and application thereof, in order to verify efficiency and functionality.

VI INFORMATION SECURITY MEASURES FOR THE AREA OF INDUSTRIAL SECURITY

Article 67

Information security measures for the area of Industrial Security are:

- Conclusion of classified contracts,
- Facility Security Clearance,
- Security requirements for concluding classified contracts,
- Transportation of classified material,
- Access to classified information during international visits,
- Exchange of personnel within projects or programs.

Conclusion of Classified Contracts

Article 68

Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall, when concluding classified contracts within which classified information is exchanged, make tender documentation in such a way that it only contains unclassified information or information classified as RESTRICTED. Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall sign, with the legal entities applying for the tender, a statement on the protection of classified information of the tender documentation.

Article 69

(1) Legal entity, as a party in the contract classified as TOP SECRET, SECRET and CONFIDENTIAL, shall have a Facility Security Clearance and the employees of the legal entity that will have access to classified information shall have an appropriate Certificate, and can only have access to that classified information which is part of the contract and for which they have a Need-to-Know.

(2) Instead of a Facility Security Clearance, a contract classified as RESTRICTED shall contain a clause on mutual protection of classified information and the employees of the legal entity who will have access to classified information shall be security briefed and shall sign a statement on handling classified information.

Facility Security Clearance

Article 70

Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall submit a request for Facility Security Clearance issuance for legal entities, for concluding contracts classified as TOP SECRET, SECRET and CONFIDENTIAL, to the Office of the National Security Council.

Article 71

When taking part in international classified contracts, legal entities shall submit a request for Facility Security Clearance issuance to the Office of the National Security Council, after the Clearance has been requested by the competent security authority of another country or international organization.

Article 72

The request for Facility Security Clearance issuance shall contain:

- Name, address and ID number of the legal entity for which the Clearance is requested,
- Reason for requesting the Clearance,
- Classification level of the classified information for which the Clearance is requested,
- Fully completed and authorized Questionnaire for security vetting of the legal entity.

Article 73

(1) The procedure for Facility Security Clearance issuance shall begin with signing a contract between the Office of the National Security Council and the legal entity.

(2) The contract referred to in paragraph 1 of this Article shall, among other things, stipulate consent for security vetting for the legal entity, delivery of the Questionnaire for security vetting of the employees of the legal entity who will have access to classified information, and delivery of the remaining documentation or implementation of other actions from the contract.

(3) Instruction for the implementation of information security measures and standards for the protection of classified information within a legal entity shall be an integral part of the contract referred to in paragraph 1 of this Article.

Article 74

Security vetting of a legal person shall include:

- Control of ownership, ownership structure, information of companies owned, control of complete business and financial obligations, with regard to possible security risks,
- Security vetting of owner, director, members of managing and supervisory boards, shareholders and stakeholders who may, by virtue of their functions, have access to classified information,
- Security vetting of the person proposed for the position of the security officer at the legal entity, for his or her deputy and employees who will have access to classified information.

Article 75

The Office of the National Security Council shall issue a Facility Security Clearance for the legal entity when, based on the report by the competent security and intelligence agency, it determines that there are no security impediments and in case all the information security measures and standards referred to in Article 73 paragraph 3 of this Regulation have been implemented.

Article 76

The Office of the National Security Council shall issue a Facility Security Clearance within the period no longer than six months from signing the contract referred to in Article 73 of this Regulation.

Article 77

Facility Security Clearance is issued for a period of 5 years.
During the validity of the Clearance referred to in paragraph 1 of this Article the Office of the National Security Council shall carry out the procedure of suspension or revocation of the Clearance when the conditions defined in the contract referred to in Article 73 of this Regulation have changed.

Article 78

A legal entity employing a foreign citizen in a position requiring access to classified information shall, through the Office of the National Security Council, request a Clearance from the competent authority of the state of the employee's citizenship.

Article 79

(1) The form of Clearance referred to in Article 77 paragraph 1 of this Regulation is defined by the Office of the National Security Council, it is enclosed to this Regulation and makes its integral part.

(2) The form of an appropriate international facility security clearance shall be determined, in each individual case, by the Office of the National Security Council, in accordance with the standards determined in the scope of international agreements signed between the Republic of Croatia and other states and international organizations.

Security Requirements for Concluding Classified Contracts

Article 80

(1) When concluding classified contracts, state bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall make, as an annex to the contract, instructions on security measures in the project and classification of information in the project.

(2) International classified contracts shall contain a Project Security Instruction, with Instruction on classification of information in the project as its integral part.

Transportation of Classified Material

Article 81

(1) Security measures referred to in Article 80 shall be implemented continuously during the transportation of classified material, while the protection of a classified consignment shall be in line with the highest classification level of a certain document in the consignment.

(2) Legal entity, when transporting materials classified as TOP SECRET, SECRET and CONFIDENTIAL, shall have a Facility Security Clearance and the personnel handling the consignment shall have appropriate Personnel Security Clearances.

(3) Transportation shall be performed using the exact route, point-to-point, in the shortest period possible, and shall include measures for the prevention of unauthorized access to classified information.

Article 82

Plan for the transportation of classified material within the Republic of Croatia shall be agreed upon by the contracting parties in accordance with Article 81 of this Regulation.

Article 83

(1) Plan for the transportation of classified material in international classified contracts shall be proposed by the contracting party that orders the transportation.

(2) Exceptionally from paragraph 1 of this Article, if more transports of the same kind are organized within a short period, a unique transportation plan may be made.

(3) The Office of the National Security Council shall authorize the transportation plan and provide consent for international transportation of classified material when that is stipulated in an international agreement.

Access to Classified Information during International Visits

Article 84

(1) Bodies and legal entities, when sending employees on international visits within which they will have access to information classified as TOP SECRET, SECRET and CONFIDENTIAL, shall inform the competent authority of that state or international organization about the said employees, through the Office of the National Security Council, if an international agreement on mutual protection of classified information has been signed.

(2) The Office of the National Security Council shall issue to the bodies and legal entities security approvals for visits of representatives of other states, international organizations and legal entities, during which they will have access to classified contracts, programs and projects, on the basis of appropriate clearances, if a signed agreement on mutual protection of classified information exists.

(3) Contracting parties to programs or projects from classified contracts, within which the international visit is organized, are responsible for the initiation of the procedure with the Office of the National Security Council, which includes notification about the visit and exchange of appropriate clearances with the competent authority in the other state or international organization.

(4) Bodies and legal entities, when hosting visits referred to in paragraph 2 of this Article, shall keep records of the visits and access by the individuals to classified information.

Article 85

Exceptionally from Article 83 paragraph 3 and Article 84 paragraphs 2 and 3 of this Regulation, security and intelligence agencies, in the course of cooperation with foreign security and intelligence agencies, directly exchange, transport or access operative and analytical classified information.

Exchange of Personnel within a Program or Project

Article 86

(1) When an employee possessing a clearance is transferred to a legal entity in another state, within the same program or project, the legal person whose employee is transferred shall request from the Office of the National Security Council to deliver the necessary clearances to the competent security authority of that state.

(2) The employee referred to in paragraph 1 of this Article shall be briefed on security standards the implementation of which is mandatory during international visits.

VII INFORMATION SECURITY RISK MANAGEMENT

Article 87

(1) When handling classified information, state bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation, shall manage the information security risk.

(2) Information security risk management comprises permanent risk assessment and risk processing in order to prevent destruction, disclosure and loss of or unauthorized access to classified information.

Information Security Risk Assessment

Article 88

(1) Information security risk assessment is a comprehensive process of assessing the risk to classified information.

(2) Results of the risk assessment make the basis for the selection of appropriate protection measures, in accordance with the risk management priorities.

(3) Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall keep records of risk assessment, which shall contain the date of the assessment, risk description, assessment and the probability of impact of each risk, applied security measures and a statement on necessary security measures with the designated person and the period of implementation.

Risk Processing

Article 89

Risk processing is a process in which the degree of acceptability is determined for each estimated risk, in order for it to be accepted, reduced or avoided.

Article 90

(1) The risk may be accepted if the damage that would arise from it would be less severe than the damage that would arise from not taking a certain action.

(2) Risk reduction is performed by applying security measures in order to prevent destruction, disclosure and loss of, as well as unauthorized access to classified information.

(3) Risk avoidance means the implementation of organizational measures in order to avoid the actions that may cause risk.

(4) The decision on handling the remaining risk, after risk processing, shall be made by the head of the body or legal entity.

Article 91

After making the decision on risk processing, bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall make a plan of risk processing which shall determine the implementation of the necessary measures.

Article 92

The results of risk assessment and risk processing shall be regularly revised, in accordance with the needs of the body or legal entity, due to possible internal or external changes.

VIII OVERSIGHT OF INFORMATION SECURITY MEASURES AND STANDARDS

Article 93

(1) Oversight of the implementation of information security measures and standards in bodies and legal entities using classified or unclassified information shall be conducted by security officers from those bodies and legal entities.

(2) The Office of the National Security Council shall conduct oversight referred to in Article 30 paragraph 1 of the Data Secrecy Act in all bodies and legal entities using information classified as TOP SECRET, SECRET and CONFIDENTIAL at least once in two years, and at least once in four years in bodies and legal entities using information classified as RESTRICTED and UNCLASSIFIED.

(3) Security and intelligence agencies shall participate in the oversight of the implementation of information security measures in the framework of the activities in the area of counterintelligence protection prescribed by a separate act.

Article 94

(1) The Office of the National Security Council shall make a report on the oversight referred to in Article 92 paragraphs 1 and 2 of this Regulation and deliver it in written form to the head of the body or legal entity in which the oversight was conducted.

(2) The report referred to in paragraph 1 of this Article shall also contain instructions which shall be implemented by the bodies and legal entities within a stipulated period in order to remove the established deficiencies and irregularities.

(3) The head of the body or legal entity referred to in paragraph 1 of this Article may deliver a statement about the report to the Office of the National Security Council within 15 days from the day of the receipt of the report.

(4) The Office of the National Security Council shall respond to the statement referred to in paragraph 3 of this Article within 30 days from the day of the receipt of the statement.

Article 95

When the Office of the National Security Council has established, based on the oversight referred to in Article 92 paragraphs 1 and 2 of this Regulation, that the prescribed security standards are not being implemented, it shall submit a written report to the competent security and intelligence agency and the Information Systems Security Bureau, and they will initiate further prescribed actions from their scope of activity.

IX TRANSITIONAL AND FINAL PROVISIONS

Article 96

Bodies and legal entities referred to in Article 1 paragraph 2 of this Regulation shall adopt security measures and align their operation with the provisions of this Regulation and Ordinances referred to in Articles 15 and 18 of the Information Security Act within 12 months from the adoption of this Regulation.

Article 97

(1) Bodies and legal entities that have, in accordance with the Act on Information Secrecy Protection (Official Gazette 108/1996), created their own information systems, shall conduct security accreditation of classified information systems in accordance with this Regulation, within 24 months from the adoption of this Regulation.

(2) Until the implementation of security accreditation of classified information systems, bodies and legal entities referred to in paragraph 1 of this Article shall not use in those systems classified information of other states and international organizations with which the Republic of Croatia has signed international agreements on mutual protection of classified information.

Article 98

The conditions stipulated in Article 8 paragraph 1 of this Regulation, for information systems, shall be fulfilled within 18 months from the adoption of this Regulation.

Article 99

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