UNOFFICIAL TRANSLATION

ROMANIA

GOVERNMENT OF ROMANIA

GOVERNMENT DECISION no. 585/2002

NATIONAL STANDARDS ON THE PROTECTION OF CLASSIFIED INFORMATION IN ROMANIA

GOVERNMENT DECISION NO. 585/13.06.2002

CHAPTER I

GENERAL PROVISIONS

Art. 1 – The national standards for the protection of classified information in Romania include the implementation norms of the Law 182/2002 on the protection of classified information regarding:

a) classifications of state secret information and norms regarding the minimum protection measures within each class;
b) obligations and responsibilities of public authorities and organizations, economic entities and other public and private legal persons, as to the protection of state secret information;
c) norms regarding access to classified information, as well as, the security vetting procedure;
d) general rules regarding the recording, drawing up, storage, processing, multiplication, handling, transport, transmission and destruction of state secret information;
e) rules of identification and marking, compulsory inscriptions and mentions on state secret documents, on classification levels, requirements for recording the number of copies and addressees, storage terms and regime, interdictions of multiplication and circulation of documents;
f) conditions for photographing, filming, cartography and execution of works of fine arts in facilities and places of special importance for the protection of state secret information;
g) rules regarding the access of foreign citizens to state secret information;
h) protection of classified information as part of secret industrial contracts - industrial security;
i) protection of information-generating sources - INFOSEC.

Art. 2 - (1) These standards establish the national system for the protection of classified information, in accordance with the national interest, with NATO criteria and recommendations, and are compulsory for all legal and natural persons handling such information.

(2) The equivalence of national and NATO classification levels is the following:

a) Strict secret de importanta deosebita
("strictly secret of special importance") - NATO top secret
b) Strict secret (Strictly secret) - NATO secret
c) Secret (Secret) - NATO confidential
d) Secret de serviciu (Job secret) - NATO restricted

Art. 3 - The terms used in these standards shall have the following meaning:

- Designated Security Authority - DSA - organization legally authorized to establish, for its field of activity and responsibility, its own structures and measures for the co-ordination and control of the activities related to the protection of information classified as state secret. According to the law, the Designated Security Authorities are: Ministry of National Defense, Ministry of Interior, Ministry of Justice, Romanian Intelligence Service, Foreign Intelligence Service, Guard and Protection Service, Special Telecommunications Service;

- ***Authorization for access to classified information*** - document issued, with the approval of the competent security authorities, by the head of the legal person holding classified information, certifying that, in performing his tasks, its holder may have access to information classified as state secret of a certain secrecy level, according to the need-to-know principle;

- Industrial Security Authorization – document issued by the National Registry Office for Classified Information - ORNISS - for an industrial facility, certifying that the respective industrial facility is empowered to participate in the negotiation procedure of a classified contract;

- Special authorization – document issued by ORNISS certifying that an individual is vetted and accredited to perform photographing, filming, map-drawing activities or to produce works of fine arts on the territory of Romania, in premises, areas or places with special relevance for the protection of information classified as state secret;

- Industrial security approval - document issued by the DSA, certifying that the contracting industrial facility implemented all the security measures necessary for the protection of classified information handled while carrying on a concluded contract;

- Security clearance certificate – document issued to a person with direct tasks in the field of classified information protection, i.e. security officer or employee of the security structure, attesting that he/she was vetted and accredited to hold, have access to or work with classified information of a certain secrecy level;

- Facility Security Clearance – document issued by ORNISS to an industrial facility attesting that this facility is empowered to deploy industrial and/or research activities which require access to classified information;

- Classification of information – assignment of a class and of a secrecy level to the information;

- Classified contract – any contract containing and dealing with classified information, concluded between the parties, under the terms of the law;

- Contracting party – industrial, commercial, execution, research and design or service-rendering entity within a classified contract;

- Contractor – party in a classified contract, beneficiary of the works or services rendered by the contracting party;

- Control of classified information - any activity meant to verify the way classified documents are managed;

- Declassification – suppression of the classification markings and discharge of the classified information of the protective regulations stipulated by the law;

- Dissemination of classified information – release of classified information to entities or persons empowered to have access to such information.

- Classified document – any physical media containing classified information, in original or in copy, such as:

a) paper – holographic documents, typed or printed matter, sketches, maps, charts, photographs, drawings, carbon copies, listings;
b) magnetic tapes, audio-video cassettes, microfilms;
c) computer storage media – floppy disks, CDs, hard-disks, PROM and EPROM memories, ribbons;
d) portable processing devices – electronic note-books, laptops – whose hard-disk is used for the storage of information;

- ***Security officer*** – person assigned with the protection of classified information within authorities, public organizations, economic operators with integral or partial state share capital and other legal public or private persons;

- Management of classified information – any activity of drawing up, accounting, accessing, processing, copying, handling, transporting, sending, keeping records, archiving or destroying classified information;

- Security incident – any action or inaction contrary to the security regulations whose consequences have led to or are to determine compromise of classified information;

- Restriction indicator – text or symbol in the text signaling restriction of access or activities in areas, facilities, premises or places with relevance for the protection of classified information;

- Compromised classified information – classified information that has lost its integrity, has been misplaced, lost or accessed totally or partially by unauthorized individuals;

- Organizations performing coordination activities and control of the measures regarding the protection of classified information or Competent Authority – Ministry of National Defense, Ministry of Interior, Ministry of Justice, Romanian Intelligence Service, Foreign Intelligence Service, Guard and Protection Service, Special Telecommunications Service, according to their competences established by law;

- Marking – writing the secrecy level of the information and indicating its special protection requirements;

- Classified material – document or product manufactured or being manufactured that needs protection against unauthorized disclosure;

- Need-to-know – principle according to which access to classified information is granted individually only to those persons who, in order to fulfill their duties, have to handle or have access such information;

- Negotiations – activities referring to the awarding of a contract or sub-contract, from the notification of intention to call for bids to the end of the bid;

- Industrial facility – research or production facility that carries out scientific, technological, or economic activities related to the national security or defense, or which are of a special importance for Romania's economic, technological and scientific interests;

- Facility, premise or place of special importance for the protection of classified information – a premise or a specially-designated perimeter where information classified as state secret is managed;

- Contracting party – any of the parties that agree to negotiate, conclude or carry on a classified contract;

- Protection of information-generating sources – all measures designed for the protection of classified information drawn-up, stored or transmitted by automated data processing and/or communication systems or networks;

- Industrial security – system of norms and measures governing the protection of classified information in the field of contractual activities;

-Protection of classified information system – all legal, procedural, and physical measures, of personnel and information-generating sources protection meant to ensure the security of classified documents and material;

- Security structure – compartment specialized in the protection of classified information, organized within the public authorities and organizations, economic operators with integral or partial state share capital and other legal public or private persons;

- Subcontractor – party undertaking the carrying on of a part of the classified contract, under the coordination of the contracting party;

- Downgrading – change of classification level of information classified as state secret;

- Entity holding classified information or entity – public authority or organization, economic operators with integral or partial state share capital or other legal public or private person which, according to the law, has the right to hold classified information;

- Security vetting – all measures taken by the Designated Security Authorities, according to their competences, in order to establish the honesty and professionalism of individuals with a purpose to approve the issuing of the security clearance certificate or authorization of access to classified information;

- Security area –perimeter specially delimited and arranged where classified information is managed

CHAPTER II

CLASSIFICATION AND DECLASSIFICATION OF INFORMATION MINIMUM PROTECTIVE MEASURES SPECIFIC TO SECRECY CLASSES AND LEVELS

SECTION 1 Classification of Information

Art. 4 - (1) According to the law, information is classified state secret or “secret de serviciu” (restricted), depending on its importance for the national security and the consequences resulting from its unauthorized dissemination or disclosure.

(2) State secret information is that information whose disclosure may result in serious damage to the national security and defense, and which, depending on the importance of the protected values, is included in the following secrecy levels provided by law;

a) strict secret de importanta deosebita (NATO top secret)

b) strict secret (NATO secret);

c) secret (NATO confidential).

(3) The information whose disclosure may result in damage to a private or public legal person is classified as “secret de serviciu” (restricted).

Art. 5 - (1) Public authorities drawing up or handling state secret information shall draft a guide for its correct and uniform classification.

(2) The guide mentioned under paragraph **(1)** will be approved personally and in writing by those empowered or by senior officials authorized to assign secrecy levels, according to the law.

Art. 6 – Public authorities and organizations draft their own lists with categories of state secret information for their fields of activity which are approved and up-dated by Government Decision.

Art. 7 – The lists with "secret de serviciu" (restricted) information are established by the heads of the organizations holding such information.

Art. 8 – The lists with "secret de serviciu" (restricted) information will include information referring to the activity of the organization and which, according to the law, is not considered state secret information, but should be known only by those persons who need it in fulfilling their duties, and whose disclosure may damage the interests of the organization.

Art. 9 – The organizations managing classified information shall analyze whenever necessary the lists of state secret information and shall submit to the Government for approval proposals for up-dating and completing the lists, according to the law.

Art. 10 – The class and classification level of information shall be assigned after consultation of lists of state secret information and "secret de serviciu" (restricted) information, drawn up according to the law.

Art. 11 – The hierarchical head of the originator shall check whether the information has been correctly classified and shall take measures if inappropriate secrecy levels have been assigned.

Art. 12 - (1) The periods for classification of state secret information shall be set by the originator, depending on its importance and on the consequences resulting from its unauthorized disclosure or dissemination.

(2) The classification periods of state secret information, on classification levels, except when it needs longer protection are up to:

- 100 years for "strict secret de importanta deosebita" information;
- 50 years for "strict secret" information;
- 30 years for "secret" information;

(3) The periods provided under paragraph 2 may be extended by Government Decision, based on good argument, at request of the heads of organizations holding classified information or, as the case may be, of the senior officials authorized to assign classification levels.

Art. 13 – Any person empowered or senior official authorized to assign classification levels shall order periodic checks of all state secret

information that has been assigned classification levels, occasion, if necessary, for reassessment of classification levels and storage periods.

Art. 14 - (1) A document resulting from the processing of the information with different classification levels shall be classified according to its new content that may be higher than that of the original documents.

(2) The document resulting from the unprocessed accumulation of excerpts from classified information shall receive the class or the secrecy level corresponding to the content of the excerpt with the highest secrecy level.

(3) Summaries, translations and excerpts of classified documents shall receive the class or the secrecy level corresponding to the content.

Art. 15 – Marking classified documents is meant to draw attention of the persons handling or accessing it that they are in possession of information which should be specifically accessed and protected, according to the law.

Art. 16 – Under-assessment or over-assessment of the secrecy level or class shall be brought to the attention of the originator. In case he decides for reclassification, he will inform all the holders of that information.

Art. 17 - (1) Information shall be classified only if it needs protection. Secrecy levels and classification periods shall apply as long as unauthorized disclosure or dissemination of that information may damage the national security and defense, public order or the interests of public or private legal persons.

(2) Under-assessment or over-assessment of the information secrecy level and of the duration for which it has been stored may be contested by any Romanian legal or natural person in the administrative courts for contentious matters.

Art. 18 – (1) No later than 12 months from the coming into force of this Decision, holders of state secret information and “secret de serviciu” information, established as such by the Council of Ministers’ Decision no. 19/14.01.1972 shall submit to the authorized persons or authorities empowered to assign secrecy levels, propositions regarding the new classification of this information in secrecy classes and levels, as the case may be.

(2) Until establishment of the new secrecy levels, state secret information and “secret de serviciu” information under paragraph (1) shall maintain its secrecy level and period and shall be protected according to these standards.

SECTION 2
Declassification and downgrading of classified information

Art. 19 – State secret information shall be declassified by Government Decision, at motivated request of the originator.

Art. 20 - (1) Information shall be declassified if:

a) the classification period has expired;

b) its disclosure shall not endanger national security and defence, public order or the interests of private or public legal persons holding it;

c) the classification level has been assigned by an unauthorized person.

(2) Declassification or downgrading of state secret information shall be done by persons or senior officials authorized by law to assign classification levels, with prior notice of organizations coordinating the activity and controlling the measures for the protection of classified information according to their competence.

(3) Originators of state secret information shall periodically assess the need to maintain the secrecy levels previously assigned, and shall submit to the persons and senior officials authorized proposals as the case may be.

Art. 21 – Whenever possible, the originator of a classified document shall mention if the document may be declassified or downgraded, at a certain date or on a certain occasion.

Art. 22 - (1) When changing the class or secrecy level initially assigned to information, the originator shall inform the security structure/officer who will mention it in the recording registries.

(2) The date and the new secrecy class or level shall be marked on the document above or under the old marking and the latter shall be invalidated by drawing an oblique line.

(3) The originator of declassified or downgraded information shall ensure that all addressees are informed on this, in writing and in due time.

Art. 23 - (1) Classified information determined as compromised or irreversibly lost shall be declassified.

(2) Declassification shall be done only based on an investigation that established the loss or compromise of the respective information or of its material format, with the written consent of the originator.

Art. 24 – “Secret de serviciu” information shall be declassified by the heads of the organizations originating it, by deleting it from the lists as provided under article 8, which shall be reassessed whenever necessary.

SECTION 3
Minimum protective measures for classified information

Art. 25 – The protective measures for classified information shall be established in relation with:

a) secrecy levels and classes of information;

b) amount and format of information;

c) rank, position and number of persons who have or may have access to information, based on the security clearance certificate or access authorization and with the observance of the need-to-know principle;

d) threats, risks and vulnerabilities with consequences upon classified information.

Art. 26 – Transmission of classified information to other users shall be done only if they hold security clearance certificates or access authorizations appropriate for the required secrecy level.

Art. 27 - Security clearance certificates of individuals, whose conduct, attitude or manifestations may create premises of insecurity for state secret information, shall be immediately withdrawn and the organizations performing coordination activities and control of the measures regarding the protection of classified information shall be informed, according to their competence.

Art. 28 – Heads of organizations and individuals managing classified information shall inform the organizations with tasks of coordination and control in the field, on any indications which may result in security risks to such information.

SECTION 4
Security structure/officer

Art. 29 - (1) Security structures with specific tasks shall be established, under the terms of the law, in organizations holding such information, for the implementation of the protective measures of classified information.

(2) In case the organization holds a small amount of classified information, the tasks of the security structure shall be fulfilled by the security officer.

(3) The security structure shall be organized under the terms of the law.

(4) The head of the security structure, respectively the security officer is a deputy of the head of the legal person or a member of the organization's board.

Art. 30 – The head of the security structure, respectively the security officer, shall hold an appropriate security clearance at the highest level of classification for state secret information managed by the organization.

Art. 31 - (1) As general tasks, the security structure/officer shall:

a) work out and submit for approval to the senior management the internal norms on the protection of classified information according to the law;
b) draw up the plan for the prevention of classified information leakage and submit it for approval to the competent authorities, and after approval, take measures for its implementation;
c) coordinate the activity of protection in all its components;
d) be the point of contact with the organization authorized to coordinate the activity and control the measures for protection of classified information, in compliance with the law;
e) monitor the implementation of the security norms for classified information, as well as the way in which these norms are observed;
f) counsel the head of the organization on each aspect concerning security of classified information;
g) inform the head of the organization on the vulnerabilities and risks existing in the system for the protection of classified information and suggest measures to eliminate them;
h) provide support to the authorized representatives of the organizations entitled, according to their legal competence, to conduct security vetting upon persons for which access to NATO classified information is required;
i) organize specific training activities for persons with access to classified information;
j) ensure custody and record of all security clearance certificates and authorizations for access to classified information;
k) permanently update the record of security clearance certificates and access authorizations;
l) draft and update the lists of classified information generated or stored by the organization, according to secrecy classes and levels;
m) submit to the head of organization proposals as to establishing facilities, premises and places of special importance for the protection of classified information in its area of responsibility and, if necessary, request support from competent organizations;

n) perform, upon approval of the head of the organization, checks on the implementation of the legal measures for the protection of classified information;
o) fulfill other tasks related to the protection of classified information, according to the law.

(2) The tasks of the security structure personnel, respectively of the security officer are set by the job description approved by the head of the organization.

Art. 32 – Persons working in the security structure, or, as the case may be, the security officer, shall be subject to permanent training programs organized by the organizations authorized to coordinate and control the measures for the protection of classified information, according to the law.

SECTION 5
Access to classified information

Art. 33 - Access to NATO classified information is granted on the basis of the need-to-know principle only to the individuals holding security clearance certificates or access authorizations valid for the secrecy level of the information necessary for the fulfilling of their tasks.

Art. 34 – Individuals having access to “strict secret de importanta deosebita” information, under the terms of these standards, will be recorded in the consultation sheet, Annex 1, which shall be kept by the authorized holder of the document.

Art. 35 - (1) Individuals who were issued security clearance certificates or access authorizations shall be trained initially and periodically regarding the regulations on the protection of classified information.

(2) Training and briefings shall be recorded, under signature, in the individual training form shown in Annex 2.

(3) Individuals under paragraph 1 shall sign the confidentiality agreement in Annex 3.

Art. 36 - (1) In exceptional cases determined by crises, calamities or unforeseeable situations, the head of the organization may grant temporary access to classified information to certain individuals who do not hold security clearances or access authorizations, on condition that an appropriate recording system has been established.

(2) Individuals receiving temporary access to state secret information shall sign the confidentiality agreement and shall be notified to ORNISS as soon as possible, so that the vetting procedure may be carried out in compliance with the procedures.

Art. 37 – In case of “strict secret de importanta deosebita” information the temporary access shall be granted, if possible, to those individuals who already hold security clearances for access to “strict secret” information or “secret” information**.**

Art. 38 - (1) Transmission of classified information between entities shall be done with the approval of the originator, and the observance of the need-to-know principle.

(2) Delivery-receipt of classified information between the holding and the receiving entity shall be done with the observance of the protective measures provided by these standards.

Art. 39 – The security officer/structure of the holding entity shall ensure that the representative of the receiving entity has a security clearance or access authorization appropriate to the secrecy level of the classified information delivered or received.

CHAPTER III

GENERAL RULES ON DRAFTING, DRAWING UP, RECORDING, STORAGE, PROCESSING, MULTIPLICATION, HANDLING, TRANSPORT, TRANMISSION AND DESTRUCTION OF CLASSIFIED INFORMATION

Art. 40 – (1) In entities holding classified information special compartments shall be organized for recording, drafting, storage, processing, reproduction, handling, transport, transmission and destruction in secure conditions.

(2) The activity of special compartments under paragraph (1) shall be coordinated by the security structure/officer.

Art. 41 – When drafting documents containing classified information the following rules shall apply:

a) the originator, the registering date and number, the secrecy class and level, the copy number and, if necessary, the addressee number shall be entered in the heading;

b) the registering numbers shall be written on all copies and their annexes and they shall be preceded by a zero (0) for “secret” documents, by two zeros (00) for “strict secret” documents, by three zeros (000) for “strict secret de importanta deosebita” documents and by the letter S for “secret de serviciu” documents;

c) the rank, position, name and surname of the head of the originating organization and of the person who has drafted the document and their signatures shall be legibly written at the end of document, followed by the stamp of the organization.

d) the secrecy class or level assigned to the document shall be marked on each page;

e) the current number of the page followed by the total number of pages shall be marked on each page of the documents containing classified information.

Art. 42 - (1) If the document has annexes, the record number of each annex, its number of pages and the secrecy class or level shall be indicated at the end of the text.

(2) Annexes will be classified according to their content and not to that of the document they are attached to.

(3) The accompanying note to the document shall not contain detailed information referring to the content of the documents annexed.

(4) The annexed documents are signed, if necessary, by the person who has signed the basic document.

(5) The stamp of the originating entity shall be compulsory applied on the annexed documents.

Art. 43 - (1) When the documents containing classified information are signed by only one person, the data regarding the rank, position, name and surname of the respective person shall be applied under the text, in the middle of the page.

(2) When a document is signed by two or more persons, the rank, position, name and surname of the head of the organization shall be written on the left side of the page, and the data of the other persons shall be written on the right side of the page, in the sequence of their ranks and positions.

Art. 44 – When documents containing classified information are issued in common by two or more entities, their names shall appear separately on the heading, and the respective heads of entities shall sign at the end of the documents, from left to right, and the appropriate stamps shall be applied.

Art. 45 – Classified information shall be marked, inscriptioned and managed only by persons holding security clearance certificates or authorizations appropriate to its classification level.

Art. 46 - (1) All documents, regardless of their format, that contain classified information, shall be applied the classification level on each page.

(2) The classification level shall be marked by stamp, printing, editing or holograph, as follows:

a) on the right side at the top and bottom, on the outside part of the covers, on the title page and on the first page of the document;

b) in the middle, at the top and bottom, on all the other pages of the document;

c) below the caption, the title, or the scale of maps, and outwardly – at the back of the page – when all charts, diagrams, maps, drawings etc., are folded.

Art. 47 – The parts clearly identifiable of complex classified documents, such as sections, annexes, paragraphs, titles, with different secrecy levels or which are not classified shall be marked in accordance with their classification and secrecy level.

Art. 48 – The classification marking shall be applied separately from the other markings, with different letters and/or colors.

Art. 49 - (1) All classified documents which are being drafted or at the stage of project shall bear the mention “Draft” or “Project” and shall be marked according to the secrecy class or level of the information they contain.

(2) Classified documents which are being drafted or at the stage of project shall be managed under the same terms as for the final documents.

Art. 50 – Documents or material containing classified information and are addressed to a specially appointed person shall be marked under the sender’s box with the caption “Personally”.

Art. 51 - (1) Photographs, films, microfilms and their negatives, rolls, bobbins and storage containers shall be marked visibly with a label indicating the date and registering number, as well as the classification level.

(2) Microfilms shall have marked at both ends the secrecy class or level, and at the beginning of the roll, the list of content elements.

Art. 52 - (1) The secrecy class or level of information recorded on audio tapes is recorded verbally, both at the beginning and at the end of the recording.

(2) Marking of the secrecy class or level on the video tapes shall ensure the display on the screen of the secrecy class or level. In case the secrecy class or level cannot be accurately determined, before recording the video tapes, the marking shall be applied by inserting a tape segment at the beginning and at the end of the video tape.

(3) Audio and video tapes containing classified information shall maintain the highest secrecy class or level assigned until the time of:

a) destruction by authorized means;

b) assignment of a higher classification level by adding a new recording with a higher level of secrecy.

Art. 53 – The projections of images must show at the beginning and at the end, the date and registering number, as well as the secrecy class and level.

Art. 54 - (1) Rolls, bobbins and storage containers for magnetic tapes, including video tapes, on which state secret information was recorded, shall bear visibly the highest secrecy class and level assigned to them, which shall be kept until their destruction or demagnetization.

(2) When recording on magnetic tape, the secrecy class or level shall be mentioned both at the beginning and at the end of each passage.

(3) In case of separation from the physical support each end of the tape shall be marked visibly with the secrecy class or level.

Art. 55 – In all cases, the packages or supports for the storage of documents or materials containing classified information shall be marked with the secrecy class or level, the date and registering number and a list with their denominations shall be attached to them.

Art. 56 – (1) When classified documents are used as sources for other documents, the marking of the source documents shall determine those of the final document.

(2) The final document shall bear the mentions of the source documents used for their drafting.

Art. 57 – Number and initial registering date of the classified document shall be kept, even if the document is amended, until the secrecy class or level of the respective document shall be reassessed.

Art. 58 – The heads of entities shall take the necessary measures of registering and control of classified information, so that this could be located at any time.

Art. 59 - (1) Records of material and documents containing classified information shall be kept in special registries, in compliance with the models provided in Annexes 4, 5 and 6.

(2) Each document or material shall bear the date and registering number from the record registries.

(3) The registering numbers are preceded by the number of zeros corresponding to the secrecy class or level, or by the letter “S” for “secret de serviciu”.

(4) All registries, recording books and receipts shall be recorded in the unique registry, according to Annex 7.

(5) Management documents, serial printed matters and other documents and materials specially recorded are exempted from registration in the unique registry.

Art. 60 - (1) Documents and materials containing classified information recorded in the registries under article 59 shall not be recorded in other registries.

(2) Originators and holders of classified information shall keep record of all the received or sent documents and of the documents drafted by the entity, according to the law.

(3) The name and surname of the person who has received the document shall be mentioned in the record registries for classified information, and the person shall sign for receipt in the recording book provided in Annex 8.

Art. 61 - (1) The numbers will be assigned consecutively in the registries, during a calendar year.

(2) The registering numbers shall be applied on all copies of the documents and materials containing classified information, as well as on the annexed documents.

(3) Yearly, the documents shall be put in files according to their subjects and the storage periods established by archivist catalogues, according to the law.

(4) Categorization of documents and materials containing classified information shall be done separately, depending on their support and format, and using appropriate means for their protection and maintenance.

Art. 62 - (1) “Strict secret de importanta deosebita” information shall be kept physically separated and shall be separately recorded from the other classified information.

(2) “Strict secret” information and “secret” information may be recorded in the same registry.

Art. 63 – Maps, topographic plans, maps assemblage and other similar documents shall be recorded in registries for classified information provided in Annexes 4, 5 and 6.

Art. 64 – Assignment of the same registering number to documents with different content is forbidden.

Art. 65 – The registries shall be filled in by the designated person holding an appropriate security clearance certificate.

Art. 66 - (1) Reproduction by typing and computer processing of classified documents shall be done only by authorized person with access to such information.

(2) Reproduction of classified documents shall be done by authorized persons only in specially designed rooms.

Art. 67 - (1) Documents containing classified information resulted from reproduction shall be recorded in the registry for multiplied classified information, Annex 9.

(2) The numbers will be assigned consecutively, starting with figure1, over a calendar year, and shall be applied on all copies of the document.

Art. 68 - (1) Reproduction shall be mentioned both on the original document and on the resulted copies.

(2) On the original documents the mention shall appear at the bottom on the right of the last page.

(3) On the copies the mention shall be applied on the first page, under the registering number of the document.

(4) In case of successive copying at different dates of a classified document, the original document shall be marked at each operation of copying which will be entered in the registry.

(5) The copies resulted from the reproduction of the state secret document shall be numbered successively, even if the operation is done at different times and at different dates.

Art. 69 - (1) Reproduction of classified documents shall be made with the approval of the head of the holding entity and of the security structure/officer, both mentioned on the reproduction request or on the accompanying note mentioning why the reproduction is necessary.

(2) The Prosecutor Office, courts of law and investigation committees shall multiply documents containing classified information only under the terms of these standards.

(3) Excerpts from documents containing classified information are made on the basis of a copy request, with the approval of the head of the organization, and the word “Excerpt” shall be applied on the resulted document below the copy number and the registering number of the original document.

(4) The secrecy class or level assigned to an original document shall be identically applied on the reproductions and translations.

Art. 70 - (1) If the originator wants to have exclusive control on the reproduction, the document shall bear a visible indication saying that: “Partial or total reproduction of this document is forbidden”.

(2) Classified information entered on documents with restrictive reproduction specification, bearing the mention “It is forbidden to reproduce this document” shall not be reproduced.

Art. 71 – In case of copying a document containing classified information the following rules shall apply:

a) the number of needed copies shall be established;

b) the request for reproduction under article 69, paragraph 1, shall be filled in and approved after which it shall be recorded in the register – annex 4 or 5 as the case may be;

c) the original document is given to the copy operator against signature;

d) after verifying the copies resulted, the beneficiary shall sign in the Registry of reproduced classified information, in accordance with Annex 9;

e) repartition for dissemination of reproduced copies shall be mentioned by the security structure/officer at the back of the request for copy;

f) the request for copy and the copies are returned against signature to the security structure/officer for dissemination or transmission.

Art. 72 - (1) When typing, computer processing or copying classified documents in more than two copies, the addressees and the number of copies will be mentioned at the back of the original.

(2) In case the number of addresses is large, a dissemination table shall be drafted which will be registered as a document and annexed to the original document.

(3) The copies shall bear consecutive numbers regardless of the date they were produced, and the number of copies resulted after typing or computer processing shall also be taken into account.

Art. 73 – Classified documents may be microfilmed or stored on optical disks or magnetic supports under the following conditions:

a) microfilming and storage is made, with the approval of the originator, by personnel authorized for the secrecy class or level of the respective information;

b) microfilms, optical disks and magnetic supports shall enjoy the same protection as the original document;

c) all microfilms, optical disks and magnetic supports shall be specifically recorded and annually checked just like the original documents.

Art. 74 - (1) Multiplied classified documents shall be disseminated with the approval of the security structure/officer.

(2) Classified information may be disseminated back to the initial addressee, applying these regulations.

(3) The originator shall indicate all restrictions as to the dissemination of classified information. When such restrictions are imposed, the re-dissemination shall be done only with the written approval of the originator.

Art. 75 – In case a state secret document is consulted by an authorized person for which the need to access such documents has been established in order to fulfill his/her duties, this activity shall be mentioned in the consultation sheet, Annex 1.

Art. 76 - (1) Classified information whose classification period has expired shall be archived or destroyed.

(2) Storage in archives or destruction of a classified document shall be mentioned in the main registry by stating the archive number or the record number of the destruction certificate.

(3) Destruction of replaced or obsolete classified information shall be made only with the approval of the originator.

(4) Destruction of classified documents or rough copies containing classified documents shall be made so that to avoid reconstruction.

Art. 77 - (1) Working documents, rough copies or materials drafted when drawing up a document that contain classified information will be destroyed, as a rule.

(2) In case they are kept, they will be dated, marked with the highest secrecy level of the information contained, recorded and protected according to the secrecy class or level of the final document.

Art. 78 - (1) "Strict secret de importanta deosebita" information meant to be destroyed shall be returned to the issuing entity together with a returning notice.

(2) Each such information shall be recorded in a destruction certificate approved by the head of the organization and signed by the security structure/ officer and the person taking part in the destruction, authorized to have access to "strict secret de importanta deosebita" information.

(3) In emergency cases, the protection, by destruction of "strict secret de importanta deosebita" information shall always against other documents or materials.

(4) The destruction certificates and recording documents shall be kept for at least 10 years.

Art. 79 - **(1)** Destruction of "strict secret", "secret" and "secret de serviciu" information shall be recorded in a destruction certificate signed by

two persons authorized to have for access to information of such level, and endorsed by the security structure/officer and approved by the head of the organization.

(2) The destruction certificates and recording documents for “strict secret”, “secret” and “secret de serviciu” information shall be kept by the compartment that performed the destruction for at least 3 years, and after that they shall be archived and kept for at least 10 years.

Art. 80 - (1) Destruction of rough copies with state secret information shall be made by the persons who have drafted them.

(2) The destruction certificate for rough copies shall be drawn up if these copies have been registered.

Art. 81 - (1) Documents and materials containing classified information are transported on the Romanian territory by the specialized entity of the Romanian Intelligence Service, according to the norms set by Government Decision.

(2) Documents and materials containing classified information are transported abroad by diplomatic pouch, and by diplomatic couriers selected and trained by the Foreign Intelligence Service.

(3) It is forbidden to transmit documents and materials containing classified information by S.N. “Posta Romana” (Romanian Mailing Company) or by other transport companies.

Art. 82 – The heads of the organizations holding classified information shall designate, from their own security structure and under the provisions of these standards, at least one delegate empowered to transport and carry out the delivery/receipt of classified mail between the organization and the specialized entity of the Romanian Intelligence Service.

CHAPTER IV

PROTECTION OF STATE SECRET CLASSIFIED INFORMATION

SECTION 1

Obligations and responsibilities of public authorities and organizations, economic operators and other legal persons as to the protection of state secret information

Art. 83 – Protection of state secret information represents an obligation for all authorized persons who issue, manage or get in possession of such information.

Art. 84 – **(1)** Heads of the organization handling state secret information are responsible for the implementation of the protection measures for this information.

(2) Private legal persons holding state secret information shall comply with and implement the regulations in force established for public authorities and organizations, in their field of activity.

Art. 85 – Until the establishment and organization of the security structure or, as the case may be, until the appointment of a security officer, the heads of organizations handling state secret information shall designate a person to temporary fulfill the specific tasks of the protection of classified information, through plurality of positions.

Art. 86 – **(1)** The head of the entity managing state secret information shall:

a) ensure the organization of the security structure activity, respectively of the security officer and the special compartments designated for the management of classified information, in terms of the law;

b) request the competent organizations to perform security vetting in order to approve the issue of the security clearance and security authorization for access to classified information, for their own personnel;

c) notice ORNISS about the release of the security clearance or security authorization for each employee who works with classified information;

d) approve the list with the cleared personnel to work with state secret information and the record of the security clearance and authorization

holders and communicate them to ORNISS and to the competent organizations which coordinate the activity and control the measures regarding the protection of classified information, according to the law;

e) draw up the list of state secret information and of the terms for maintaining it in the secrecy levels and submit the list to the approval of the Government, in terms of the law;

f) set up the facilities, premises and places from their field of activity of special importance for the protection of state secret information and transmit them to the Romanian Intelligence Service, in order to be submitted for the approval of the Government;

g) request specialized assistance from organizations empowered to coordinate the activity and control the measures for the protection of state secret information;

h) submit the program of his entity regarding the prevention of the leakage of classified information to the approval of the competent organizations and ensure its implementation;

i) work out and apply the physical procedural measures and for the personnel who have access to classified information;

j) draw up the guide based on which the correct and uniform harmonization with the levels of secrecy of the state secret information shall be carried out, in strict conformity with the law, and submit it for approval to the empowered staff and officials who are entitled by law to grant levels of secrecy;

k) ensure the application and observance of the general regulations on the recording, drawing up, maintenance, processing, reproduction, handling, transport, transmission and destruction of the state secret information and the interdiction of reproduction and circulation, in terms of the laws in force;

l) communicate the competent organizations, according to their competence, the list of the subordinate positions which need access to state secret information;

m) when concluding individual work contract, collaboration contract or any other convention, specify the obligations which are incumbent on each part for the protection of classified information within or out of the entity, during the work schedule and after that, as well as at the end of the activity in that entity;

n) ensure the inclusion of the personnel of the security structure/ security officer in the continuous system of training and advanced training, according to these standards;

o) approve the internal norms for the implementation of the measures on the protection of classified information, in all its components and control the way they are observed within the entity;

p) ensure the necessary funds for the implementation of the measures on the protection of classified information, in terms of the law;

q) analyze, whenever necessary but at least half-yearly, the way in which the security structure/officer and authorized personnel ensure the protection of classified information;

r) ensure the yearly inventory of the classified documents and, on this base, take adequate measures in terms of the law;

s) inform the authorities mentioned under Article 25 of Law No. 182/2002, of the security breaches and risks regarding the state secret information, according to their competence;

t) request investigations and, if required, inform the competent prosecution bodies if compromise of classified information occurs;

(2) The organizations mentioned under Article 25 of Law No. 182/2002 are exempted from the provisions of the paragraph (1), letters f) and h).

SECTION 2
Legal protection

Art. 87 – The heads of the entities managing state secret information shall ensure the necessary conditions so that all the persons handling such information could know the regulations in force on the protection of classified information.

Art. 88 (1) – The heads of the entities managing state secret information shall inform, in writing, the organizations mentioned under Article 25 of Law No. 182/2002, about the compromise of such information, through the most operative communication system and according to their competences.

(2) The notification mentioned under paragraph (1) is made in order to obtain the necessary support to recover information, assess prejudices, reduce and remove the consequences.

(3) The notification shall contain:

a) the presentation of the compromised information, respectively its classification, marking, content, date of issue, registration number, number of copies, the originator and the person or compartment managing it;

b) a short presentation of the circumstances under which the compromise took place, including the date when it occurred, the period of time when the information was exposed to compromise and the unauthorized individuals who had or could have had access to it, if known;

c) statements about the potential information of the originator.

(4) At the request of the competent organizations, the preliminary notices shall be filled in during the security investigation.

(5) The documents regarding the assessment of the prejudices and the actions that are to be taken as a result of compromise shall be submitted to the competent organizations.

Art. 89 – The holder of the compromised state secret information is entitled to civil compensations, in compliance with the civil law, for the prejudices caused to him.

Art. 90 – **(1)** Any breach of the security regulations shall be investigated in order to establish:

a) if the respective information has been compromised;

b) if unauthorized persons who had or could have had access to state secret information are trustworthy and loyal enough, so as the result of the compromise should not create prejudices;

c) adjustment measures – corrective, disciplinary or legal – which are recommended.

(2) In case unauthorized persons have accessed classified information, they will be briefed in order to prevent the occurrence of possible prejudices.

(3) In case of offences regarding the protection of state secret information, the entities holding such information shall notify the prosecution authorities and shall make available the materials and data necessary for establishing the facts.

Art. 91 – **(1)** The security structure/officer shall keep the record of the situations referring to infringement of the security regulations, of investigation documents and of settlement measures and shall make them available for the DSAs, according to their competences.

(2) The documents mentioned in paragraph (1) shall be kept for five years.

Art. 92 Disputes regarding the quality of originator or holder or caused by the content of state secret information, including the issuer's patrimonial rights from the deeds of assignment and license, as well as the disputes regarding the inobservance of the legal provisions on the copyright and afferent rights, inventions and innovations, protection of industrial patterns, the fight against non-loyal competition and those mentioned in treaties, agreements and conventions Romania is part of, are under the competence of law courts.

SECTION 3
Protection through procedural measures

Art. 93 – All entities holding state secret information shall establish internal working norms and regulations on the protection of such information, according to the normative acts in force.

Art. 94 – **(1)** The procedural measures on the protection of state secret information shall be included in the prevention program for classified information leakage, drawn up according to Appendix 10, that will be submitted, for approval, to the competent authority which coordinates the activity and controls the measures on the protection of classified information, according to the law.

(2) The organizations referred to under article 25, paragraph (4) of Law No. 182/2002 are exempted from the obligation to submit for approval, the preventive program for classified information leakage, mentioned under paragraph (1).

Art. 95 – The confidentiality statements drawn up according to the regulations in force shall guarantee that the information to which access is granted is adequately protected.

SECTION 4
Physical protection

Art. 96 – Facilities, premises and places where state secret information is handled must be physically protected against unauthorized access.

Art. 97 - The physical security measures – window bars, security locks, entrance guards, automatic systems for surveillance control and access, security patrols, alarm systems, means for the detection of overlooking, eavesdropping or interception – shall be established according to:

a) the secrecy level, amount and place of information;
b) the type of containers where information is stored;
c) the characteristics of the building and place.

Art. 98 - Areas where state secret information is handled and stored must be organized and structured so as to correspond to one of the following categories:

a) ***Class I Security Area*** which requires that any person within this area has access to state secret information of “strict secret de importanta deosebita” and “strict secret” levels; this area requires:

- a clearly defined and protected perimeter to which all entries and exits are monitored;
- a control of the entry system which shall grant access only the appropriately cleared and specially authorized individuals;
- specification of the secrecy level of information held in the area.

b) ***Class II Security Area*** which requires that management of “secret” information is done by applying specific protective measures against the access of unauthorized persons; this area requires:

- a clearly defined and protected perimeter to which all entries and exits are monitored;
- a control of the entry system which shall grant unescorted access only to individuals cleared and authorized to enter this area;
- rules for escorting, monitoring and preventing the access of unauthorized persons to classified information.

Art. 99 – Those premises which are not occupied by personnel 24 h/day shall be checked immediately after normal working hours, to ensure that state secret information is properly secured.

Art. 100 – An ***administrative area*** may be established around the Class I or Class II Security Areas, with a visibly delimited perimeter where the control of personnel and vehicles may take place.

Art. 101 – **(1)** Access to Class I and Class II security areas shall be controlled by checking the entry pass or by an individual recognition system applied to the staff.

(2) The entities holding state secret information shall establish their own control system of the visitors, for denying their unauthorized access in the security areas.

Art. 102 – The pass shall not clearly specify the identity of the issuing entity or the place to which the holder has access.

Art. 103 – The entities shall organize, on entry to or exit from a Class I or Class II security area, planned or random checks of luggage, packages, bags and other kind of devices which may transport state secret information and material.

Art. 104 – The personnel of the guard and defense system of the facilities, premises and places in which state secret information is

managed, shall hold access authorization for the appropriate secrecy information level necessary to fulfill their tasks.

Art. 105 – Access with cameras, video-cameras, audio-video recording cameras, devices for copying information from informatics data-bases or for remote communication is forbidden in places where state secret information is held.

Art. 106 – The heads of the entities holding state secret information shall establish rules regarding the circulation and internal regulation in the security areas, so that the access be granted exclusively to the holders of security clearances and access authorizations, on the basis of need-to-know principle.

Art. 107 – Access for technical interventions, repairing works or other such activities to places where state secret information is handled, stored, processed or reproduced is allowed only to the entity employees holding appropriate access authorizations for the highest secrecy level of information they might be in possession of.

Art. 108 – (1) For better distinguishing the persons who have access to different places or premises where state secret information is handled, they shall wear specific badges or equipment.

(2) In the places and premises where state secret information is managed, the specific badges and equipment shall be established through internal order regulations.

(3) The recording of the identification cards, passes and other specific badges and equipment shall be kept by the security structure/officer of the entity.

Art. 109 - (1) Individuals who lose their access passes, specific badges or equipment shall immediately inform their hierarchic boss.

(2) In the situations referred to under paragraph (1), the head of the entity shall require the investigation of the circumstances and shall inform the competent Designated Security Authority.

(3) The security structure/officer shall take all the necessary measures for the prevention of using, by unauthorized persons, of the passes, specific badges or equipment.

Art. 110 – Access of each employee of the entity holding state secret information, to Class I or Class II security areas, shall be made through specially established entries, based on the access pass, signed by the head of the entity.

Art. 111 - (1) Access passes shall be individualized by applying specific signs.

(2) Access passes shall be endorsed half-yearly.

(3) At the end of the work contract the passes shall be withdrawn and cancelled.

Art. 112 – Access of other persons, besides those having access passes to places where state secret information is managed is forbidden.

Art. 113 – Access of individuals from outside the entity to the Administrative Area or to the security areas is allowed only if they are escorted by persons specially designated, and if they own access tickets released by the head of the entity on the basis of the identity documents.

Art. 114 - (1) Access of employees of economic operators involved in construction, repairing and maintenance works of the buildings equipment or utilities within the Administrative Areas or Security Areas, shall be done by means of temporary access documents released by the heads of the beneficiary entities, on the basis of identity documents, at the request of the authorized representatives of the economic operators.

(2) The places where the works referred to under paragraph (1) are carried out shall be monitored by persons specially designated from the beneficiary entity.

(3) The temporary access document is valid during the execution of works, is endorsed half-yearly, and at the end of the activity is returned to the issuing organization.

(4) Loss of the temporary access document shall be recorded by the security structure/officer that will require the necessary measures to be taken for preventing unauthorized persons to use it.

Art. 115 – The representatives of the organizations which, according to the legal competences, have tasks of coordination and control in the field of the protection of classified information, have access to objectives, premises and places where classified information is handled, on the basis of the job card and special delegation, signed by the head of authority they represent.

Art. 116 – The persons who are in the practical period of documentation, training stages or sharing of experience have access only to the places established by the head of the entity, on the basis of the access passes released to this end.

Art. 117 – The persons who apply for work, audiences or who have complaints and claims to make, shall be received outside the administrative areas or in special places, with the approval of the head of the entity.

Art. 118 – During the periods which exclude the working schedule and in the non-working days, patrols of the unit perimeter shall be organized, at intervals of time established in the instructions issued on the basis of the guard and defense plan of the objective.

Art. 119 – (1) The guard, surveillance and access control systems must ensure the prevention of unauthorized intrusion in objectives, premises and places where classified information is handled.

(2) The time of reaction of the guard personnel shall be periodically tested in order to guarantee the operative intervention in emergency situations.

Art. 120 – **(1)** Entities managing state secret information shall draw up the guard and defense plan for objectives, premises and places which are of relevant importance for the protection of classified information.

(2) The guard and defense plan referred to under paragraph (1) shall be registered according to the highest level of secrecy of the protected information and shall include all the security measures to be taken for the prevention of unauthorized access to them.

(3) The guard and defense plan shall be attached to the program for the prevention of the classified information leakage and shall include:

a) data regarding the delimitation and marking of the security areas, the positioning of the guard posts and the surveillance measures for the protected perimeter;
b) the access control system to the security areas;
c) the warning and alarming measures for the emergency situations;
d) the eviction plan of the documents and the modality of action in emergency situations;
e) the procedure for reporting, investigation and accounting of security breaches.

Art. 121 – State secret information is kept in special containers:

a) ***Class A containers***, nationally approved for the storage of "strict secret de importanta deosebita" information in the Class I security area;
b) ***Class B containers,*** nationally approved for the storage of "strict secret" and "secret" (secret and confidential) information in Class I or Class II security areas.

Art. 122 – (1) Class A and Class B containers shall be built in such way as to ensure the protection against surreptitious entry and damage of any kind to the information.

(2) The standards for class A and B containers shall be drawn up by ORNISS.

Art. 123 - (1) Strong rooms are rooms specially designed within Class I or Class II security areas, where state secret information may be kept on open shelves or where maps, drawings or diagrams may be displayed.

(2) Walls, floors, ceilings, doors and lockers of the strong rooms shall ensure the protection equivalent to the class of the security container approved for the storage of classified information according to its secrecy level.

Art. 124 - **(1)** Windows of the strong rooms located on the ground floor or on the top floor shall be protected with bars fixed in the concrete or ensured against surreptitious entry.

(2) After the normal working hours, the doors of the strong rooms shall be sealed, and the ventilation system shall be ensured against unauthorized access and introduction of flammable materials.

Art. 125 - In emergency situations, if the state secret information must be evicted, nationally authorized metallic cases of the class corresponding to the secrecy level of information shall be used.

Art. 126 – Locks used for containers and strong rooms where state secret information is stored, are divided into three categories:

a) **Group A** – authorized locks for Class A containers;
b) **Group B -** authorized locks for Class B containers;
c) **Group C** – locks for office furniture.

Art. 127 - ORNISS shall establish the standards of the locking mechanisms, of the cipher and locks systems, on usage groups.

Art. 128 - The keys of containers and strong rooms shall not be removed from the security areas.

Art.129 – **(1)** After the normal working hours, the keys of the containers and strong rooms shall be kept in sealed boxes by the guard and defense personnel.

(2) The keys of containers and strong rooms shall be handed over and received, under signature, in the special register, – Annex 11.

Art. 130 - **(1)** In case of emergency, a set of spare security keys or, as the case may be, a written note of the combination locks shall be kept in dark sealed envelopes, in separate containers, in a compartment established by the senior management of the organization, under appropriate control.

(2) The note of each combination shall be kept in a separate envelope.

(3) The keys and the envelopes with combinations shall be ensured the same level of protection as for the information to which they provide access.

Art. 131 – The combination locks of the containers and strong rooms will be known by a minimum number of persons designated by the head of the unit.

Art. 132 - The keys and the combination locks shall be changed:

a) each time there is a change of personnel;
b) each time there are situations which could make them vulnerable.
c) at regular intervals, preferably once in six months, but not exceeding 12 months.

Art. 133 – (1) Electronic alarm systems or surveillance systems designated for the protection of state secret information shall have spare power sources.

(2) The security personnel monitoring the alarm systems shall be warned about any malfunction or unauthorized intervention on the alarm or surveillance systems designated for the protection of state secret information.

(3) The alarm systems shall be active in case of penetration of the walls, floors, ceilings and locks, or at movements inside the strong rooms.

Art. 134 – Copy machines and fax devices shall be placed in special designated rooms and shall be used only by the authorized persons, according the secrecy level of information to which they have access.

Art. 135 – The entities holding state secret information shall ensure their protection against unauthorized active or passive eavesdropping.

Art. 136 – **(1)** Protection against passive eavesdropping of the confidential talks is made by means of phonic isolation of the rooms.

(2) Protection against active eavesdropping, by means of microphones, radio-transmitters and other implanted devices, shall be made by security inspections of the rooms, accessories, installations, communication systems, equipment and office furniture, carried out by special entities, in terms of the legal competences.

Art. 137 – **(1)** Access to the rooms protected against eavesdropping shall be particularly controlled.

(2) Periodically, the specialized personnel in finding the listening devices shall carry out physical and technical inspections.

(3) Physical and technical inspections shall be set up, after any unauthorized entry or suspicions regarding the access of unauthorized persons and after execution of repairing, maintenance, painting and redecoration works.

(4) No object shall be introduced into the rooms protected against eavesdropping, without being checked before by the personnel specialized in finding listening devices.

Art. 138 – **(1)** In areas where confidential talks take place and are ensured from a technical point of view, telephones will not be installed, and if their installation is absolutely necessary, they shall be provided with a passive unplugging device.

(2) Security technical inspections in the areas mentioned under paragraph (1) shall be conducted before the beginning of the talks, for the physical identification of the listening devices and checking of the telephonic or electrical systems or of other systems, which may be used as an attack media.

Art. 139 – **(1)** The communication equipment and the office facilities, especially the electric and electronics, shall be verified by the specialists of the competent DSA, before being used in the areas where “strict secret” and “strict secret de importanta deosebita” information is handled, in order to prevent the transmission or interception, outside the legal frame, of intelligible information.

(2) For the areas mentioned under paragraph (1), a record shall be kept with the type and the inventory numbers of the equipment and furniture moved inside or outside the rooms, which will be considered as state secret material.

SECTION 5
Personnel Security

Art. 140 – (1) Entities holding state secret information shall ensure the protection of the personnel assigned to safeguard this information or of the personnel that has access to such information, according to these standards.

(2) The protective measures for the personnel shall:

a) prevent access of unauthorized persons to state secret information;

b) guarantee that state secret information is released to the holders of security clearance/security authorizations, with the observance of the need to know principle;

c) identify those persons who, by their action or inaction, can endanger the security of state secret information and prevent their access to such information;

(3) Personnel protection shall be done by: selection, vetting, approval and authorization of access to state secret information, revalidation, control and briefing of the personnel, withdrawal of the security clearance/security authorization.

Art. 141 – (1) Granting of the security clearance – annex no. 12 – and of the access authorization to classified information – annex no. 13, according to the secrecy level, is conditioned by the approval of the designated security authority.

(2) In order to issue the security clearance/access authorization, the head of the entity requests, in writing, ORNISS, according to annex no. 14, to conduct the security vetting of the person who is going to be granted access to state secret information.

(3) The application under paragraph (2) shall be accompanied by the special forms, provided in annexes no.15, 16 and 17, according to the secrecy level of information, filled in by the respective person, introduced into separate sealed envelopes.

(4) Depending on the approval notice communicated by the designated authority, ORNISS shall approve the issuing of the security clearance/security authorization and shall officially notify the head of the organization.

(5) After obtaining the approval mentioned under paragraph 4, the head of the organization shall notify ORNISS and shall issue the security clearance/security authorization, according to article 154.

Art. 142 – The Security clearance/security authorisation shall be issued only based on the approval notices given by the designated security authority following the vetting of the respective person, with his/ her written consent.

Art. 143 – Within the approval procedures special attention shall be paid to the persons who:

a) are going to have access to “strict secret” and “strict secret de importanta deosebita” information;

b) have positions that require permanent access to a large amount of state secret information;

c) can be vulnerable to hostile actions, as a result of the importance of the function in which they shall be assigned, of the relation background or of the former working place.

Art. 144 – (1) The necessity of the approval notice shall be evaluated based on the vetting and on the background investigation of the respective person.

(2) When the individuals are going to be assigned to functions that could facilitate access to state secret information only under certain circumstances – guards, couriers, maintenance personnel – attention shall be paid to the first security vetting.

Art. 145 – Entities that manage classified information shall keep a register of security clearances/security authorizations for access to classified information – annex no. 18.

Art. 146 – (1) Whenever there are signs that the holder of the security clearance/security authorization no longer fulfills the compatibility criteria regarding access to state secret information, the security vetting shall be resumed at the request of the head of the organization transmitted to ORNISS.

(2) ORNISS may require resumption of the vetting at the notification of competent authorities, when incompatibilities regarding access to state secret information are signaled.

Art. 147 – The vetting procedure for the granting of access to state secret information is aimed at identifying security risks corresponding to the management of state secret information.

Art. 148 – (1) The security structure/officer shall make available for the assigned person the standard forms corresponding to the level of access for which the security clearance/access authorization is required and shall give assistance for their filling in.

(2) Depending on the secrecy level of information for which the security approval is requested, the deadlines for an answer from the organizations authorized to conduct the security vetting are:

a) for access to “strict secret de importanta deosebita” information – 90 working days;

b) for access to “strict secret” information – 60 working days;

c) for access to “secret” information – 30 working days.

Art. 149 – Within 7 (seven) working days from receiving the request, ORNISS shall transmit to the competent designated security authorities the standard request for starting the vetting procedure – annex no. 19, to which it shall attach the sealed envelope with the standard forms filled in.

Art. 150 (1) After receiving the forms, the authorized organization shall conduct the vetting within the deadlines stipulated under article 148

and shall communicate in writing – annex no. 20 – to ORNISS the approval regarding the granting of the security clearance/access authorization to classified information.

(2) If security risks are identified, the DSA shall assess if these are an obstacle for granting the security approval.

(3) If relevant elements regarding the protection of state secret information are signaled, the security interests shall prevail in making the decision of granting the security notice.

Art. 151 – (1) Within 7 working days since the reception of the answer from the designated security authority, ORNISS shall decide upon granting the security clearance/access authorization to state secret information and shall transmit it to the applicant unit – annex no. 21.

(2) The notification address of ORNISS' decision shall be done in 3 copies, of which one is sent to the applicant entity and the second to the organization that conducted the vetting.

(3) If the notice is positive, the head of the applicant entity shall issue the security clearance to the person referred to, after previous notification at ORNISS – annex no. 22.

Art. 152 - (1) The vetting for access to state secret information shall be conducted by the following organizations, with the observance of the legislation in force on the responsibilities in the field of the protection of such information,:

a) **Romanian Intelligent Service** for:
- its own personnel,
- personnel belonging to the authorities and public organizations in the competence area, according to the law,
- personnel belonging to economic operators with state integral or partial capital and to public or private legal persons, other than those given to the competence of the organizations mentioned under the letters b), c) and d) of this article;

b) **Ministry of Defense** for:
- its own military and civil personnel,
- personnel belonging to the Central State Office for Special Issues, to the National Administration of State Reserve, to the legal persons established by law and the military personnel that develops its activity abroad;

c) **Foreign Intelligent Service** for:
- its own military or civil personnel,
- Romanian personnel belonging to diplomatic representatives, to permanent consular missions, to cultural centers, international organisms and to other representatives of the Romanian state abroad,

- foreign citizens abroad within contracts, advanced training stages, research programs or as employees in companies;

d) **Ministry of Interior**, **Ministry of Justice**, **Guard and Protection Service**, and **Special Telecommunications Service** for their own personnel and belonging to the legal persons, whose activity they coordinate.

(2) Organizations mentioned under paragraph (1) are authorized to request and receive information from legal and natural persons in view of granting the access authorization to classified information.

Art. 153 – The competent entities for conducting the security vetting shall cooperate, based on protocols, in fulfilling their tasks and objectives.

Art. 154 – The Security clearance/ access authorization is issued in two original copies; one is kept by the security structure/officer and the other one is sent to ORNISS, which shall inform the competent organization that conducted the vetting.

Art. 155 – The validity of the security clearance/ access authorization issued for a person is up to 4 years; during this period, the vetting can be resumed whenever the conditions stipulated in article 167 are achieved.

Art. 156 – For its own personnel, the Ministry of Defense, Ministry of Interior, Ministry of Justice, Romanian Intelligence Service, Foreign Intelligence Service, Special Telecommunications Service and Guard and Protection Service shall work out internal instructions regarding the vetting, approval, issuance and accountability of the security clearances/access authorizations.

Art. 157 – The decision regarding the issuance of the security clearance/access authorization shall be made on the basis of all available information and shall take account of:

a) undeniable loyalty of the person,

b) character, habits, relations and discretion of the person, which could offer guaranties on:

- correctness in the management of the state secret information,
- suitability of unescorted access to security compartments, facilities, premises and places where state secret information is stored,
- observance of the regulations on the protection of state secret information in his/ her field of activity.

Art. 158 – (1) The main criteria for assessing eligibility when granting the security approval for the issuance of the security clearance/access authorization take into account both the character features and the

situations or circumstances that may lead to security vulnerabilities and risks.

(2) The character, professional and social conduct, conceptions and life environment of the husband/wife or spouse of the petitioner shall be considered relevant and taken into account when issuing the security approval notice.

Art. 159 – The following situations which are imputable both to the petitioner and to his/ her husband/ wife, spouse, or cohabitant represent elements of incompatibility for access to state secret information:

a) if he/she committed or attempted to commit, conspired with or aided and abetted another to commit any act of espionage, terrorism, treason or other offences against the state security;

b) if he/she attempted, encouraged, participated in, cooperated with or supported acts of espionage, terrorism or persons suspected to belong to this category or to be members of foreign organizations or powers that are against the lawful order in our country;

c) if he/she is or was a member of any organization that sought, seeks or supports the overthrow of the constitutional order by violent, subversive or other illegal means;

d) if he/she is or was a supporter of any organization stipulated at letter c), is or has recently been closely associated with members of such organizations in such a way as to raise justified suspicions regarding the person's trustworthiness and loyalty.

Art. 160 – Any of the following situations can be elements of incompatibility for the petitioner's access to state secret information, if he/she:

a) deliberately withheld, misrepresented or falsified of significance information with relevance, particularly of a security nature, or has deliberately lied in completing the personnel security forms or during the course of the security interview;

b) has been convicted of a criminal offence, or offences indicating habitual criminal tendencies;

c) has serious financial difficulties or there is a significant disagreement between his/her life-style and declared income;

d) has a history of alcohol dependence or is drug-addicted or addicted to other substances banned by the law;

e) has or had immoral conduct, or deviations of conduct, which may give rise to the risk of the person's vulnerability to blackmail or pressure;

f) has demonstrated disloyalty, dishonesty, unreliability or indiscretion;

g) has infringed regulations regarding the protection of classified information;

h) is suffering or has suffered from physical or mental diseases which may cause defects of judgement confirmed by medical investigation conducted with the petitioner's consent;

i) may be liable to pressure through relatives or close associates who could be vulnerable to foreign intelligence services whose interests are hostile to Romania and its allies.

Art. 161 – (1) Requests for conducting the security vetting in view of approving the issuance of the security clearances/access authorizations to state secret information, shall take into consideration the persons who:

a) in exercising their duties work with data and information of the "secret" level;

b) belong to the executive and administrative personnel and, by virtue of this, can come into contact with data and information of this level,

c) due to the position they own, are supposed to work with data and information of the "secret" level;

d) are supposed not to be professionally promoted in their position, if they do not have access to such information.

(2) The approval for access to state secret information of the "secret" level shall be based on:

a) checking the correctness of data mentioned in the Basic Form, annex no.15;

b) recommendations from the employment places and from the frequented groups of people, at least from three persons.

(3) If clarification of certain aspects is required or at the request of the vetted person, the representative of the organization authorized to conduct the security vetting may have a meeting with this person.

Art.162 – (1) In order to issue security clearance/ access authorization to "strict secret" (secret) information vetting is done upon persons who:

a) in exercising their duties work with data and information of the "top secret" level;

b) belong to the executive and administrative personnel and, by virtue of this, can come into contact with data and information of this level;

c) due to the position they own, are supposed to work with data and information of the "top secret" level;

d) are supposed not to be professionally promoted in their position, if they do not have access to such information.

(2) The approval for access to state secret information of the "top secret" level shall be based on:

a) checking the correctness of data mentioned in the Basic Form and in the Additional Form, annex no.15 and 16;

b) minimum recommendations from places of employment and from frequented groups of people, at least from three persons;

c) checking the data presented in the form about family members;

d) enquiries at the place of employment and at the residence, that should cover a period of 10 years prior to the date of the approval notice, or starting with the age of 18;

e) an interview with the vetted person, if it is considered that this could clarify aspects resulted from the vetting.

Art. 163 – (1) In order to issue security clearances/ access authorizations for "strict secret de importanta deosebita", vetting shall be conducted on the persons who:

a) in exercising their duties, work with data and information of the "strict secret de importanta deosebita" level;

b) belong to the executive and administrative personnel and, by virtue of this, can come into contact with data and information of this level;

(2) The approval for access to "strict secret de importanta deosebita" information shall be based on:

a) checking the correctness of data mentioned in the Basic Form and in the Additional Form, annex no.15,16 and 17;

b) enquiries to find out the conduct and antecedents at the present and previous place of employment and at the present and previous residence, as well as at the education establishments attended, starting with the age of 18 and shall not be limited only to the hearing of the persons indicated by the petitioner of the approval notice;

c) enquiries on the environment attended in order to identify the existence of security risks within it;

d) an interview with the petitioner, in order to detail aspects resulted from the enquiries;

e) if after the enquiries, there are uncertainties regarding the physical sanity or behavior of the vetted person, he/she can undergo a psychological test with his/ her consent.

Art. 164 – (1) If during the vetting on any level, there is information that highlights security risks, a supplementary vetting shall be conducted using methods and means specific to organizations with competence in the national security field.

(2) In case of supplementary vetting mentioned under paragraph 1, the vetting deadlines shall be prolonged accordingly.

Art. 165 – According to the secrecy level of state secret information to which access is granted, the enquiry for finding out antecedents shall gradually take into consideration the following:

a) consultation of the civil status registers for checking the personal data in order to establish, without any doubt, the identity of the petitioner;

b) checking of the police central and local criminal record, in the database of the Commercial Register, as well in other records;

c) establishing the person's nationality as well as present and previous citizenship;

d) confirmation of training in schools, universities and other educational establishments attended by the petitioner, since the age of 18;

e) finding out about the conduct at present and previous place of employment, with recommendations obtained from employment files, annual appreciations of the performances and efficiency of activity, or provided by the heads of organizations and compartments or by the colleagues;

f) organizing interviews and discussions with persons who could make appreciations on the background, activity, behavior and honesty of the vetted person;

g) finding about his behavior during military service and type of discharge;

h) existence of security risks due to possible pressure exercised from abroad;

i) solvency and financial standing of the person;

j) identifying signs and obtaining evidence according to which the petitioner is or was a member of or an affiliate to any organization, association, movement, foreign or national group of persons, who supported or encouraged acts of violence, in order to impinge on other persons' rights, or who seek to change the form of government by unlawful means;

Art. 166 – (1) If a person has security clearance/ access authorization to national classified information, he/ she can be also issued security clearance for access to NATO classified information valid for the same level of secrecy or for a lower level.

(2) If classified NATO information to which access is requested under the provisions of paragraph (1) is of a higher level than the one for which the person referred to has security clearance/access authorization, the necessary vetting shall be conducted according to the standards in force.

(3) Validity of security clearance/authorization issued under the provisions of paragraph (1) and (2) shall cease when the validity deadline of the initial clearance/ authorization expires.

Art. 167 – (1) Revalidation of the approval notice regarding access to classified information implies re-vetting the holder of the security clearance/ access authorization, with a view to keeping or withdrawing it.

(2) Revalidation may be done at the request of the unit where the person is working, or of ORNISS, in any of the following situations:

a) when exercising his/her duties, the holder needs access to information of a higher level;

b) when the validity period of the security clearance/access authorization previously possessed has expired;

c) in case there are modifications in the identification data of the holder;

d) when there are security risks regarding the eligibility for access to classified information.

Art. 168 – When requesting revalidation, a new security clearance/access authorization shall not be issued in the following situations:

a) in case of non conformance between the data stated in the standard form and the real ones;

b) in case of security during the validity period of the security clearance/access authorization;

c) in case ORNISS specifically requests it.

Art. 169 – For revalidation of access to state secret information the same activities as for issuing initial notice shall be performed and vetting shall be reported at the period from the issuing of the previous security clearance.

Art. 170 – (1) Persons who are issued security clearances/access authorizations shall be briefed regarding the protection of classified information, before starting activity and whenever necessary.

(2) Training activity shall be carried out according to a plan in order to prevent, counteract and eliminate risks and threatening of the security of classified information.

(3) Personnel training is performed differentially, according to the secrecy level of information to which the security clearance or access authorization grants access and shall be registered in the personal training record which is kept at the security structure/ officers.

(4) All persons hired in positions that imply access to classified information shall be thoroughly briefed on the necessity and means of ensuring protection of this information, both before their appointment, as well as at pre-established intervals.

(5) After each period of briefing, the person holding a security clearance or access authorization shall sign that he/she is aware of the content of the regulations regarding the protection of state secret information.

Art**. 171 – (1)** Briefing of the personnel aims at a correct assimilation of the security standards and of the means for an efficient implementation of the measures regarding the protection of classified information.

(2) The designated security authorities shall organize and coordinate the briefing of the security structures/officers.

Art. 172 – (1) The security structure/officer shall plan and organize the briefing of the personnel.

(2) Designated security authorities shall monitor, according to their competences, the performance of the personnel briefing.

Art. 173 – (1) Individual briefing of the persons holding security clearances/access authorizations shall be carried out according to their professional duties.

(2) All persons managing classified information shall know the regulations for the protection of classified information and the internal procedures of applying specific security measures.

Art. 174 – (1) Training of the personnel shall be made by lessons, briefings, lectures, symposiums, exchange of experience, seminars, practical meetings, and can be finalized by exams or certificates attesting the level of knowledge.

(2) Training activities shall be organized by the security structure / officer in compliance with the themes included in the curriculums approved by the heads of the unit.

Art. 175 – Security clearance/ access authorization ceases its validity and shall be withdrawn in the following cases:

a) at ORNISS request,

b) upon decision of the head of the unit that issued the clearance/ authorization,

c) at the request of the competent designated security,

d) when the holder leaves the unit or changes his/ her place of work within the unit, if the new place of work does not suppose working with such state secret information,

e) when the level of access is changed.

Art. 176 – When the security clearance/ access authorization is withdrawn, under the provisions stipulated in Article 175, letters a)-d), the employee shall be denied access to state secret information and the head of the unit shall notify this to ORNISS.

Art. 177 – After making the decision of withdrawal, the unit shall require ORNISS to return copy no.2 of security clearance/ access authorization, after which it shall destroy both copies based on a destruction certificate.

SECTION 6

Access of foreign citizens, Romanian citizens with dual citizenship, as well as of stateless persons, to state secret information and to the places where such activities are developed, objects are exhibited or works of this kind are executed

Art. 178 - Foreign citizens, Romanian citizens with dual citizenship, as well as stateless persons may have access to state secret information, based on the need-to-know principle and on conventions, protocols, contracts and other agreements concluded in compliance with the law.

Art. 179 - (1) The individuals mentioned under Article 178 shall be vetted and cleared according to these standards, at the request of the head of the unit within they are going to carry out activities involving access to state secret information.

(2) On the basis of ORNISS consent, the head of the unit shall issue to the respective individuals access authorization according to the secrecy level of the information to which they will have access, valid only for the period when common activities are carried out.

Art.180 - (1) The individuals mentioned under Article 178 who carry out technical assistance activities, consulting, scientific collaboration or specialization shall wear badges different from those used by the personnel and they shall permanently be accompanied by individuals specially appointed by the head of the unit.

(2) The unit head shall strictly delimit the areas and departments where the individuals mentioned under Article 178 may have access to and shall take measures in order to prevent their presence in other places where state secret information is managed.

Art. 181 - (1) The security structure/officer shall brief the individuals mentioned under Article 178 on the rules they have to comply with in the field of state secret information protection.

(2) The access authorization shall be issued only after the individuals have become familiar with the regulations on the protection of classified information and after they have signed the confidentiality statement.

Art. 182 – Non-observance by the individuals mentioned under Article 178 of the rules on the protection of classified information shall imply the withdrawal of their access authorization.

CHAPTER V
PROVISIONS FOR PHOTOGRAPHING, FILMING, MAP DRAWING AND EXECUTION OF WORKS OF FINE ARTS IN FACILITIES AND PLACES OF SPECIAL IMPORTANCE FOR THE PROTECTION OF CLASSIFIED INFORMATION

Art. 183 - (1) Photographing, filming, map drawing and execution of works fine arts on the territory of Romania, in facilities, areas or places of special importance for the protection of state secret information, without special authorization issued by the ORNISS is forbidden. ORNISS shall keep records on these special authorizations, according to annex no. 23.

(2) The special authorization shall be issued by ORNISS on the basis of the security notice released by the DSA, as well as by the authorities and organizations that have facilities, areas and places of special importance for the protection of classified information in area where activities of this kind are to be carried out.

(3) The facilities and means mentioned under Article 17 of Law no.182/2002 can be filmed and photographed by the military personnel for the internal needs of the military organizations, based on the written approval of the ministries or heads of the respective organizations for the facilities, areas or places in their competence.

Art. 184 – The troops of the Ministry of National Defense, Ministry of Interior and Romanian Intelligence Service which train and perform practical activities or are located within the facilities mentioned under Article 17 of Law no.182/2002, can be photographed or filmed for instructive and military training purposes, with the approval of the heads or of persons mandated of these organizations.

Art. 185 - Photographing, filming, map drawing or execution of works of fine arts in the security or administrative areas of the organizations holding state secret information, are allowed only with the written consent of the persons mandated to grant secrecy levels as stipulated under Article 19 of Law no. 182/2002, according to their material competences.

Art. 186 - (1) The request sent to the ORNISS for issuing the special authorization for filming, photographing, map drawing or execution of works of fine arts shall also mention the subject and place of activity, the equipment used, the period in which these activities shall be carried out, the identity of the person who will carry them out, as well as the approval mentioned under Article 185.

(2) The response deadline shall be of 60 working days from the day when the request was received.

(3) Before starting the activities, the holders of special authorizations shall present themselves to the heads of the organizations where these activities shall be conducted in order to agree on the way of carrying out the activities and for the checking of the equipment to be used.

Art. 187 – If the applicant holds access authorization of a level corresponding to that of the respective facility, the special authorization shall be issued within 15 working days from the date when the request was received, with the observance of the need-to-know principle.

Art. 188 – The facilities, areas and places where photographing, filming, map drawing or execution of works of fine arts are carried out, only upon approval, shall be marked with interdiction indicators, placed by organizations to which they belong, with the authorization of the local public administration.

Art. 189 - (1) The issuing, possession or use of geodetic topo-photogrammetric and cartographic information and documents, which are state secrets, shall be treated in the same way as provided in regulations in force on the protection of classified information in Romania, regarding their classification, marking, inscription, processing, handling, accounting, drawing up, multiplication, transmission, storage, transport and destruction.

(2) The ministries and the other central and local public administration bodies, which draw up state secret geodesic, topo-photogrammetric and cartographic documents, shall include these documents in their own lists of classified information, according to the legal provisions in force.

Art. 190 – Air-filming and air-photographing shall be carried out in the presence of a representative from the Ministry of National Defense, who, at the end of the activity, shall take and process the negatives consulting with the designated security authorities and shall submit the processed material to ORNISS, in order to be delivered to the beneficiaries.

CHAPTER VI
CONTROL OF THE MEASURES REGARDING THE PROTECTION OF CLASSIFIED INFORMATION

Art. 191 - (1) The Romanian Intelligence Service, through its specialized unit, has general competence in controlling the implementation of the protective measures by public organizations and units holding classified information.

(2) The control activity within the Ministry of National Defense, Ministry of Interior, Ministry of Justice, Romanian Intelligence Service, Foreign Intelligence Service, Guard and Protection Service, Special Telecommunications Service is established under the orders of the heads of these organizations, according to the law.

(3) The control of the protective measures for classified information within the Parliament, Presidential Administration, Government and the Supreme Council of National Defense shall be performed in compliance with the law.

(4) The Foreign Intelligence Service establishes and performs the control activity within Romania's diplomatic missions abroad.

Art. 192 – The control activity is aimed at:

a) assessing the efficiency of substantial protective measures applied within different holders of classified information, according to the law, to the provisions of these standards and other norms in the field, as well as to the programs for preventing classified information leakage;

b) identifying the vulnerabilities existent in the classified information protection system which might lead to the compromise of such information, in order to take the appropriate preventing measures;

c) taking measures in order to remedy the deficiencies and to improve the organizational and functional framework at the level of the controlled structure;

d) finding the cases of infringements of norms on the protection of the classified information and imposition of sanctions or, in case of criminal offence, informing the prosecution authorities;

e) briefing the Supreme Council of National Defense and Parliament on the implementing by the organizations holding classified information, of the regulations in the field.

Art. 193 - (1) Each control shall end with a report of the findings, drawn up by the team/ person who conducted the control.

(2) If the control reveals facts and deficiencies representing major security risks for the protection of classified information, the Supreme Council of National Defense shall be immediately briefed and the controlled organization shall take immediate measures to remedy the deficiencies, initiate administrative investigation and, if necessary, apply the sanctioning measures and inform the prosecution authorities, if there are indications on the existence of criminal offences.

Art. 194 – According to their targets, the control activities can be:

a) ***total controls***, aiming at verifying the entire organizational, structural and functional system for the protection of classified information;

b) ***field controls***, aiming at verifying certain fields of the protection of classified information;

c) ***emergency controls***, aiming at verifying some punctual aspects, established following the detection of a security risk.

Art. 195 – In accordance with the way they are planned and organized, controls can be:

a) planned;
b) on the spot;
c) in emergency situations.

Art. 196 – The heads of the organizations to be controlled shall make available to the control teams all the requested information on the way the measures for the protection of classified information stipulated by the law are enforced.

Art. 197 - Yearly or whenever necessary, the heads of the organizations holding classified information shall organize internal controls on the way the information is managed.

CHAPTER VII
INDUSTRIAL SECURITY

SECTION 1
General Provisions

Art. 198 - The provisions of this chapter shall apply to all public or private legal persons who carry on or request the carrying on of contractual activities involving access to classified information.

SECTION 2
The responsibilities of the National Registry Office for Classified Information – ORNISS - and of the Designated Security Authorities in the field of the protection of classified information subjected to contractual activities

Art. 199 – In the field of the protection of classified information subjected to contractual activities, ORNISS has the following responsibilities:

a) to establish the strategy of unitary implementation, at national level, of the measures for the protection of classified information subjected to contractual activities;

b) to issue the industrial authorization and the facility security clearance, upon the request of the legal persons concerned;

c) to organize, at national level, the accountability of: the legal persons holding industrial security authorizations; legal persons holding facility security clearances; natural persons holding personnel security clearances or access authorizations issued for the negotiation or running of a state secret contract;

Art. 200 - The designated security authorities have the following responsibilities, according to their legal competence:

a) to conduct the vetting procedures for issuing the industrial security notice which is sent to ORNISS in order to issue the authorization or the facility security clearance;

b) to provide specialized assistance to industrial facilities for the implementation of the security standards on the protection of classified information handled within the industrial activities;

c) to carry out training programs for the personnel with responsibilities for the protection of classified information handled within the industrial activities;

d) to investigate all cases indicating breaches of security regulations, destructions, losses, or unauthorized disclosure of classified information released or generated within a classified contract;

e) to ensure that any industrial facility where classified information is to be managed appointed a security structure/officer responsible for exercising attributions on the protection of classified information within classified contracts;

f) to monitor, in accordance with the law, the way classified information is protected during the negotiation and carrying on of contracts, and should any risks or vulnerabilities be indicated, will report immediately to ORNISS and recommend the necessary measures;

g) to authorize the programs for preventing classified information leakage from the industrial facilities, the security annexes of the classified contracts and monitors their observance;

h) to conduct security inspections and to report their results to ORNISS;

i) to verify and submit to ORNISS recommendations for settling the disputes, complaints and observations related to the implementation and observance of the security norms within classified contracts.

SECTION 3
Protection of the classified information subject of the contractual activities

Art. 201 - (1) The clauses and the protection procedures shall be set out in the Security Aspects Letter of each classified contract, which involves access to classified information.

(2) The Security Aspects Letter stipulated under paragraph (1) shall be drawn up by the Contracting Party holding classified information which will be used in carrying on the classified contract.

(3) Periodically, the clauses and the protection procedures shall be inspected and controlled by the competent designated security authority.

Art. 202 – The contracting party holding classified information which shall be used in carrying on a contract is responsible for classifying and defining all components of the contract, according to the norms in force, to which purpose, the contracting party may require the support of the designated security authorities, according to the material competences set forth by law.

Art. 203 – The following general rules shall be applied when classifying contracts:

a) at all stages of planning and execution, the contract shall be classified on appropriate levels, depending on the content of the information;

b) classifications shall be applied only to those parts of the contract which need to be protected;

c) when, in carrying on of a contract, information from different sources is used, with different levels of classification, the contract shall be classified according to the highest level of classification and the protective measures shall be established appropriately;

d) the declassifying or changing the class or secrecy level of the information within the contract shall be endorsed by the head of the legal person who authorized the initial classification.

Art. 204 - Should it be necessary to protect information contained in a contract that has previously not been identified for classification, the contractor shall be responsible for initiating the classification and protection procedures, in compliance with the regulation in force.

Art. 205 – If a contracting party entrusts part of a contract to a sub-contractor, he shall make sure that the sub-contracting party holds an industrial authorization/facility security clearance, shall inform the

contractor and, at the conclusion of the sub-contract the sub-contracting party shall include protection clauses and procedures, according to the provisions of these standards.

Art. 206 - **(1)** In the process of negotiating a classified contract, only those authorized representatives of the industrial entities holding industrial security authorization issued by ORNISS, which keep their records, are allowed to participate.

(2) The industrial security authorizations shall be issued for each classified contract.

(3) If the industrial entity does not hold industrial security authorization for the negotiation of that contract, the authorization procedure shall be initiated.

Art. 207 - (1) Invitations to bids or offers in respect of classified contracts shall contain a clause requiring a prospective contractor to return the classified documents which were provided to him, in case he does not submit a bid until the deadline for the opening of bids or does not win the bid within the period stipulated by the organizer, which will not exceed 15 days after notification.

(2) In the situations under paragraph (1), the contractor who lost the bid shall keep the confidentiality of the information to which he had access.

Art. 208 - The contractor shall keep the record of all participants in the negotiation meetings, their identification data, the confidentiality statements, the organizations they represent, the kind and purpose of the meetings and the information to which they had access.

Art. 209 – The contracting parties who intend to carry out industrial activities with sub-contracting parties shall comply with the procedures stipulated under this chapter.

Art. 210 – The contracting and sub-contracting parties shall implement and observe all measures for the protection of classified information which were provided or generated during the carrying on of the contracts.

Art. 211 – The designated security authorities, according to their competence, shall ensure that the industrial entity meets the following requirements:

a) to have a security structure/officer responsible for the protection of classified information which is subject of the contractual activities;

b) to provide the necessary support for the periodic security inspections, through the entire duration of the classified contract;

c) to forbid dissemination, without the written authorization of the document originator, of any classified information entrusted to him during the carrying on of a classified contract;

d) to allow access to classified information within the classified contract only to individuals holding security clearance or access authorization, in accordance with the need-to-know principle;

e) to have the necessary means to inform on any act of compromise, disclosure, destruction, theft, sabotage, subversive activities or any other risks regarding the security of the handled classified information or of the employees involved in carrying on of the respective contract, on any changes that may occur in the ownership, control or management of the industrial facility affecting the security status of the facility;

f) to impose to all sub-contracting parties security obligations similar to those applied to the contracting party;

g) not to use any classified information to which it has access, without the prior written consent of the originator, for any other purposes than those specific to the contract;

h) to return all classified information it was entrusted with, as well as that generated during the carrying on of the contract, unless such information has been approved for destruction, or its retention was duly authorized by the contractor, for a strictly determined period of time;

i) to comply with the established procedure on the protection of classified information related to the contract.

Art. 212 - After the classified contract has been let, the contacting party shall inform ORNISS for initiating the procedure of issuing the facility security clearance.

Art. 213 - The classified contract shall be carried on only if:

a) ORNISS has issued the Facility Security Clearance ;

b) Personnel Security Clearances or access authorizations have been issued for the individuals who, in fulfilling their duties, need access to state secret information;

c) the cleared personnel of the contracting party was briefed on the industrial security procedures by the security structure/officer and signed the individual training form.

SECTION 4
Vetting procedure, security notice and certification of the industrial facilities involved in the negotiation and carrying on of classified contracts

Art. 214 - Vetting, security notice and issue of industrial security authorization and facility security clearance represent all the security procedures applying exclusively to industrial facilities which have or shall have access to classified information within state secret contracts or sub-contracts concluded with holders of such information.

Art. 215 - (1) In order to participate in negotiations for concluding a classified contract, the head of the industrial facility shall send to ORNISS a request to issue the security industrial authorization - annex no. 24, to which he shall attach the industrial security form - annex no. 25.

(2) After the competent security authority has released the security notice, ORNISS shall issue the industrial security authorization - annex no. 28.

(3) The record of the industrial security authorizations issued according to paragraph (2) shall be kept in accordance with annex no. 31.

Art. 216 - (1) In order to carry on classified contracts, ORNISS issues facility security clearances to industrial facilities - annex no.29.

(2) The security notice procedure for the issuing of the facility security clearance is conducted upon the request for the issuance of the facility security clearance - annex no. 30, the security form – annexes no. 26 and 27 and the copy of the security aspects letter mentioned under article 201.

(3) ORNISS shall keep the records of the facility security clearances according to annex no.32.

Art. 217 – The vetting for issuing the industrial security authorizations and the facility security clearances has to ensure the accomplishment of the following main objectives:

a) to prevent the access of unauthorized person to classified information;

b) to ensure that the classified information is released on the basis of the facility security clearance and the “need-to-know” principle;

c) to identify those persons who, through their actions, may endanger the security of classified information and to ban their access to such information;

d) to ensure that the industrial facilities have the capacity to protect classified information during the negotiation process or during the carrying on of the contract.

Art. 218 - (1) In order to be granted the industrial security authorization/clearance, the industrial facility shall meet the following requirements:

a) to possess programs for preventing classified information leakage, approved according to the regulations in force;

b) to have economic stability;

c) not to have made a serious management mistake that will seriously endanger the security conditions of the handled classified information;

d) to observe the security obligations within all classified contracts previously carried on;

e) the personnel involved in carrying on of a contract shall hold personnel security clearance of the same level as that of the information handled within the classified contract.

(2) Failure to meet the requirements stipulated under paragraph (1) as well as the deliberate lying in completing the form or the documents submitted for certification shall be deemed as ineligibility criteria for being granted the industrial facility security clearance/ authorization.

Art. 219 - An industrial facility shall not be considered economically stable if it:

- is involved in an insolvency process;
- is declared bankrupt or it is involved in the judicial reorganizing procedure or bankruptcy;
- is involved in a litigation, which affects its economic stability;
- does not fulfill its financial liabilities to the state;
- does not succeed in fulfilling in due time, systematically, its financial liabilities to natural or legal persons.

Art. 220 - (1) An industrial facility shall not correspond from the viewpoint of the protection of classified information if security risks are detected.

(2) Such **security risks** are:

a) activities carried on against the national security interests or Romania's commitments undertaken under bilateral or multinational agreements;

b) relations with foreign natural or legal persons which may endanger Romania's interests;

c) associations, natural and legal persons which may be considered as risk factors for Romania's national interests.

Art. 221 - (1) For the issuing of the industrial security authorization/ facility security clearance, the applicant shall send to ORNISS the following documents:

a) the request to issue the authorization / facility security clearance;

b) the security form duly completed, in a sealed envelope.

(2) For the issuing of the facility security clearance, the applicant shall also attach a copy of the security aspects letter.

Art. 222 - Within 7 working days from the receipt of the application, ORNISS shall request the competent designated security authority to conduct the vetting procedure.

Art. 223 - The security notice released by the competent designated security authority shall guarantee that:

a) the economic unit has no security risks;

b) the physical security measures stipulated in the regulations in force and the norms regarding the access to classified information are appropriately applied;

c) the industrial facility is financially solvable;

d) the industrial facility is not, or has not been, involved in the activity of any organizations, associations, trends, groups of strangers or nationals who adopted or adopt a support or approval policy of committing sabotage, subversive or terrorist acts.

Art. 224 - Security vetting is conducted as follows:

a) **Level I security vetting** – to release the security notice necessary to issue the industrial security authorization;

b) **Level II security vetting** – to release the security notice necessary to issue the confidential facility security clearance;

c) **Level III security vetting** – to release the security notice necessary to issue the secret facility security clearance;

d) **Level VI security vetting** – to release the security notice necessary to issue the top secret facility security clearance;

Art. 225 – The following activities shall be conducted within the security vetting:

(1) For level I security vetting:

a) check if the data provided in the industrial security form are correct, according to annex no. 25;

b) check the correct implementation of the provisions of the provisions of the program for preventing the leakage of classified information;

c) assess the security status of any person having decisional authority - associates, shareholders, managers, people in board of directors and the security structure - or executive authority, involved in negotiating the classified contract;

d) check the minimal data regarding the solvability and economical stability of the industrial facility – field and object of its activity, judicial status, shareholders, banking warrantees;

(2) For level II security vetting:

a) check if the data provided in the industrial security form are correct, according to annex no. 26;

b) assess the security status of any person having decisional authority - associates, shareholders, managers, members in board of directors and the security structure - or executive authority, involved in carrying on the classified contracts;

c) check the minimal data regarding the solvability and economical stability of the industrial facility – field and object of its activity, judicial status, shareholders, banking warrantees;

d) check the implementation of the norms and measures for the physical security, personnel security and document security, for the confidential level.

(3) For level III security vetting:

a) check if the data provided in the industrial security form are correct, according to annex no. 27;

b) assess the security status of any person having decisional authority - associates, shareholders, managers, people in board of directors and the security structure - or executive authority, involved in carrying on the classified contracts, and designated to participate in the negotiation of classified contracts;

c) check the minimal data regarding the solvability and economical stability of the economic unit – field and object of its activity, judicial status, shareholders, banking warrantees - including aspects referring to branches, subsidiaries and companies to which it is associated, financial data;

d) check the existence of its own authorized communications and informatics system, at secret level;

e) check the implementation of the norms and measures for the physical security, personnel security and document security, for the secret level.

f) discussions with owners, members in board of directors, security officers, employees, in order to clarify data resulting from the questionnaire, where applicable.

(4) For level IV security vetting:

a) check if the data provided in the industrial security form are correct, according to annex no. 27;

b) assess the security status of any person having decisional authority - associates, shareholders, managers, people in board of directors and the security structure - or executive authority, involved in carrying on the classified contracts.

c) check the minimal data regarding the solvability and economical stability of the economic unit – field and object of its activity, judicial status, shareholders, banking warrantees - including aspects referring to branches, subsidiaries and companies to which it is associated, financial data;

d) check the existence of its own authorized communications and informatics system, at top secret level;

e) check the implementation of the norms and measures for the physical security, personnel security and document security, for the top secret level.

f) discussions with owners, members in board of directors, security officers, employees, in order to clarify data resulting from the questionnaire, where applicable.

Art. 226 - In case of an industrial facility in whose management/share holding participate foreign citizens, Romanian citizens with dual citizenship and/or steles persons, ORNISS together with the competent DSA, shall assess the extent in which the foreign interest represents a threat for the protection of state secret information that may be entrusted to that industrial facility.

Art. 227 - In order to fulfill their tasks and duties in the protection of classified information field, the competent DSAs cooperate on the basis of the protocols they shall sign, with ORNISS approval.

Art. 228 – In order to conduct security notice procedure, the industrial facility shall allow the access of the DSA's representatives to their premises, to their equipment, operations and any other activities, and shall submit the necessary documents and provide, upon request, other data and information.

Art. 229 - (1) If, after the vetting, the security criteria to ensure adequate protection for the classification level of the information managed within the classified contract are fulfilled, ORNISS shall issue and transmit to the industrial facility, the industrial security authorization or the facility security clearance.

(2) If the industrial facility fails to meet the necessary security criteria, ORNISS shall not issue the industrial security authorization or facility security clearance and shall inform the industrial facility in this respect. ORNISS is not compelled to state the reason for this denial. The denial for granting the industrial security authorization or facility security clearance shall be also transmitted to the designated security authority which conducted the security vetting.

(3) When factors which are not considered risks are detected, but they are relevant for security, the security interests shall prevail in deciding to issue the industrial security authorization or facility security clearance.

Art. 230 - Within 7 working days from the receipt of the security notice, ORNISS shall issue the industrial security authorization or the facility security clearance or, where applicable, shall communicate the denial to the industrial facility.

Art. 231 - The industrial facility shall report to ORNISS all the changes in the security data provided in the filled in questionnaire, during the entire validity period of the industrial security authorization or facility security clearance.

Art. 232 - The terms for issuing the industrial security authorization or facility security clearance are:

a) for industrial security authorization – 60 working days;
b) for facility security clearance of confidential level – 90 working days;
c) for facility security clearance of secret level – 120 working days;
d) for facility security clearance of top secret level – 180 working days;

Art. 233 - (1) The industrial security authorization is valid until the conclusion of the contract or until withdrawal from the negotiation.

(2) If during the period mentioned under paragraph (1) the negotiated classified contract is let, the contracting party shall request ORNISS the issuing of the facility security clearance.

(3) The validity of the facility security clearance is established by the duration of the contract, but it is no longer than 3 years, after which the contracting party shall request its revalidation.

Art. 234 – If ORNISS decides to withdraw the industrial authorization/facility security clearance, it shall inform the contracting party, the contractor and competent designated security authority.

Art. 235 – ORNISS shall withdraw the industrial authorization/facility security clearance in the following situations:

a) at the request of industrial facility;
b) on the competent DSA’s motivated demand;
c) at the end of validity;
d) at the completion of the contract;
e) when the previously granted access level is changed.

CHAPTER VIII

PROTECTION OF INFORMATION - GENERATING SOURCES INFOSEC

SECTION 1
General provisions

Art. 236 - The ways and measures for the protection of classified information in electronic format are similar to those on paper support.

Art. 237 - The specific terms used in this chapter, applicable to INFOSEC field are defined as follows:

- INFOSEC – all measures and structures for the protection of classified information processed, stored or transmitted through communications and informatics systems and other electronic systems, against threats and other actions that may endanger confidentiality, integrity, availability, authenticity and non- repudiation of classified information, as well as any actions that may affect the functioning of the information systems, no matter if they are accidental or intentional. The INFOSEC measures cover computer security, transmission and emission security, cryptographic security, as well as detection and prevention of threats to which information and systems are exposed;

- Information in electronic format - texts, data, images, sounds, recorded on storage devices or magnetic, optical or electric supports, or transmitted as waves, tension, or electromagnetic field, in the atmosphere or communications networks.

- ***system of automated data processing – ADPS*** - all interdependent elements including: computing equipment, basic software products and applications, methods, procedures, and, if applicable, the personnel, organized in such a way as to ensure the functions of storage, automated processing and transmission of information in electronic format, and which are under the coordination and control of a single authority. An ADPS can comprise subsystems some of which can be in their turn ADPS.

- the specific security components of an ADPS, necessary to ensure an appropriate level of protection for classified information which is to be stored or processed in an ADPS, are:

- hardware / firmware / software functions and characteristics;
- operation procedures and modes;
- accountability procedures;
- control of access;
- definition of an ADPS operation area;
- definition of working stations operation area/remote terminals;

- restrictions imposed by the management policy;
- physical structures and devices;
- means of control for personnel and communications.

- data transmission networks – DTN - all interdependent elements including: communications equipment, programs and devices, hardware and software technique, methods and procedures for transmission and reception of data and network control, and, if applicable, the relevant personnel. They are organized to ensure the functions of transmitting information in electronic format between two or more ADPS - or to allow interconnection with other DTNs. A DTN may use the services of one or more communications systems; more DTNs may use the services of a single communication system.

The security features of a DTN comprise: security features of individual ADPS connected, together with all components and facilities associated to the networks - communication network facilities, mechanisms and procedures of identification and labeling, access control, programs and procedures of control and revision - necessary to ensure an appropriate level of protection for classified information transmitted through DTN.

- local DTN – data transmission network interconnecting more computers or network equipment, situated in the same perimeter.

- communications and informatics system – CIS – informatics system through which information in electronic format is stored, processed and transmitted, composed of at least an ADPS, isolated or connected to a DTN. It may have a complex configuration, made of more interconnected ADPS and/or DTNs.

- ADPS, DTN and CIS security - implementation of security measures at ADPS, DTN and CIS in order to prevent or hamper extraction or change of classified information stored, processed or transmitted through them - by intercepting, alteration, destruction, unauthorized access with electronic means, as well as invalidation of services and functions, by specific means.

- confidentiality – to ensure access to classified information only based on the security clearance, in compliance with the secrecy level of the information accessed and the permission resulted from the enforcement of the need-to-know principle.

- integrity – interdiction to change - by deleting or adding - or to destroy classified information without authorization;

- availability – to ensure the conditions necessary to find and easily use classified information, whenever necessary, with the strict observance of its confidentiality conditions and integrity;

- authenticity – to ensure the possibility to check the presumed identity of an ADPS or DTN user.

- non-repudiation – measure to ensure that after the emission/reception of information in a secured communications system, the

originator/beneficiary cannot misleadingly deny, that he sent/received the information.

- security risk – probability that a threat or vulnerability of ADPS or DTN – CIS actually exist.

- risk management - has as a purpose to identify, control and minimize the security risks and it is a continuous activity meant to establish and maintain a security level in the field of communication and information technology - (CIT) in an organization. Starting from risk analysis, the threats and vulnerabilities are identified and assessed, and appropriate measures are taken to counter the risks, designed at a cost price corresponding to the consequences deriving from disclosure, change or delete of information that should be protected.

- the "two-men" rule – obligation that two persons cooperate to fulfill a specific duty.

- security informatics product - security component incorporated in a ADPS or DTN - CIS, used to increase or ensure confidentiality, integrity, availability, authenticity and non-repudiation of the stored, processed or transmitted information.

- computer security – COMPUSEC - implementation at the level of each computer of the hardware, software and firmware facilities, in order to prevent unauthorized disclosure, handling or unauthorized delete of classified information or unauthorized invalidation of certain functions.

- communication security – COMSEC – implementation of security measures in telecommunications with a purpose to protect messages in a telecommunication system that might be intercepted, studied, analyzed, and by reconstruction, may lead to disclosure of classified information.

COMSEC represents all the procedures including:

a) transmission security measures;
b) TEMPEST security measures;
c) cryptographic coverage measures;
d) physical, procedural, personnel and document security measures;
e) COMPUSEC measures.

- TEMPEST - all measures of testing and ensuring the security against information leakage through parasite electromagnetic emissions.

- assessment consists in a detailed technical and functional examination of the security aspects of an ADPS, DTN - (CIS) or of the security products, by an appropriate authority.

The assessment process verifies:

(a) the existence of the required security facilities/ functions;

(b) the absence of compromising secondary effects resulting from the implementation of the security facilities;

(c) the overall functionality of the security system;

(d) the fulfillment of the specific security requirements for an ADPS and DTN-CIS;

(e) the determination of the trust level of ADPS or DTN-CIS or of the implemented computer security products;

(f) the existence of the security performances of the computer security products installed in ADPS or DTN-CIS.

- certification – the issuance of a finding document, to which an analysis document is attached, reporting the assessment and its results. This finding document mentions the extent to which ADPS and DTN-CIS meet the security requirements as well as the extent to which the computer security products meet the requirements referring to the protection of classified information in electronic format;

- accreditation is a stage when an ADPS or DTN-CIS is authorized or approved to process classified information within its operational environment/space.

The accreditation stage shall take place after all appropriate security procedures have been implemented and after a sufficient level of system resources protection has been achieved. Accreditation is mainly made on the basis of the Specific Security Requirements (SSR), including the following:

(a) a justifying statement upon the objective of system accreditation; classification level(s) of information to be processed and handled; recommended protected operational mode(s);

(b) a justifying statement upon the risk management - mode of risk treatment / accounting / solving - identifying the threats and vulnerabilities, as well as the adequate countermeasures;

(c) a detailed description of the security facilities and recommended procedures designed for ADPS or DTN - CIS. This description shall represent the essential element for completing the accreditation process;

(d) a plan for the implementation and maintenance of the security features;

(e) a plan for carrying on security test, assessment and certification stages, regarding ADPS or DTN - CIS;

(f) a certificate and, where required, supplementary elements of accreditation.

- ADPS area - represents a working area, containing one or more operating computers, their local peripheral and storage units, control units and specific network and communication equipment. ADPS area does not include the separate area in which remote peripheral devices, terminal or workstations are located, even though these devices are connected to the central computing equipment of the ADPS area;

- ***remote terminal/workstation area*** represents an area – separated from ADPS area – including:

(a) computing technique equipment;

(b) local peripheral devices, terminals or remote workstations connected to the equipment within the ADPS area;

(c) communication equipment.

- ***threat -*** an accidental or deliberate potential compromise of ADPS or DTN - CIS by loss of confidentiality, integrity or availability of information in electronic format or by affecting the functions ensuring the authenticity and non- repudiation of information.

- vulnerability - weakness or lack of control that would allow or facilitate a technical, procedural or operational manoeuvre, which would threat a specific asset or target.

Art. 238 – Abbreviations used in this chapter refer to:

a) CITSC - security component for communication and information technology established within the organizations holding classified information;

b) CIT – communication and information technology;

c) SSR – specific security requirements.

Art. 239 - **(1)** Information in electronic format may be:

a) stored and processed within ADPS or transmitted through DTN;

b) stored and transported through memory supports, electronic devices – memory chips, punched paper or other specific devices;

(2) Uploading information on the media provided under paragraph (1) letter b, as well its interpretation in order to become legible shall be done through specialized electronic equipment.

Art. 240 - **(1) A**DPS, DTN and CIS may store, process or transmit classified information only if they are authorized according to this decision.

(2) In order to authorize ADPS and DTN – CIS, the organizations shall establish, with the approval of their senior management, their own security strategy on whose basis they shall implement their own security systems which shall include the use of trained personnel and information protective measures, including the access control to informatics and communications services and systems, with the observance of the need to know principles and the granted secrecy level.

(3) ADPS and DTN - CIS shall be accredited and periodically evaluated in order to maintain the accreditation.

Art. 241 - (1) The unitary implementation of the regulations in force on the protection of classified information in electronic format is applied at a national level. The issuing and implementing system of the security measures for the protection of classified information which is stored, processed or transmitted through ADPS or DTN – CIS, as well as the control of their implementation shall be done by a functional structure having regulation, control and authorization tasks. This structure includes:

(a) an agency for granting functioning accreditation in a secure environment;

(b) an agency working out and implementing security methods, means and measures;

(c) an agency responsible for the cryptographic protection.

(2) The agencies under paragraph (1) are subordinated to the nationally designated organization for the protection of classified information, ORNISS.

(3) The measures for the protection of classified information in electronic format shall be permanently up-dated by detecting, documenting and management of threats and vulnerabilities to classified information and to the system processing, storing and transmitting it.

Art. 242 – The INFOSEC security measures shall be structured according to the classification level of the information they protect and its content.

Art. 243 – The head of the organization holding classified information is responsible for the security of their own classified information which is stored, processed or transmitted in ADPS or DTN - CIS.

Art. 244 - (1) A security component for the communication and information technology - CITSC, subordinated to the security structure/officer shall be established within each entity managing ADPS or DTN- CIS where classified information is stored, processed or transmitted.

(2) Depending on the amount of work and if the security requirements allow it, CITSC tasks may be carried on only by the CIT security officer or may be taken over by the security structure/officer within the respective entity.

(3) CITSC fulfils tasks on:

a) the implementation of methods, means and measures required for the protection of classified information in electronic format;

b) the operational exploitation of ADPS or DTN – CIS under security conditions;

c) the coordination of the cooperation between the entity holding ADPS or DTN – CIS and the authority ensuring the accreditation;

d) the implementation of security measures and the cryptographic protection of ADPS or DTN – CIS.

(4) CITSC represents the contact point of the competent agencies with the entities holding in order to manage ADPS or DTN – CIS and as the case may be, may be temporarily invested by these agencies with some of their tasks.

(5) CITSC proposals on security line become operational only after being approved by the head of the organization managing the respective ADPS or DTN – CIS.

Art.245 – CITSC is established at the level of each ADPS or DTN – CIS and represents the individual or compartment appointed by the security agency for informatics and communication to implement the security methods, means and measures and to exploit ADPS or DTN – CIS in security circumstances.

Art. 246 - CITSC is led by the TSC security officer and is composed of security administrators and, if applicable, other specialists of ADPS or DTN - CIS. The whole CITSC structure belongs to the personnel of the organization administrating ADPS or DTN – CIS.

Art. 247 – The exercising of CITSC attributions shall comprise the whole life cycle of ADPS or DTN – CIS, starting with the designing and continuing with the working out of the specifications, testing of the installation, accreditation, periodic testing for reaccreditations, operational exploitation, modification and ending with final disposal. Under some special circumstances, the CITSC role may be taken over by different components of the organization, during the life cycle.

Art. 248 - The CITSC mediates the cooperation between the senior management of the entity to which ADPS or DTN – CIS belongs and the security accreditation agency, when the entity:

a. plans to develop or acquire an ADPS or DTN – CIS;
b. recommends changes to an existing system configuration;
c. recommends to interconnect an ADPS or DTN – CIS with another ADPS or DTN – CIS;
d. recommends changes to the security mode of operation of an ADPS or DTN – CIS;
e. recommends changes to the existing programs, or to use new software packages, for optimization of ADPS or DTN – CIS security;
f. initiates procedures to modify the security classification level for an ADPS or DTN – CIS, which has been already accredited;
g. plans or recommends the undertaking of any other activity referring to the improvement of the already accredited security of ADPS or DTN – CIS.

Art. 249 – CITSC, with the approval of the Security Accreditation Authority decides on the security standards and procedures to be observed by the equipment suppliers during the development, installation and testing of the ADPS or DTN – CIS and is also responsible for the justification, selection, implementation and control of those security components of ADPS or DTN – CIS.

Art. 250 - From its establishment, CITSC sets out, for the security and management structures ADPS or DTN – CIS the necessary responsibilities to be fulfilled throughout the entire life cycle of ADPS or DTN – CIS.

Art. 251 – The INFOSEC activity within ADPS or DTN – CIS shall be managed and coordinated by individuals holding appropriate personnel security clearance with experience in the field of TSC systems and their security, gained in the INFOSEC accredited education institutions or by individuals who have worked for at least five years in the field.

Art 252 - Protection ADPS or DTN – CIS of weapon or sensor systems shall be determined in the general context of the systems to which they belong, and shall be implemented by using the provisions of these standards.

SECTION 2
Organizational structures with specific responsibilities in the INFOSEC field

A. The Security Accreditation Agency

Art. 253 - The Security Accreditation Agency is subordinated to the authority designated at national level for the protection of classified information, including delegated representatives of the DSAs involved, depending on the ADPS or DTN – CIS to be accredited, and having the following tasks:

a) to ensure at national level the security accreditation/reaccreditation of ADPS or DTN – CIS that store, process or transmit classified information, depending on its secrecy level;

b) to ensure the assessment and approval of ADPS or DTN – CIS systems or of some of their components;

c) to establish the accreditation criteria for ADPS or DTN - CIS.

Art. 254 -The Security Accreditation Agency exercises its attributions in the INFOSEC field, on behalf of the organization designated at national level, for the protection of electronic classified information including delegated representatives of the DSAs involved, acting at national level.

B. The Communications and Informatics Security Agency

Art. 255 - The Communications and Informatics Security Agency CISA is the structure, acting at national level, subordinated to the

organization designated at national level, for the protection of electronic classified information including delegated representatives of the DSAs involved, acting at national level.

Art. 256 - CISA is responsible for the establishment and implementation of the means, methods and measures for the protection of classified information, which is stored, processed or transmitted through the ADPS or DTN - CIS, having the following main responsibilities:

a) to coordinate the activities for the protection of classified information stored, processed or transmitted through ADPS or DTN - CIS;
b) to work out and promote specific regulations and standards;
c) to assess the causes of the security breaches and manages the database concerning the threats and vulnerabilities of the information and communication systems, as a necessity for the risk management;
d) to notify the security breaches in the field to the Security Accreditation Agency ;
e) to integrate the measures on the physical, personnel, administrative documents, COMPUSEC, COMSEC, TEMPEST and cryptographic protection;
f) to conduct periodic inspections on ADPS or DTN - CIS regarding re-accreditation;
g) to submit ADPS or DTN - CIS security systems to certification and authorization.

Art. 257 - In fulfilling its duties, CISA cooperates with the SAA, CMDA, as well as with other structures with responsibilities in the field.

C. The Cryptographic Material Distribution Agency

Art. 258 - The CMDA is established at national level, subordinated to the organization designated at national level, for the protection of classified information and has the following main responsibilities:

a) to ensure the management of cryptographic material and equipment;

b) to ensure the distribution of cryptographic material and equipment;

c) to report the security breaches it has encountered to the organization designated at national level for the protection of classified information;

d) to cooperate with the Security Accreditation Agency, the agency for establishing and implementing the security methods, means and measures, as well as with other structures with responsibilities in the field.

SECTION 3
Measures, requirements and operation modes

A. Measures and requirements specific for INFOSEC

Art. 259 - (1) The measures for the protection of classified information in electronic format shall apply to ADPS or DTN - CIS storing, processing or transmitting such information.

(2) The organizations holding classified information shall establish and implement a set of security measures of ADPS or DTN - CIS - physical, personnel, administrative, TEMPEST and cryptographic.

Art. 260 - The security measures for the protection of ADPS or DTN - CIS shall ensure the access control, in order to prevent or detect unauthorized disclosure of information. The process of certification and accreditation shall determine the adequacy of these measures.

B. Security requirements specific for ADPS or DTN – CIS

Art. 261 – (1) The specific security requirements - SSR form a binding agreement between the SAA and the CITSC and shall include security principles and measures which shall lie at the basis of the process of certification and accreditation of ADPS or DTN - CIS.

(2) SSRs shall be worked out for each ADPS and DTN - CIS storing, processing or transmitting classified information, shall be established by CITSC and approved by the Security Accreditation Agency.

Art. 262 - The SSRs shall be stated even from the designing stage of ADPS or DTN - CIS and shall be developed during the whole system's life cycle.

Art. 263 - The SSRs are based on the national protective standards, parameters covering the operational environment security, the minimum level of personnel clearance, the classification level of information managed and the operation mode of the system to be accredited.

C. Operation modes

Art. 264 - ADPS and DTN - CIS storing, processing or transmitting classified information shall be certified and accredited to operate during certain periods of time and in one of the following operation modes:

a) dedicated;
b) system-high;
c) multi-level.

Art. 265 - (1) In **the operation mode dedicated,** all individuals having access to ADPS or DTN shall possess a personnel security clearance for the highest classification level of the information stored, processed or transmitted within these systems. The "need-to-know" principle for these persons shall be established for all the information stored, processed or transmitted within the ADPS or DTN – CIS.

(2) In this operation mode, the "need-to-know" principle does not imply a mandatory requirement for information separation within the ADPS or DTN as CIS security means. The other security measures provided shall ensure the meeting of the requirements imposed by the highest classification level of the information handled and by all categories of information of the special destination stored, processed or transmitted within ADPS or DTN.

Art. 266 - (1) In **the operation mode system-high,** all individuals having access to ADPS or DTN-CIS shall possess a personnel security clearance for the highest classification level of the information stored, processed or transmitted within these systems, and the access to information is differentiated, according to "need-to-know" principle.

(2) In order to ensure the differentiated access to information, according to "need-to-know" principle, security facilities providing a selective access to the information within ADPS or DTN-CIS shall be established.

(3) The other security measures shall meet the requirements for the protection of information of the highest classification level and for all categories of the special destination information stored, processed or transmitted within ADPS or DTN-CIS.

(4) All information stored, processed or transmitted within ADPS or DTN-CIS under this operation mode shall be protected as information with a special destination, having the highest classification level of all information stored, processed or transmitted within the system.

Art. 267- (1) In **the operation mode multi-level**, the access to classified information shall be differentiated, according to the “need-to-know” principle, in compliance with the following rules:

a. not all persons entitled to have access to ADPS or DTN - CIS hold personnel security clearances for access to information of the highest level of classification, that is stored, processed or transmitted through these systems;

b. not all individuals having access to ADPS or DTN-CIS have also access to all information stored, processed, transmitted within these systems.

(2) The implementation of the rules stipulated under paragraph (1) implies in compensation the establishment of some security facilities meant

to ensure a selective, individual access mode to information within ADPS or DTN-CIS.

D. Security administrators

Art. 268 - (1) ADPS security of the network and of CIS site shall be ensured by the security network administrators.

(2) The security administrators are:

a) ADPS security administrator

b) Network security administrator

c) CIS site security administrator.

(3) The functions of security administrators shall ensure the fulfillment of the CITSC tasks. If applicable, these functions may be cumulated by a single specialist.

Art. 269 - (1) The ADPS security administrator is appointed by the CITSC and is responsible for the supervision of the development, implementation and management of the security measures within the ADP system, including the participation in the working out of the Security Operating Procedures.

(2) Following the recommendation of the Security Accreditation Authority, CITSC may appoint ADPS administration structures having the same responsibilities.

Art. 270 - The security network administrator is appointed by CSTIC for a large CIS as well as in the case of interconnecting more ADPSs, and it performs tasks related to the management of communications security.

Art. 271 - (1) The CIS site Security Administrator is appointed by CITSC or by the competent security authority and is responsible for ensuring the implementation and maintenance of the security measures applicable to the respective CIS site.

(2) The responsibilities of a CIS site Security Administrator may be carried out by the security officer/structure of the organization, as part of his professional duties.

(3) A *CIS site* represents a particular location, or a group of locations where an ADP system and/or a DTN is operating. The responsibilities and the security measures for each location of a remote terminal/workstation shall be clearly identified.

E. Users and visitors

Art. 272 - (1) All users of ADPS or DTN-CIS are responsible for the security of these systems – mainly depending on the granted rights – and are guided by the security administrators.

(2) The users shall be authorized for the class and secrecy level of the classified information stored, processed or transmitted within ADPS or DTN-CIS. When granting individual access to information, the observance of the "need to know" principle shall be taken into consideration.

(3) Information and awareness of users on their security duties shall enhance the security system.

Art. 273 - Visitors shall have security authorization at appropriate level and meet the need-to-know principle. When access of a visitor without authorization is deemed necessary, supplementary security measures shall be taken so that the visitor may not have access to classified information.

SECTION 4
INFOSEC Components

A. Personnel Security

Art. 274- (1) Users of ADPS or DTN-CIS are authorized and allowed to access the classified information according to "need to know" principle and depending on the classification level of the information stored, processed or transmitted through these systems.

(2) Organizations holding classified information in electronic format shall establish special measures for briefing and supervision the personnel, including the system designing personnel having access to ADPS or DTN, in view of preventing and removing vulnerabilities to unauthorized access.

Art. 275 - ADPS or DTN-CIS shall be designed so that when assigning tasks and responsibilities to the personnel, no individual can have access or knowledge to all programs and security keys - passwords, personal identification devices.

Art. 276 - The operating procedures for the personnel within ADPS or DTN-CIS shall ensure a clear segregation between programming and system/network operation. Except for special circumstances, members of the personnel are prohibited from both programming and operating the systems or networks, and special procedures must be established in order to detect such circumstances.

Art. 277 - For any change to an ADPS or DTN-CIS, the cooperation of at least two persons is mandatory - the two-men rule. The security procedures must clearly state those situations where the two-men rule is to be implemented.

Art. 278 - In order to ensure that the security measures are properly implemented, the ADPS or DTN-CIS personnel and the personnel responsible for their ADP security shall be briefed so as to know each other's attributions.

B. Physical security

Art. 279 - The ADPS and/or DTN-CIS locations and remote terminal areas where classified information is presented, stored, processed or transmitted or where access to such information is possible are stated security Class I or Class II security areas of the facility and observe the physical protective requirements established by these standards.

Art. 280 - The following general security measures are applicable to ADP and remote terminal-workstation areas, where classified information are processed or accessed:

a) Access of both personnel and materials, as well as departure from these areas are controlled by well defined means;
b) Areas and locations where ADPS or DTN-CIS remote terminal/workstation security may be modified shall never be occupied by a single authorized employee;
c) Individuals requiring temporary or intermittent access to these areas shall be authorized, as visitors, by the person responsible for security issues in the area, appointed by the security administrator of the CIS site. Visitors shall be permanently accompanied to ensure that they are denied access to classified information and to equipment in use.

Art. 281 - Depending upon the security risk, and on the secrecy level of the information stored, processed and transmitted, the two-men rule may be enforced in other areas too. Such areas are established from the project inception stage and are specified within the Specific Security Requirement.

Art. 282 - When an ADPS is operated in a stand-alone mode, permanently disconnected from another ADPS, taking into account environmental conditions, other procedural or technical security measures, and the part played by that ADPS within the overall operation, the Security Accreditation Authority (SAA) shall establish specific protective measures, adjusted to the structure of this ADPS, according to the classification level of information managed.

C. Access control to ADPS and/or DTN-CIS

Art. 283 - All information and material controlling access to an ADPS or DTN-CIS shall be controlled and protected under appropriate regulations for the highest level of classification and the category of the information to which the respective ADPS or DTN-CIS grants access.

Art. 284 - When no longer in use, the information and control material mentioned under the previous article shall be destroyed according to the provisions of these standards.

D. The security of classified information in electronic format

Art. 285 - Classified information in electronic format shall be controlled according to the INFOSEC rules, prior to their release from ADPS or DTN-CIS or from remote terminal areas.

Art. 286 – The way in which the information is presented, even if using the brevity code, transmission code or any binary representation or other form of remote transmission, shall not influence the classification level assigned to the information referred to.

Art. 287 - When information is transferred among various ADPS or DTN-CIS, it shall be protected both during transfer and at the level of the beneficiary's informatics systems, according to the classification level of the information.

Art. 288 - All computer storage media are preserved according to the highest classification level of the stored information or supporting devices, being at all times appropriately protected.

Art. 289 - Information on specific CIT storage media shall be copied according to the SecOps procedures.

Art. 290 - Re-usable information storage media, used for recording classified information, shall maintain the highest classification level for which they have previously been used, until the respective information is declassified or downgraded. In this case, the above mentioned media shall be reclassified accordingly, or shall be destroyed in compliance with the SecOPs provisions.

E. Control and accounting of information in electronic format

Art. 291 - (1) Automatic accounting of access to information classified in electronic format shall be kept in access registries and shall be doneunconditionally through software.

(2) Access registries shall be kept for a certain period of time, mutually agreed between SAA and CITSC.

(3) With respect to the records regarding access to “strict secret de importanta deosebita” information, the minimum retention period is of 10 years; for information classified “strict secret” or “secret”, the minimum retention period is of at least 3 years.

Art. 292 - (1) The storage media containing classified information used within an ADPS area can be handled as a single classified material, provided that the material is identified, marked with its classification level and controlled within the ADPS area, until it is destroyed, reduced to a record copy or placed on a permanent file.

(2) Their records shall be kept within the ADPS area, until they are submitted to control or destroyed according to these standards.

Art. 293 - When a storage medium is generated within a CIS, and it is afterwards transmitted to a remote terminal/workstation, appropriate security measures shall be taken, approved by the Security Accreditation Authority (SAA). The procedures shall also contain specific instructions with respect to the accountability of information in electronic format.

F. Handling and control of media for the storage of classified information in electronic format

Art. 294 - (1) All state secret computer storage media shall be identified and controlled according to the secrecy level.

(2) For unclassified and “secret de serviciu” information local security regulations shall apply.

(3) The identification and control shall ensure the following requirements:

a) for “secret” level:

- a means of identification - serial number and marking of the classification level -separately for such a medium;
- well defined procedures for issuing, receiving and final disposal or maintenance of the storage media;
- manual or printed records indicating the secrecy content and level of information, recorded on the storage media;

b) for “strict secret” and “strict secret de importanta deosebita” levels, detailed information regarding the storage medium, including the content and classification level, shall be kept within an appropriate registry;

Art. 295 - Spot-checking and overall control of storage media in order to ensure consistency with the identification and control procedures in force shall meet the following requirements:

a) for “secret” level – the spot-checks of the physical presence and contents of the computer storage media shall be conducted periodically, in order to ensure that these storage media do not contain information with a higher classification level;
b) for “strict secret” - all storage media shall be inventoried periodically, conducting spot-checks for their physical presence and contents, in order to ensure that these media do not contain information with a higher classification level;
c) for “strict secret de importanta deosebita” level all storage media shall be checked periodically, at least annually, and are spot-checked for their physical presence and contents.

G. Declassification and destruction of media for the storage of classified information in electronic format

Art. 296 - Classified information recorded on re-usable storage media are erased only in accordance with the SecOPs.

Art. 297 - (1) When a storage medium is going to be disposed of, it shall be declassified eliminating any classification marking, being further used as an unclassified storage media. If the medium cannot be declassified, it shall be destroyed by an approved procedure.
(2) Storage media containing “strict secret de importanta deosebita” information are forbidden to be declassified and reused, but can be destroyed only in conformity with the SecOps procedures.

Art. 298 - Classified information in electronic format stored on non-reusable media - punched cards or tapes - shall be destroyed according to the SecOps procedures.

SECTION 5
CIT general security rules

A. Communications security

Art. 299 - All the means used for the electromagnetic transmission of classified information follow the communications security instructions issued by the organization designated at national level for the protection of classified information.

Art. 300 - An ADPS - CIS shall be provided with the necessary means for denying access to classified information from all remote terminals/workstations, when required, by physical disconnection or by special software procedures approved by SAA.

B. Security at installation and against electromagnetic emanations

Art. 301 - Initial installation of an ADPS or DTN-CIS and any major change within, shall be carried out by authorized personnel only, according to the provisions of these standards. The works shall be under constant supervision of technically qualified personnel with access to classified information of the highest level, which the respective ADPS or DTN-CIS shall store, process or transmit.

Art. 302 - All ADPS and DTN-CIS equipment shall be installed according to the specific regulations in force issued by the organization designated at national level for the protection of classified information, and in compliance with the appropriate technical directives and standards.

Art. 303 - ADPS and DTN-CIS systems storing, processing and transmitting state secret information shall be appropriately protected against security vulnerabilities caused by compromising emanations - TEMPEST.

C. Security during the processing of classified information

Art. 304 - Processing of information shall be carried out according to the Security Operating Procedures (SecOPs), stipulated in these standards.

Art. 305 - Release of state secret information to unmanned installations is forbidden, unless specific regulations approved by the Security Accreditation Authority (SAA) and specified by the SecOPs.

Art. 306 - Information classified “strict secret de importanta deosebita” cannot be stored, processed and transmitted within ADPS and DTN-CIS having potential or existing users who do not hold security clearances issued according to these standards.

D. Security operational procedures - SecOps

Art. 307 - SecOPs are a description of the implementation of the security strategy to be adopted, of the operating procedures to be followed and of the responsibilities of the personnel.

Art. 308 - SecOPs are established by the agency for working out and implementation of the security methods, means and measures, in cooperation with CITSC and SAA having coordination tasks, and with other authorities with responsibilities in the field. SAA shall approve the SecOPs before authorizing the storing, processing or transmitting of classified information through ADPS - DTN-CIS.

E. Protection of software products and configuration management

Art. 309 - CITSC shall conduct periodic controls ensuring that master copies of all software products - general-purpose operating systems, subsystems and software packages - in use, are being protected according to the classification level of the information they have to process. Programs security - application software shall be established on the basis of an assessment of their secrecy level, taking into consideration the classification level of the information to be processed.

Art. 310 – (1) Use of unauthorized software by SAA is forbidden.

(2) Back-up copies, off-site or periodic saves of data resulted from processing shall be preserved according to the provisions of the SecOps.

Art. 311 - (1) Software versions in use shall be checked at regular intervals in order to ensure their integrity and correct functioning.

(2) New or modified software versions shall not be used for processing state secret information until their security procedures are tested and approved according to the SSR.

(3) A software improving the system capabilities and containing no security procedure cannot be used until it is verified by CITSC.

F. Checks for detecting software viruses and malicious software

Art. 312 -Checking for software viruses and malicious software shall be carried out according to the requirements of SAA.

Art. 313 - (1) New or modified software versions - operating systems, subsystems, software packages and applications software - stored on various media, to be introduced in an organization, shall be mandatory checked on stand-alone computer systems, in order to identify malicious software or computer viruses, before being used within ADPS - DTN-CIS. The installed software shall be periodically checked.

(2) These checks shall be conducted more frequently, if ADPS - DTN-CIS are connected to other ADPS - DTN-CIS or to a public communications network.

G. Technical maintenance of ADPS - DTN-CIS

Art. 314 - (1) The maintenance contracts for ADPS - DTN-CIS that store, process or transmit state secret information shall specify the requirements to be met so that the maintenance personnel and their specific equipment be introduced in the operating area of the respective systems.

(2) The maintenance personnel shall possess security clearances at a level corresponding to the secrecy level of the information to which they have access.

Art. 315 - The removal of the equipment from an ADPS DTN – CIS area shall be done according to the SecOps.

Art. 316 - The requirements stipulated under article 314, shall be clearly stated in SSR, and the procedures of carrying out the respective activity shall be established in the SecOPs. Maintenance operations, requiring remote access diagnostic procedures shall be permitted if and only if the respective activities are carried out under stringent security control, and only with the approval of the SAA.

H. Procurement

Art. 317 - ADPS or DTN-CIS systems and their hardware and software components shall be procured from internal or external suppliers selected from those agreed by SAA.

Art. 318 - Components of security systems implemented in ADPS or DTN-CIS ADPS shall be accredited based on a detailed technical documentation as to their design, manufacturing and distribution.

Art. 319 - ADPS or DTN-CIS systems that store, process or transmit state secret information, or the basic components of these systems - general-purpose operating system, security-enforcing limited functionality products and products for network communication - shall be procured only after they have been assessed and certified by SAA.

Art. 320 - For ADPS or DTN-CIS systems that store, process or transmit "secret de serviciu" information, the systems and their baseline components shall comply, as much as possible, to the criteria stated by these standards.

Art. 321 – When leasing or purchasing some hardware or software components, particularly some specific storage media, it should be taken into account that such equipment, after having been used in ADPS or DTN-CIS systems storing and processing classified information, shall be protected according to these standards. Once classified, the respective components shall be taken out of the ADPS or DTN-CIS areas only their declassification.

I. ADPS or DTN-CIS accreditation

Art. 322- (1) All ADPS and DTN-CIS systems, prior to being used for storing, processing or transmitting classified information, shall be accredited (by SAA based on information provided by SSRS, SecOPs and any other relevant documentation.

(2) ADPS and DTN-CIS systems and remote terminals/workstations shall be accredited as part of ADPS and DTN-CIS systems to which they are connected. When an ADPS or DTN-CIS system serves both NATO and national organizations/structures, the accreditation shall be done by the national security authority, after consultation with the designated security authorities and INFOSEC agencies.

J. Assessment and certification

Art. 323 - In the situations regarding multi-level security operation mode, prior to the proper accreditation of ADPS or DTN-CIS, hardware, firmware and software shall be assessed and certified by SAA. To this end, the organization designated at national level for the protection of classified information shall establish differentiated criteria for each secrecy level of information handled by ADPS or DTN-CIS.

Art. 324 - The requirements for assessment and certification are included in the ADPS and DTN-CIS system planning, and are clearly stipulated in the SSRS, as soon as the security mode of operation has been established.

Art. 325 - The following situations require the security assessment and certification, within the multi-level security mode of operation:

a) For ADPS or DTN-CIS systems storing, processing or transmitting "strict secret de importanta deosebita" classified information;
b) ADPS or DTN-CIS systems storing, processing or transmitting "secret" classified information where:
   (i) ADPS or DTN-CIS is interconnected with another ADPS or DTN-CIS - for example under another CITSC.
   (ii) ADPS or DTN-CIS has a number of potential users which cannot be specifically defined.

Art. 326 - The assessment and certification processes shall be carried out in accordance with the principles and instructions approved by expertise teams of technically qualified and appropriately cleared personnel. These teams shall be composed of experts selected by the Security Accreditation Agency.

Art. 327 - (1) The assessment and certification processes shall establish the extent to which an ADPS or DTN-CIS meets the security requirements, as stated in the SSRs, taking into consideration that, after completion of the assessment and certification, certain sections – paragraphs or chapters of SSRs may require modification or updating.

(2) The assessment and certification processes shall begin from the defining stage of ADPS or DTN-CIS and continue through the development stages.

Art. 328 - For any ADPS or DTN-CIS storing, processing or transmitting state secret information, CITSC establishes the control procedures, which could determine if the changes in the CIS may compromise their security.

Art. 329 - (1) The changes implying re-accreditation, or requiring prior approval of the SAA, shall be clearly identified and stated in the SSR.

(2) After any modification, repair or failure, which could have affected the security devices of ADPS or DTN-CIS, CITSC shall conduct an inspection to ensure the correct operation of the security devices.

(3) Maintaining accreditation of the ADPS or DTN-CIS shall depend on the meeting of the checking criteria.

Art. 330 - (1) All ADPS and DTN - CIS that store, process or transmit state secret information shall be inspected or reviewed on a periodic basis by the Security Accreditation Agency.

(2) For ADPS and DTN - CIS that store, process or transmit top secret information, the inspection shall be conducted at least once a year.

L. Security of microcomputers or personal computers

Art. 331 - (1) Microcomputers or personal computers (PCs) with fix hard disks or other non-volatile storage media, operating either in stand-alone mode or as networked configurations, as well as portable computing devices with fix hard disks, are considered as information storage media in the same sense as other removable computer storage media.

(2) If they store classified information, these standards shall apply.

Art. 332 - The equipment provided under article 331 shall be granted the level of protection for access, handling, storage and transportation, according to the highest classification level of information ever stored or processed within it, until downgraded or de-classified in accordance with the legal procedures.

M. The use of privately-owned computing equipment

Art. 333 - (1) It is forbidden to use privately-owned removable computer storage media, software hardware, software for the storage, processing and transmission of classified information.

(2) For unclassified or “secret de serviciu” information, the appropriate internal regulations of the organization shall apply.

Art. 334 - It is forbidden to bring privately-owned hardware, software and removable media into areas where classified information is stored, processed or transmitted, without the permission of the head of the organization.

N. The use of contractor-owned equipment or of such provided by other organizations

Art. 335 - The use, within a facility, of contractor-owned equipment and software for the storage, processing or transmission of classified information is permitted only with the approval of CITSC and of the head of the organization.

Art. 336 - The use, within a facility, of the equipment and software provided by other organizations may also be permitted. In this case the

equipment shall be recorded in the inventory list of the organization. In either case, approval from CITSC is necessary.

O. Marking of information with a special destination

Art. 337 - The marking of information with special destination, is currently applied to classified information requiring limited distribution and special handling, in addition to the granted security classification level.

CHAPTER IX
OFFENCES AND SANCTIONS TO THE NORMS ON THE PROTECTION OF CLASSIFIED INFORMATION

Art. 338 (1) The following acts are considered offences to the norms on the protection of classified information:

a) illegal possession, theft, disclosure or unauthorized destruction of state secret information;

b) non-observance of the measures stipulated under articles 18, 25-28, 29, 96-139 and 140-181;

c) non-observance of the obligations stipulated under articles 31, 41-43, 213, 214;

d) non-observance of the norms stipulated under articles 140-142, 145, 159, 160, 162, 163, 179-181, 183 paragraph (1) and 185-190;

e) non-observance or incorrect observance of the obligations stipulated under article 240, paragraph (2) and (3), article 243 and article 248, as well as non-observance of the rules stipulated under articles 274-336.

(2) The offences stipulated under paragraph (1) are sanctioned as follows:

a) offences stipulated under paragraph (1) letter a) are sanctioned for the illegal possession or damaging of classified information cases with a fine of 500.000 lei up to 50.000.000 lei and in cases of theft, disclosure, or unauthorized destruction cases with a fine of 10.000.000 lei up to 100.000.000 lei;

b) deeds mentioned under paragraph (1), letters b) and c) are sanctioned with a warning or a fine of 500.000 lei up to 25.000.000 lei;

c) deeds mentioned under paragraph (1), letters d) are sanctioned with a warning or a fine of 1.000.000 lei up to 50.000.000 lei;

d) deeds mentioned under paragraph (1), letters e) are sanctioned with a warning or a fine of 5.000.000 lei up to 50.000.000 lei;

(3) The persons or authorities who detect the offences may also apply, if the case may be, the complimentary sanction consisting in

confiscating, in accordance with the law, of the goods meant for, used or resulted from offences.

(4) The provisions of the general regulations regarding the juridical regime of offences are applied accordingly.

Art. 339 (1) The offences and sanctions stipulated under article 338 are detected and applied, by special designated persons from Romanian Intelligence Service, Ministry of National Defense, Ministry of Interior, Ministry of Justice, Foreign Intelligence Service, Guard and Protection Service, Special Telecommunications Service, according to their competence.

(2) The following categories may detect the offences and apply the sanctions stipulated under article 338, within the limits of their established competence:

a) special designated persons from ORNISS;

b) heads of the public authorities and organizations, economic units with partial or total state share capital and of other public legal persons;

c) authorities or persons stipulated under the general regulations regarding the juridical regime of offences.

(3) Complaints against finding reports and applying sanctions are settled according to the general regulations regarding the juridical regime of offences.

CHAPTER X
FINAL PROVISIONS

Art. 340 – The list of functions, including education and experience, as well as the wages of the personnel with responsibilities in the field of accounting, drawing up, storage, processing, multiplication, handling, transport, transmission and destruction of classified information are established according to the normative acts in force.

Art. 341 – The heads of the organizations handling classified information, shall take measures so that the provisions of these standards shall be made known to all employees and for:

a) establishing internal specialized structures with responsibilities for applying these standards;
b) designating the personnel with duties and responsibilities in handling classified information;
c) initiating the approach stipulated by the law and by these standards, in order to obtain the authorizations for access to classified information.

Art. 342 – At the request of the legal persons from the legal competence of the Romanian Intelligence Service, R.A. Rasirom shall assess the compliance and will summit to ORNISS proposals for the issuing of the quality accrediting certificates for the systems and equipment used for the physical protection of classified information.

Art. 343 - **(1)** These standards shall be interpreted and applied in accordance with the Norms on the protection of North Atlantic Treaty Organization classified information in Romania, adopted through the Government Decision no. 353 of 15.04.2002.

(2) Should there appear any incompatibilities between the two regulations mentioned under paragraph (1), the Norms on protection of North Atlantic Treaty Organization classified information in Romania endorsed through the Government Decision no. 353 of 15.04.2002 shall prevail.

Art. 344 - The provisions of these standards on offences and sanctions to the norms on the protection of classified information shall be applied after 60 days from their publication.

Art. 345 - The annexes no. 1-32 shall be constitutive parts of these national standards on the protection of classified information.