RULES ON IMPLEMENTATION OF THE PROTECTION OF CLASSIFIED INFORMATION ACT

Prom. SG. 115/10 Dec 2002, amend. SG. 22/11 Mar 2003, suppl. SG. 6/23 Jan 2004, amend. SG. 56/11 Jul 2006, amend. SG. 84/19 Oct 2007, amend. SG. 44/9 May 2008, amend. SG. 91/21 Oct 2008, amend. SG. 7/27 Jan 2009, amend. SG. 5/19 Jan 2010, amend. SG. 27/5 Apr 2016, suppl. SG. 64/16 Aug 2016, amend. and suppl. SG. 68/22 Aug 2017, amend. and suppl. SG. 79/8 Sep 2020

Chapter one.
GENERAL PROVISIONS

Art. 1.(1) With the Rules shall be provided:

1. the conditions and the order for conceding of classified information;
2. the order and the way for announcing of the list of the categories of information – official secret;
3. the marking of the classified information;
4. the order for conceding of data for entering in the register of art. 35 of the Protection of Classified Information Act (PCIA) and the conditions and the order for making inquiries in it;
5. the procedure for investigating for reliability and its termination as well as the keeping of the files for the investigations;
6. the establishing and the functioning of the registries for classified information;
7. the measures, the techniques and the means for ensuring of documentary security;
8. the measures for ensuring of personal security of the classified information;
9. the system of principles and measures for ensuring of industrial security.

(2) These Rules shall be implemented also with regard to foreign classified information, conceded by other state or international organisation, as far as other is not provided by an international agreement, to which the Republic of Bulgaria is a party.

Chapter two.

INFORMATION SECURITY

Section I.

Conditions and order for conceding and exchange of information

Art. 2.(1) In implementation of its functions under PCIA the State commission for security of information (SCSI), the services for security and the services for public order, as well as the respective organisational units shall create, process, maintain and preserve information funds.

(2) The specific rules for management of the data from the information funds of para 1 shall be determined with act of the chief of the respective organisational unit.

Art. 3. The information activity of SCSI and of the services for security and the services for public order shall be implemented observing the requirements for:

1. lawfulness;

2. objectivity, precision, comprehensiveness and observing the provided law terms;

3. (amend. - SG 79/20, in force from 08.09.2020) protection of the classified information, of the carriers of such information, , of the communication and information systems, and ensuring of access according to the order, established in PCIA and in the acts for its implementation;

4. ensuring of co-ordination, information exchange and interaction between the services for security and the services for public order according to their functions;

5. opportunity for integration of the information funds accounting for the ppecifics of the activity of the services for security and SCSI and establishing of unified information system ambience;

6. protection of the personal data and rights of the citizens at the collecting, the preservation, the use and the conceding of information.

Art. 4. The state commission for the security of information shall give instructions in connection with the exchange of information in implementation of the objectives of the PCIA between SCSI, the services for security and the services for public order, in co-ordination with the chiefs of this services.

Art. 5. (1) The information activity of SCSI and of the services for security shall include:

1. collecting, processing, systematising, preservation, use and conceding of information, referring to the functioning of the national system for protection of the classified information, as well as for the needs of the state management and for the implementing of their tasks and activities, determined by PCIA;

2. information – analytical and prognostic activity by preparing of assessments of the national system for protection of the

classified information and conceding them to other state bodies;

3. informing of the supreme management bodies of the legislative and the executive power, as well as the bodies of the local government about the status, the risks and the dangers for the correct functioning of the national system for protection of the classified information.

(2) The information activity of the services for public order and of the employees for security shall include the activities of para 1, item 1 within their authority for the respective organisational unit as well as information – analytical and prognostic activity by preparing of assessments about the status of the established systems for protection of the classified information within the respective organisational units and conceding them to SCSI.

(3) The activity for collecting and exchange of the classified information shall be implemented by SCSI, the services for security and the services for public order, as well as the employees for the security of information by collecting data:

1. presented voluntary by individuals and corporate bodies;

2. from state bodies, organisations and corporate bodies, maintaining information funds

3. from foreign states and organisations, received by the order of the international exchange or on the basis of international agreements;

4. from other sources of information.

Art. 6. At fulfilment of their functions under PCIA SCSI and the services for security shall collect and manage information about corporate bodies and individuals, sites and activities, as well as about facts and events, connected with them, having relation to the national system for protection of the classified information.

Art. 7.(1) Classified information shall be conceded by SCSI, the services for security and the services for public order and by the employees for security of the information to state bodies, organisations, corporate bodies and individuals only in the cases, provided in PCIA.

(2) The services for security and the services for public order can refuse conceding of information when this can lead to revealing of the person, who co-operates with the services, and with objective protection of the sources and the techniques for tacit collecting of information.

Art. 8. The state commission for the security of the information, the services for security and the services for public order according to their competence under the law shall have right to access to the information systems and the documents of information funds, about which there is information, that they contain data about the investigated persons, the data of art. 6 or data about activities, threatening the national system for protection of the classified information and the use of which can facilitate the preservation of the national system for protection of the classified information.

Art. 9.(1) The chairman of SCSI, the chiefs of the services for security and the services for public order or officials, authorised by them, shall direct written request to the bodies of the state power, the bodies of local government and the local administration, to individuals and corporate bodies and to all organisational units for conceding of the information and access to the necessary documents for confirmation of the data:

1. at conducting of the procedures for investigation, and

2. at implementing the functions of art. 9 and 12 of the PCIA.

(2) The persons of para 1 shall be obliged to concede the required information and access even when the data are not complete.

(3) The conceding of data shall be done free of charge in compliance with the request and according to the technical capacity of the respective fund and within term not longer than 14 days from the date of receiving of the request of para 1, unless in it a shorter term is defined.

(4) The term of para 3 may be extended by the applicant after receiving of a motivated written proposal by the obliged subject, competent to fulfil the request, but with not more than 14 days.

(5) Upon request of the applicant the obliged subjects of para 1 shall ensure for him physical access to the necessary documents from the information fund, which administrators they are, as well as concede if necessary copies or certified copies.

Art. 10. The State commission for security of information, the services for security and the services for public order shall at fulfilment of their tasks and activities mutually concede data under the conditions and by the order of the PCIA. For the purpose they can connect mutually their information systems by order, defined by SCSI.

Art. 11.(1) The services for security shall have right to track information by putting marking in the information funds and systems of the state bodies, of corporate bodies or individuals with objective acquiring of data, necessary for protection of the national system for classified information.

(2) With the marking of para 1 the services for security require:

1. information to be conceded to them and/or

2. to be notified about each change in the data of art. 6.

(3) The services for security shall require in writing the markings of para 1, pointing out the way of marking, the purpose of this measure, the term of effect of the marking and the way of delivering of the information.

(4) The state bodies, the organisations or the persons, who must concede data from their information massifs and/or have made the marking in their archives upon request by the services for security, shall implement the measure, pointed out in the written request of para 3, creating for this purpose the necessary organisational and technical prerequisites.

(5) The subjects of para 4 cannot inform the checked person, as well as other persons or organisations about the contents of the materials, pointed out, activities and undertaken measures, connected with the marking.

(6) Upon dropping of the grounds, being motive for making the marking, the services for security shall immediately inform in writing the administrators of data about termination of the effect of the marking.

Section II.
Information funds

Art. 12. (1)In implementation of their tasks and the activities under the PCIA SCSI, the services for security and the services for public order shall crate, process, maintain and preserve independent information funds.

(2) In implementation of the tasks and the activities of art. 20, para 1 and art. 22, para 1, items 1 and 4 of the PCIA in the organisation units shall be created information funds.

(3) The information funds of para 1 and 2 can also be automated, being crated, processed, maintained and preserved separately from the other information funds.

Art. 13. The state commission for security of information, the chiefs of the services for security and the services for public order and of the organisational units shall manage the established information funds, be responsible for their lawfulness and undertake measures for prevention of unregulated access and/or deleting of data.

Art. 14. In the information funds of SCSI, at the services for security and the services for public order, as well as at the organisational units are contained personal data under the conditions and with the amount, defined with the PCIA and with the Protection of Personal Data Act (PPDA).

Art. 15. (Amend. - SG 79/20, in force from 08.09.2020) The personal data, contained in the files for investigation for reliability of the persons according to art. 70, para 3 of the PCIA, shall be classified information, being official secret, unless in the collection of the materials and/or the documents of the file there is information of higher level of classification for security of information, called hereinafter "level ofr classification".

Art. 16. (Repealed - SG 79/20, in force from 08.09.2020)

Section III.
Conceding and exchange of classified information between the Republic of Bulgaria and other states or international organisations

Art. 17. A proposal for concluding of international agreements for protection of classified information can make the ministers and the chiefs of departments according to art. 3 of the International Agreements of the Republic of Bulgaria Act.

Art. 18. Decision for conceding or exchange of classified information under this section shall be taken by SCSI:
1. upon written request by other state or international organisation;
2. upon proposal by the chiefs of the organisational units;
3. upon proposal by the chiefs of the services for security and services for public order.

Art. 19.(1) In implementation of its authorities for protection of the classified information SCSI and the services for security shall co-operate with the respective bodies and services of other states and international organisations.

(2) The State commission for security of information upon proposal by the persons of art. 18, item 3 can issue permission for conceding or exchange of classified information under this section with services and bodies for security of other states or international organisations about classified information of mutual interest and within their competence.

(3) The permission of para 2 shall be general and contain the kind, the subject, the amount and the way of exchange of classified information, as well as the term, during which information is conceded or exchanged.

(4) The conceding or exchange of classified information shall be terminated with decision of SCSI upon proposal by the persons of art. 18, item 3.

Art. 19a. (New - SG 79/20, in force from 08.09.2020) (1) At the proposal of the persons under Art. 18, item 2, the **State Commission on Information Security** (SCIS) shall issue a permit for provision or exchange of classified information under this section with another state or with an international organization, for a specific case or for a certain period.

(2) In the proposal under Para. 1 shall obligatorily be indicated the state or the international organization, to which classified information must be provided, the need of such provision, the level of classification for security of the information to be provided, the type, subject, volume and manner of provision or exchange, as well as the period, during which such information must be provided or exchanged.

(3) The permit under Para. 1 shall contain the highest level of security classification of the information to be provided, the type, subject, volume and manner of providing or exchanging, as well as the period during which information will be provided or exchanged.

(4) The State Commission on Information Security shall refuse to allow provision or exchange in cases where there is no entered into force international agreement for protection of classified information with the respective state or international organization, or any of the conditions of provision or exchange contradicts the specific international agreement or the applicable law.

Art. 20. (amend. - SG 91/08) The permission for visit, given under art. 181, shall be considered as decision in the sense of art. 18.

Chapter three.
ORDER AND WAY FOR ANNOUNCING OF THE CATEGORIES OF INFORMATION, DEFINED AS OFFICIAL SECRET FOR THE SPHERE OF ACTIVITY OF THE ORGANISATIONAL UNIT AND LIST OF THE POSITIONS OR THE TASKS, FOR WHICH IS REQUIRED ACCESS TO CLASSIFIED INFORMATION, BEING OFFICIAL SECRET (TITLE AMEND. - SG 91/08)

Art. 21.(1) The chief of the respective organisational unit shall announce with an order the list of the categories of information, subject to classification as official secret.

(2) Chief of a state body, managing the rights of ownership of the state in organisational units – commercial companies with more than 51 percent state participation, shall announce with an order the general list of the categories of classified information, being official secret for the sector, sub-sector or the commercial activity.

(3) The list of para 1 shall contain only categories of information created, processed and preserved in the organisational unit, according to art. 26 of the PCIA, determined as secret in special laws.

(4) The scope of the list of para 1 can be narrower than the one provided in the special laws.

(5) The list of para 1 shall be public.

Art. 22. (revoked - SG 91/08)

Art. 23.(1) The chief of the organisational unit shall determine with an order list of the positions or the tasks, for which is required access to classified information, being official secret.

(2) (Suppl. - SG 79/20, in force from 08.09.2020) The chief of the respective organisational unit shall send a copy of the list of para 1 to the SCIS and to the respective security authority.

Art. 24. (amend. – SG 27/16, in force from 05.04.2016, amend. - SG 79/20, in force from 08.09.2020) The chiefs of art. 37, para 1 of the PCIA, except the chiefs of the State Intelligence Agency and of service "Military information" at the Minister of Defence, shall provide the lists of art. 37 to the respective service for security.

Chapter four.
ORDER FOR CONCEDING OF DATA FOR ENTERING IN THE REGISTER OF SCSI AND CONDITIONS AND ORDER FOR MAKING REFERENCES IN IT
Section I.

Register of classified information

Art. 25.(1) The register of classified information of art. 35 of the PCIA, called hereinafter "the register" shall contain data about:

1. the organisational unit, in which the respective material or document has been created;
2. the date of its creating and the provided date for removal of the level of classification;
3. identification number of the material or the document, under which it exists in this register;
4. the unique registration number of the material or the document, determine in art. 68, para 1;
5. the legal ground for classification of the material or the document;
6. the grading for security through the level of classification;
7. each change or removal of the level of classification of the material or the document, as well as the date of implementing it.

(2) The data from the register shall be conceded to persons, received permission for access to the respective level of classified information, and observing the principle "Need to know".

(3) References in the register of para 2 shall be made with written application to SCSI, in which are pointed out the data, for which is required the reference.

(4) The reference shall be in writing and it shall be issued by SCSI in 14 days after receiving the request.

Art. 26. To entering shall be subject only the circumstances of art. 25, para 1 and the consequent changes in them.

Art. 27. (1) The register shall be maintained as unifies electronic data base about the documents and materials, marked with grading for security.

(2) The State commission for security of information shall be responsible for the maintaining of the register as electronic data base and for the preservation of the information on magnetic carriers.

Section II.
Keeping of the register of classified information

Art. 28. (1) The data of art. 25, para 2 shall be conceded by the chief of the respective organisational unit or by official, authorised by him for entering in the register within terms, defined by SCSI, after giving of the unique number to the respective registry.

(2) The data of para 1 shall be conceded on physical carrier.

Art. 29. The activities for entering in the register shall be implemented by officials, determined with an order by the chairman of SCSI.

Art. 30.(1) The officials of this chapter shall be responsible for the reliability of the input information and for the observing of the term of art. 28.

(2) When it is found, that the term of art. 28 has not been observed, SCSI shall send a written signal to the respective body of appointment to undertake disciplinary measures for the guilty employees.

Art. 31.(1) The entering in the register shall be implemented on the basis of permanent individual identification number and separate file in the register, which shall be given to each registry of organisational unit, conceding information about the circumstances, subject to entering.

(2) The new circumstances shall be entered so, that the information, contained in the previous entering, is not affected.

(3) When an entered circumstance is deleted, in the respective field shall be recorded, that the entering is deleted, and a date shall be put. The deleting cannot lead to destroying or damaging of the information about the deleted entering.

(4) Errors, admitted at the entering, shall be corrected, noting in the respective field correction. The correction cannot lead to destroying or damaging of the information about the corrected circumstances.

Art. 32. The electronic data base shall be maintained in a way guaranteeing entity of the information and the controlled access to it for entering and reference according to the requirements of the PCIA.

Chapter five.
DOCUMENTARY SECURITY
Section I.
Marking of classified information and designation on the materials, containing classified information

Art. 33.(1) Each classified information , being state or official secret, shall be marked by putting on the material respective grading for security.

(2) The circumstance, that the classified information is marked, shall mean that:

1. material has been created, containing classified information, on which is put grading for security;

2. the material and the classified information are subject to measures for protection, corresponding to the level of classification, defined in the PCIA and in the acts for its implementation;

3. access to classified information shall be given to other organisational unit observing the principle "Need to know";

4. the classified information and the grading for security on the material can be changed only with the consent of the person of art. 31, para 1 of the PCIA or of his higher chief.

Art. 34.(1) The grading for security shall be put on visible place by typing, printing, writing, depicting, putting of labels, stickers or in another way, durably, clearly, legibly, understandably and without abbreviations.

(2) (amend. – SG 44/08) A record shall be worked out about the results of the checks of para 1 by the commission, which shall be conceded to the employee for security of information and to the State Agency "National Security".

Art. 35.(1) (Suppl. - SG 79/20, in force from 08.09.2020) The change of a put grading for security shall be implemented by crossing with one horizontal line each element of the grading, except for the date of creation of the document, in a way allowing its reading, after which a new grading for security shall be put.

(2) The new grading for security shall be put immediately next to the old one, noting: the new grading of security; the date of the change; the new date of expiry of the term for protection of the classified information, when it is different from these, pointed out in the law; the legal grounds for making of the change; the position, the name, the family name and the signature of the one, who makes the change.

(3) Deleting, erasing, physical removal or painting over of grading for security, subject to change, shall not be permitted.

Art. 36.(1) At removal of the classification of the information the grading for security shall be deleted each element of grading being crossed with one horizontal line in a way, allowing reading it without putting new grading for security.

(2) At removal of the classification shall be noted the date, the legal ground for the removal, the position, the name, the family name and the signature of the one, who makes the removal.

(3) (new - SG 68/17) In the cases of removal of the classification due to expiry of the terms for protection of the classified information, the security grading shall be considered deleted as the expiration of the respective term even without the actions under Para. 1 and 2.

Art. 37. (amend. - SG 91/08, amend. - SG 79/20, in force from 08.09.2020) The change of the grading for security shall be reflected in the respective register of art. 70, item 1.

Art. 38. On the material at a visible place shall be put unique registration number by typing, printing, writing, depicting, putting of labels, stickers or in another way, durably, clearly, legibly, understandably and without abbreviations.

Art. 39. Documents on paper, containing classified information shall be formed by putting the following designations:

1. on the first page:

a) at the highest part, centred, shall be put the name and the address of the organisational unit, where has been created the document on paper;

b) at the upper left corner immediately after the text of item a) shall be put the unique registration number of the document and the consequent number of the copy of it; in case document has been prepared in one copy, shall be written "only one copy";

c) in the cases of copying of the document on the copy under the designation of item b) shall be noted the consequent number of the copy;

d) at the upper right corner immediately after the text of item a) shall be put the grading for security, which shall contain the elements of art. 30, para 2 of the PCIA;

e) at the low right corner shall be put the number of the page and the number of the pages of the whole document, divided with the symbol "/";

2. on the second and the following pages:

a) at the upper right corner shall be put the level of classification;

b) (suppl. - SG 79/20, in force from 08.09.2020) at the lower left corner shall be put the unique registration number of the document and the number of the copy; in case of reproduction, the serial number of the copy shall also be placed on the made copy;

c) at the low right corner shall be put the number of the page and the number of the pages of the whole document, divided with the symbol "/";

3. on the last page shall be put the designations, pointed out in item 2 and after the end of the basic text shall be put:

a) description of the appendices with the following data: number of the appendix (title); level of classification; number of pages;

b) position, signature, name and family name of the person, who signs the document and date of the signing of the document;

c) the number of the printed copies and the addressee for each of them;

d) (suppl. - SG 79/20, in force from 08.09.2020) name and family name of the person having prepared the document, or a personal staff number for security services employees, public order services and the Office of Protection under the Prosecutor General, and date of preparing of the document – only if this person is different from the person, who signs the document;

e) (suppl. - SG 79/20, in force from 08.09.2020) name and family name of the person having printed the document, or a personal staff number for security services employees, public order services and the Office of Protection under the Prosecutor General and date of printing of the document – only if this person is different from the person, who signs the document;

f) the word "Co-ordinated:", signature, name and family name of the persons, who co-ordinate the document, and the date of co-ordinating of the document;

g) the number of the copies and the addressee of each of them;

4. the appendices of the document shall be designated by:

a) on the first page at the upper right corner is written "Appendix No … of document No …"; under this text is written the level of classification;

b) on the first page at the lower right corner are written the number of the page and the number of the pages of the appendix, divided with the symbol "/"; the appendix shall be numbered separately from the basic document;

c) on the second page and the following pages shall be put the designations of item 2.

Art. 40.(1) The person of art. 31, para 1 of the PCIA can write on the document the following orders to the addressee:

1. "The giving of information, contained in the document, without the written consent of the person, signed the document, is forbidden";

2. "The copying without the written consent of the person, signed the document, is forbidden";

3. "The transcribing without the written consent of the person, signed the document, is forbidden";

4. "The making excerpts without the written consent of the person, signed the document, is forbidden".

(2) On the document can be put also other orders, referring to the work with it.

Art. 41. For collection of documents, containing classified information, shall be put the following designations:

1. at the upper left part of the external side of the front cover shall be put the number, under which the collection of documents is registered in the register of art. 70, item 2;

2. in the middle of the external side of the front cover shall be written the nomenclature number and the topic of the collection of documents from the Nomenclature list of the collections of documents of art. 116;

3. at the upper right part of the external sides of the front and the back covers shall be put the level of classification of the collection of documents;

4. at lower left part of each page of the description of the documents shall be put the number of item 1 if the description does not contain classified information, or registration number by the order of art. 68, if the description contains classified information;

5. all other pages shall have the initial grading for security and designations of the respective document.

Art. 42. For printed issues or bound documents:

1. the front cover shall be formed according to art. 39, item 1 without the designations of item e);

2. on the external side of the back cover on the upper right part shall be put the grading for security;

3. the other pages shall be according to art. 39, item 2.

Art. 43. Films and sound records, containing classified information, being state or official secret, shall be marked by putting of grading for security on the physical carrier and they shall start and finish respectively with written or verbal information about the grading for security.

Art. 44. (amend. - SG 91/08) On boxes and packing, containing materials – carriers of classified information, grading for security shall be put, which is the same of the material with highest level of classification, in the ways, defined in art. 34.

Art. 45. If necessary upon proposal by the employee for the security of information the chief of the organisational unit can permit the putting of additional designations on the materials, which refer to and are valid only for the organisational unit.

Section II.
Classification of the information

Art. 46. The classification of the information shall be an activity upon which is established:

1. whether the concrete information is in the list of categories of information according to appendix No 1 of art. 25 of the PCIA or in the list of art. 26, para 3 of the PCIA;

2. is there threat or danger from damage or damage of the interests of item 1 in the respective degree, determined according to art. 28, para 2 and art. 26, para 1 in connection with § 1, item 15 of the additional provisions of the PCIA;

3. whether the unregulated access to it would create danger for the interests of item 1, and

4. are their public interests, subject to protection according to art. 25 and 26 and in connection with § 1, items 13 and 14 of the additional provisions of the PCIA.

Art. 47. (1) (Previous text of Art. 47 - SG 79/20, in force from 08.09.2020) The information shall be classified according to its own contents and not according to the classification of the information, on which it is based, or on the information it refers to.

(2) (New - SG 79/20, in force from 08.09.2020) The classification level of a document that includes annexes shall correspond at least to the highest classification level of those annexes.

Art. 48. Within the obligatory training of art. 38, para 1, item 2 of the PCIA the organisational units shall prepare their employees correctly to determine whether given information is classified, for defining the level of classification, as well as for the conditions and the order for its changing or removing.

Art. 49.(1) The chiefs of the organisational units shall determine internal rules observing the lawful requirements for the correct determining of the level of classification, as well as for its change or removal.

(2) In the rules of para 1 with regard to prevention the occurrence of damages in the sense of § 1, item 15 of the additional provisions of the PCIA for the sphere of activity of the organisational unit shall be graded the possible damages, which can occur as result of unregulated access to classified information, created or preserved in the organisational unit.

Art. 50. (suppl. - SG 68/17) The chief of the organisational unit shall create organisation and determine order for periodic reconsidering of the classified information, created in the organisational unit, with objective change or removal of the levels of classification or the extension of the terms for protection.

(2) (new - 68/17) Where national interests require an extension of the terms of protection under Art. 34 of the PCIA, the organisational unit in which the document is created, sends a written motivated request for extension to the SCSI, indicating the extension period, subject to the requirement of Art. 34, para. 2 of the PCIA. The request shall be sent at least three months before the expiry of the relevant protection period.

(3) (new - 68/17) The State Commission for the Security of the Information shall pronounce on the request within two weeks of its receipt by decision granting an extension of the time limit specified in the request or refusing an extension.

(4) (new - 68/17) The decision of the SCSI is final and cannot be appealed.

(5) (prev. para. 2 - SG 68/17) The level of classification shall be removed:

1. after the expiry of the respective term according to art. 34 of the PCIA;

2. after the expiry of the instructed term in the grading for secrecy;

3. upon falling away of the grounds for protection of the classified information.

(6) (prev. para. 3 - SG 68/17) The level of classification shall be changed:

1. upon change of the grounds for determining of the level of classification for security;

2. upon incorrect defining of the level of classification.

(7) (prev. para. 4, amend. - SG 68/17) In the cases of para 6, item 2 the person, established the incorrect defining of the level of classification, shall inform the person of art. 31, para 1 of the PCIA or his higher chief.

(8) (prev. para. 5, amend. - SG 68/17) The organizational unit shall notify in three months the SCSI and all the recipients upon extension of the terms for protection and at the change of the classification level or upon its removal carried out under Para. 5, item 3. In the cases of absence of notification in the specified term is considered that no extension of the term of protection, change of the classification level or its removal, was made under Para. 5, item 3.

(9) (prev. para. 6, amend. - SG 68/17) In cases under Para. 8 the recipients shall immediately mark the change or the removal of the grading for security on the material and reflect this circumstance in the respective registers.

(10) (prev. para. 7, amend. - SG 68/17) Always when it is possible, the person of art. 31, para 1 of the PCIA shall mark on the material orders for removal or change of the level of classification at the elapse of defined term or at the occurrence of certain event.

Section III.
Registries for classified information

Art. 51. (1) The chief of the organisational unit, in which is received, created, registered, processed, distributed, conceded and copied classified information, shall create registry for classified information as separate organisational division.

(2) The payroll detachment, the structure, the number of the employees and the measures for protection of the registry shall be determined depending on the levels of classification and the amount of the classified information.

(3) If necessary at the organisational unit can also be created more than one registry.

(4) In the structure of the registry, if necessary, can also be included other divisions, working with classified information as typing, copying, bibliographic, stenography, drawing, editing, distribution-courier etc.

(5) (Suppl. - SG 79/20, in force from 08.09.2020) If necessary, temporary points can be opened, which are divisions of the respective registry and ensure conditions for creating, receiving, registering, distribution, copying and guarding of classified information, received from the same registry, and when they are authorised by SCSI – also from other registries.

(6) The control point shall keep account of the movement of the materials – carriers of classified information, which are registered in it.

(7) For the registries and the control points shall be ensured separate premises, located in zones for security, corresponding to the levels of classification of the information and protected with the necessary measures for protection of the classified information under the PCIA.

(8) The chief of the organisational unit, in which is preserved and exchanged foreign classified information, shall organise, shall organise under the management of SCSI registry in the field of the international relations.

(9) The activity of the registry of para 8 shall be organised in compliance with the concluded international agreement and the rules for protection of the classified information of the respective international organisation or of the state – source of the classified information.

(10) At SCSI shall be created central registry in the field of the international relations.

Art. 52. (1) Depending on the amount and the character of the classified information the chiefs of organisational units can in co-ordination with SCSI open specialised units for preservation of materials, containing classified information.

(2) (New - SG 79/20, in force from 08.09.2020) In the foreign representations of the Republic of Bulgaria in coordination with the SCIS, specialized units for creation, processing, storage and destruction of materials containing classified information may be opened.

(3) (Previous Para. 2, amend. - SG 79/20, in force from 08.09.2020) The way of work with the materials of para. 1 and 2 shall be determined by the chiefs of the organisational units in compliance with the requirements of the PCIA, the Implementing Rules and other secondary legislation acts in the field of classified information protection.

(4) (New - SG 79/20, in force from 08.09.2020) The manner of work with cryptograms in the units under Para. 2 shall be determined by the ordinance under Art. 42, Para. 3 of the Act on the State Agency “National Security”.

(5) (Previous Para. 3, suppl. - SG 79/20, in force from 08.09.2020) Classified information, exchanged between the organisational units and their representatives abroad, shall be preserved in the organisational units within the statutory terms. In the specialized units under Para. 2, second and subsequent copies and copies of documents and materials containing classified information, shall be stored, within the statutory terms or until the necessity of their use disappears.

(6) (Previous Para. 4 - SG 79/20, in force from 08.09.2020) At the representations of the Republic of Bulgaria abroad as

exception, temporarily, can be preserved classified information with level of classification "Top secret" while observing the respective measures for security.

Art. 53. The registries are so equipped, that:
1. to be guaranteed the protection of the classified information from not regulated access, and
2. the revealing of the kind and of the character of the work, done by them to be not revealed.

Art. 54.(1) The registries shall be opened after check for meeting of the requirements for protection of the classified information and receiving of unique identification number from SCSI.

(2) The check of para 1 shall be implemented by a commission, appointed by the chief of the organisational unit, which shall include the employee for security, representative of the respective organisational unit and representative of the respective service for security.

(3) The commission of para 2 shall prepare a record in 3 copies – one for each SCSI, the service for security and the registry of the organisational unit.

(4) Immediately after receiving of the record of para 3 SCSI shall send to the organisational unit unique identification number of the registry.

Art. 54a. (new - SG 91/08) (1) (Suppl. - SG 79/20, in force from 08.09.2020) In case of changes to the circumstances on the grounds of which an unique identification number was issued, and also when increasing the level of classification of the information processed in the registry is necessary, and also when opening check points, a new check shall be carried out under the order of Art. 54.

(2) After receiving the protocol of the conducted check the SCSI shall take a decision for approval of the issued unique identification number.

Art. 54b. (new - SG 91/08) (1) A registry for classified information shall be closed, where no classified information is produced, processed or provided in it because of returning the information to the organisational units it was received from, destruction or moving to archive under the rules of Chapter Five, Section IX or other reasons.

(2) The proposal for closing the registry shall be made by the employee for security of information unless actually impossible and shall be approved by the head of the organisational unit. In case it is actually impossible the proposal for closing the registry shall be made by the head of the organisational unit or the maintainer of the registry.

(3) The proposal under Para 2 shall indicate the number of the documents and materials stored in the registry during its operation and the reason for closing the registry. A copy of the proposal shall be sent to SCSI and to the direct control body.

(4) The direct control body shall be obliged to perform a check under the order of the Ordinance on the Order for Performing

the Checks for Implementation of Direct Control for Protection of the Classified Information. After completion of the check the direct control body shall send to SCSI a report for the conducted check.

(5) On the basis of the data in the proposal and the report the SCSI shall take a decision for annulment of the unique identification number of which the organisational unit and the direct control body shall be notified.

Art. 54c. (New - SG 91/08, repealed - SG 79/20, in force from 08.09.2020)

Art. 55.(1) In the premises of the registries, which are not defined for work with the respective users of the organisational unit, can enter only the employees of the registry, the chief of the organisational unit, the employee for security of the information and the persons, defined with the order of art. 12 of the PCIA.

(2) If necessary the employee for security of information shall issue written permission for access to the pointed out premises of the registry also to persons out of these, pointed out in para 1.

(3) At disasters and accidents the access to the premises of the registry in working time shall be ensured by the employees of the registry and out of working time and on not working days – by an authorised official of the organisational unit.

(4) In the cases of para 3 the access to the premises of the registry shall be implemented with accompanying person - official of the organisational unit.

Art. 56. Classified information can be used, processed and preserved at the official premises of the users of the organisational unit only if they are in the respective zone for security and are protected with the necessary measures for security of information.

Art. 57.(1) The work with materials, containing classified information, preserved in the registries, shall be implemented only during the defined working time.

(2) Exception of para 1 shall be admitted with written permission by the employee for security of information.

Art. 58. The work with materials, containing classified information, out of the respective zones for security in the organisational unit shall be permitted by the employee for security of information, who shall determine also the respective measures for security at the transferring, the use and their preservation.

Art. 59. The cleaning, the repairs etc. of the premises of the registries shall be implemented after ensuring the necessary measures for protection of the classified information and in the presence.

Art. 60.(1) The activity in the registry and the employees in it shall be managed by chief of the registry, who is directly

subordinated to the employee for security of information.

(2) In the cases, when in the registry there is only one employee on the payroll, the chief of the organisational unit shall determine with an order also another employee, who meets the conditions for work in the registry.

(3) The employee, determined with an order of para 2, shall be trained about the measures for security in the registry, the rights and the obligations of the one, working in it and fulfil the obligations of employee in the registry in the cases of absence of the titulary.

Art. 61.(1) In the registry shall be appointed employees, who have permission for access to classified information with highest level of classification of the information, with which will be worked in the registry.

(2) Before starting work, the employees in the registry shall obligatory be trained to work in it.

Art. 62.(1) The chief and the employees in the registry shall:

1. be responsible for the availability and the correct accounting, receiving, use, distribution, conceding, collecting and preservation of materials, containing classified information;

2. be responsible for the accounting and the preservation of the materials, containing classified information, being in typing, copying and drawing bureaux, printing houses, photo-laboratories, depositories etc.;

3. preserve the lists of the employees, admitted to work with materials, containing classified information (appendix No 1);

4. follow the terms for protection of the classified information and report to the employee for security of information about their expiry;

5. organise the timely submitting to the archive of the materials with removed level of classification;

6. propose to the employee for security of information concrete measures for removal of existing weak points and breaches and participate in the organising and conducting of meetings, prophylactic and other measures, referring to improvement of the work for protection of the classified information.

(2) The chief of the registry apart from his obligations of para 1 shall:

1. regularly check the availability and the way of preserving of the materials, containing classified information, which are with the employees of the organisational unit; upon establishing of weak points and breaches report in writing to the employee for security of information and to the chief of the organisational unit;

2. immediately report to the employee for security of information about the cases of not regulated access to materials, containing classified information, and take measures for not admitting or restriction of the harmful consequences; inform the respective service for security through the employee for security ofr information about the cases of not regulated access to materials with level of classification "confidential" and higher;

3. take measures for returning in the registry of materials, containing classified information, which have not been returned till the end of the working time, except in the cases of art. 57, para 2.

Art. 63. At establishing of breaches of the respective measures for physical security of the premises of the registry the employees in the registry shall immediately notify the employee for security of information and the unit for guarding of the organisational unit, taking measures for preserving of the factual situation.

Art. 64. If there is attempt for not regulated access to classified information or at implemented such access the chief of the organisational unit shall inform the competent service for security and SCSI.

Art. 65.(1) The competent service for security shall:

1. implement check of the circumstances, connected with the attempt or the accomplished not regulated access to classified information;

2. undertake measures for restricting of the harmful consequences from the breach, and

3. notify the chief of the organisational unit, from which the materials originate, about the circumstances, lead to the unregulated access to classified information.

(2) The organisational unit of para 1, item 3 shall make assessment of the caused damages and undertake actions for restricting them.

(3) If there are data about implemented crime of general character the respective prosecutor's office shall be notified.

Art. 66. (Amend. - SG 79/20, in force from 08.09.2020) When the final report of the check of the competent service for security shows, that a material, containing classified information, has been irrevocably lost, the organisational unit shall remove it from account and inform the SCIS. The irrevocably lost material shall be considered destroyed in the sense of art. 33 of the PCIA.

Section IV.
Registration and accounting of the materials, containing classified information

Art. 67. For registration and accounting of the materials, containing classified information, in the registries shall be kept accounting documents.

Art. 68. (1) Each ultimately prepared material, containing classified information, being state or official secret, shall be registered with unique registration number in the respective registry in a register (appendix No 2).

(2) The unique registration number of the document or the material shall not be changed during the time of its existence.

(3) (New - SG 79/20, in force from 08.09.2020) In the specialized units under Art. 52, Para. 2, documents and materials, containing classified information, shall be registered in registers provided by the organizational unit, creator of the information, and the

cryptograms - in registers according to the ordinance of art. 42, para. 3 of the Act on the State Agency “National Security”.

Art. 69.(1) The registration number of art. 68 shall be comprised of:

1. unique identification number of the registry;
2. nomenclature number of register from the Nomenclature list of the registers of art. 74;
3. the consequent number of the material for the current year in the register (appendix No 2);
4. the date of registration.

(2) The unique registration number shall be written in the following format: number of the registry/number of the register – consequent number of the material in the register / DD.MM.YYYY.

Art. 70. At the registries shall be kept the following basic account documents:

1. registers for registering of the materials, containing classified information (appendix No 2);
2. registers of the account documents and/or the collection of documents (appendix No 3);
3. nomenclature list of the kinds of registers of items 1 and 2;
4. notebooks for reflecting of the movement of the materials within the organisational unit (appendix No 4);
5. control sheets for reflecting of acquainting with the documents (appendix No 5);
6. card – substitutes (appendix No 6) for work with collections of documents or with separate documents from them within the organisational unit;
7. descriptions of delivering and receiving of materials, containing classified information (appendix No 7);
8. delivery descriptions for delivering of materials, containing classified information, by the couriers to the recipients (appendix No 8).
9. (new - SG 79/20, in force from 08.09.2020) letters of expedition.

Art. 71. For improvement of the account and the protection of the materials, containing classified information, upon decision of the employee for security of information in the organisational unit can be:

1. supplemented the basic account documents of art. 70 with data and designations, which are not pointed out in the samples;
2. kept also other account documents apart from the obligatory of art. 70.

Art. 72. (1) In the organisational unit, depending on the concrete need, can be kept different kinds of registers (appendix No 2), as follows:

1. for all materials, containing classified information;
2. for incoming materials, containing classified information;

3. for outgoing materials, containing classified information;

4. (suppl. - SG 79/20, in force from 08.09.2020) for physical carriers for multiple recording of classified information;

5. for subjects, being state or official secret.

(2) Materials, containing classified information with level of classification "Top secret", shall be registered in separate registers (appendix No 2).

(3) The designation of the separate registers (appendix No 2) shall be determined by the employee for security.

Art. 73.(1) In the registers of art. 70, item 2 (appendix No 3) shall obligatory be registered all volumes (parts) of the registers of art. 70, item 1 (appendix No 2), of the collections of documents and the notebooks of art. 70, item 4 (appendix No 4) , which shall be kept in the registry.

(2) The employee for security of information shall determine which of the rest of the account documents to be kept in register (appendix No 3) and the designation of the separate registers (appendix No 3).

Art. 74. The Nomenclature list of the registers of art. 70, items 1 and 2 (appendices 2 and 3) shall be signed by the employee for security of information in the organisational unit and it shall contain a table with the following columns:

1. nomenclature number of the register;

2. (amend. - SG 79/20, in force from 08.09.2020) topic (designation) of the register (e.g. for incoming documents, physical carriers for multiple recording of classified information, for collections of documents; for account documents etc.);

3. level of classification of the register, if there is such.

Art. 75. (1) The notebook of art. 70, item 4 (appendix No 4) shall be designated for use in the registries and for use by the employees in the organisational unit. When used by the employees, in it shall be kept:

1. the materials, conceded to the employee or received by him;

2. the materials, preserved by the employee.

(2) The concrete designation of the notebook of para 1, which are kept in the registry, shall be determined by the employee for the security.

(3) (Amend. - SG 79/20, in force from 08.09.2020) In the registry can be kept separate notebooks (appendix No 4) for reflecting the movement of the documents with levels of classification – for physical carriers for multiple recording of classified information, for objects representing state or official secret, etc.

Art. 76.(1) The control sheet of art. 70, item 5 (appendix No 5) shall accompany the material till its submitting to archive or destroying.

(2) The control sheet shall be a separate document, which shall be destroyed with the submitting to archive or the destroying of the material, containing classified information, being state or official secret, in connection with which it has been issued.

Art. 77. The account documents on paper must be reliably bound, with consequent numbered sheets and certified with the signature for security of information.

Art. 78.(1) The account documents on paper shall be written with blue
boll-point pen (ink), precisely, clearly and legibly, in Bulgarian, except in the cases, provided in these Rules.

(2) At change of the grading for security the new data shall be written under the previous, the old being crossed with two horizontal lines in a way allowing the reading of the crossed information.

(3) At admitted mistakes all corrections shall be made by the chief of the registry with red boll-point pen (ink) and shall be certified with his signature.

(4) The data, written on the account documents, shall not be deleted, but crossed with two horizontal lines in a way, allowing the reading of the crossed information.

(5) At the end of each calendar year the registers of appendix No 2 shall be finished with full line under the last registered material and in this way is finished the giving of new consequent numbers for the respective year. Under the line shall be described the number of the used registration numbers and the signatures of the employee of the registry, keeping the respective registry and of the chief of the registry.

(6) The order of para 5 shall be applied also for other account documents, for which is necessary annual accounting of the work.

(7) The registers of appendix No 3 shall not be finished and the numbers shall be continuous.

Art. 79. (1) (Amend. - SG 79/20, in force from 08.09.2020) The account documents of this section shall be kept always when there is technical opportunity in electronic form in communicational and informational system (CIS), which is accredited by the order of art. 91 of the PCIA or is an element of such an accredited CIS;

(2) (Amend. - SG 79/20, in force from 08.09.2020) The keeping in electronic form must provide:

1. (repealed - SG 79/20, in force from 08.09.2020)

2. (amend. - SG 79/20, in force from 08.09.2020) maintainance and printing of the data, pointed out in the samples of account documents of art. 70;

3. (amend. - SG 79/20, in force from 08.09.2020) data exit in format, established by SCIS for automated keeping of the register of art. 35 of the PCIA.

(3) After the finishing of the calendar year the registers of art. 70, para 1 and 2, kept in electronic form, shall be printed out on paper and formed in the way, pointed out in art. 77. Printing out of these registers can be made also after written permission by the

employee for the security of information. At printing out of the registers division of the different types of data shall be permitted.

Section V.
Sending, submitting, transfer and receiving of materials, containing classified information

Art. 80.(1) The documents, containing classified information, which are sent to other organisational units recipients, shall be prepared in at least two copies.

(2) The first copy, called original, shall be preserved in the registry of the organisational unit, in which the document has been created, and the other copies shall be sent to the addressees.

(3) All documents, sent to other organisational units, shall be sealed with the seal of the organisational unit.

Art. 81. (1) The transfer of materials, containing classified information, can be done:

1. through a special courier service (SCS);
2. through a courier of the organisational unit;
3. (amend. - SG 79/20, in force from 08.09.2020) through communicational and information systems (CIS);
4. with the post;
5. through military post connection upon announce martial law or state of war.

(2) Each courier, carrying materials, containing classified information, on the territory of the country, shall be accompanied by at least one employee, who is guard.

(3) The courier, carrying materials, containing classified information, on the territory of the country, and the guard shall carry arms.

(4) (new – SG 64/16, in force from 16.08.2016) Carrying weapons by couriers and guards shall not be compulsory during transfer of materials, containing classified information, between registries located in one and the same guarded building.

Art. 82.(1) (suppl. - SG 07/09, amend. – SG 27/16, in force from 05.04.2016) Materials, containing classified information with level of classification "Top secret", shall be transferred only by the special courier service, except the Armed forces, the Ministry of Interior, the National Agency "National Security", the State Intelligence Agency and the National service for guarding, who can transfer these materials also with their couriers.

(2) Materials, containing classified information with level of classification "Secret" or "Confidential", shall be transferred by the order of art. 81, para 1, items 1, 2 and 3.

(3) Materials, containing classified information with level of classification "For official use" can be sent by the order of art. 81, para 1.

(4) Foreign classified information shall be transferred by the order of art. 81, para 1, items 1, 2 and 3, unless an international

agreement, to which the Republic of Bulgaria is a party, provides other.

Art. 83. The sending of materials of art. 82, para 3 by post shall be done only registered with receipt, preserved for one year in the registry, which has sent the material.

Art. 84. (Amend. - SG 79/20, in force from 08.09.2020) The transfer of documents containing classified information through CIS shall be implemented only on condition that the CIS has a certificate issued under Art. 14, item 2 of CIPA and in compliance with the established requirements for protection of classified information.

Art. 85.(1) The materials, containing classified information, being state secret, which are transferred by courier, shall be in packs.

(2) The packs are two strong, not transparent, put one into other packs of envelopes, reliably sealed and stuck all over in a way, not allowing taking out of the materials from the packing without damaging the content or the seals of these packs (appendix No 9).

(3) Courier bag, box or case with ciphering or sealing device shall be considered as external packing.

Art. 86. The transfer of the packs with courier shall be implemented with appropriate bags (cases), guaranteeing their security and entity.

Art. 87.(1) Materials, containing classified information, which due to their dimensions, weight and form cannot be put in packs, bags or cases of art. 85, shall be transferred packed and covered so, that to be guaranteed from unregulated access.

(2) Beyond the cases of para 1 when the physical carrier of classified information - due to its nature or dimensions - cannot be transferred (transported) by the general order, special measures for security shall be taken, provided in the ordinance of art. 78 of the PCIA.

Art. 88.(1) The employees of SCS shall be admitted to work after conducting of training and exam, the results of which shall be reflected in a record.

(2) (suppl. - SG 79/20, in force from 08.09.2020) SCSI shall issue a special official (courier) card to the couriers, admitted to work, with which they shall identify themselves at fulfilment of their official obligations.

Art. 89. (1) (Previous text of Art. 89 - SG 79/20, in force from 08.09.2020) An employee (courier) of the organisational unit can carry packs with materials, containing classified information, except the materials with level of classification "Top secret", except

the cases of art. 82, para 1, after conducting of training and exam, the results of which are reflected in a record.

(2) (New - SG 79/20, in force from 08.09.2020) To the employees (couriers) under Para. 1, who have successfully completed training, the SCIS shall issue a special official (courier) card, with which they identify themselves in the performance of their official duties.

(3) (New - SG 79/20, in force from 08.09.2020) The employees of the security services may transfer packages with materials containing classified information, after conducting training and examination, by identifying themselves with their official cards.

Art. 90. (Repealed - SG 79/20, in force from 08.09.2020)

Art. 91. (1) The couriers shall carry the packages with materials, containing classified information in the country travelling with official automobiles or in a separate compartment in post carriage or in a carriage of BSR, which shall not be subject to check or with aviation means.

(2) The carrying of packages with materials, containing classified information in other state shall be implemented by service "Diplomatic couriers" at the Ministry of Foreign Affairs or by special courier with air or other transport, taking measures for protection of the information from unregulated access.

Art. 92. The services for public order shall render co-operation to the couriers at fulfilment of the tasks, connected with the carrying of materials, containing classified information.

Art. 93. (amend. - SG 91/08) To the couriers shall be ensured access to the registry or place in the security zone in the organisational units, where is implemented accepting and delivery of packages with materials, containing classified information.

Art. 94. (1) For sending of materials, containing classified information, being state secret, to certain recipient an expedition letter shall be prepared in two copies: the first one is left for preservation at the registry and the second is sent to the recipient.

(2) The letter of para 1 shall contain:

1. the name of the recipient;

2. the unique registration numbers of the materials;

3. the level of classification of each of the materials;

4. the number of pages of each of the documents; in case the document has appendices, the total number of pages shall be recorded, including the appendices and the total number of pages of the appendices in format "total number of pages, including the appendices + number of the appendices / total number of pages of the appendices".

(3) The letter of para 1 shall receive number from the registry.

(4) The materials shall be put in the internal packing and the expedition letter – between the two packings of the package of

art. 85.

(5) On the external packing of the package of art. 85 shall be written without abbreviations:

1. at the upper left part – the sender and his precise address;

2. at the lower right part – the recipient and his precise address;

3. (amend. - SG 91/08) at the upper right part – the number of the expedition letter, which shall be considered as number of the package.

(6) At carrying with courier on the external packing shall be written "Only by courier".

(7) On the internal packing shall be written without abbreviations:

1. at the upper left part – the sender;

2. at the lower right part – the recipient;

3. (new - SG 79/20, in force from 08.09.2020) at the top and at the bottom - an appropriate level of classification, but not lower than the highest level of the documents contained in the package.

(8) If necessary on the internal packing shall be written "To be opened by …", pointing out the name and the position of the person, to whom is addressed the material.

Art. 95.(1) The delivery of a packages to a courier of the SCS shall be implemented with description of art. 70, item 7 (appendix No 7), which shall be prepared in two copies:

1. copy No 2 with the signature of the courier and the seal of SCS shall be preserved at the registry of the structural unit;

2. copy No 1n with the signature and the seal of the organisational unit shall be preserved at SCS.

(2) The special courier service shall sort the packages according to routes and addressees and prepare delivery descriptions of art. 70, item 8 (appendix No 8).

(3) The couriers of SCS shall distribute the packages and deliver them to the recipients against signature and seal in the delivery descriptions (appendix No 8).

Art. 96.(1) At sending of packages with courier the organisational unit shall prepare description of art. 70, item 7 (appendix No 7) in three copies.

(2) Copy No 3 with the signature and the seal of the courier shall remain in the registry of the organisational unit.

(3) Copies No 1 and 2 shall be signed by the employee, who delivers the packages, copy No 1 being stamped with the seal of the organisational unit.

(4) Copies No 1 and 2 shall be delivered to the courier.

(5) After the delivery of the packages the employee, who has accepted them, shall sign copy No 2 of the description, put seal of the addressee, date and hour of receiving and return it to the courier.

(6) Copy No 1 shall remain for preservation at the registry of the addressee.

(7) Copy No 3 shall be destroyed after the courier returns copy No 2 at the registry, sent the packages.

Art. 97. The descriptions of delivered and received packages with materials, containing classified information, shall be filled in legibly and shall be preserved for 3 years after which they shall be destroyed.

Art. 98.(1) The packages with materials, containing classified information, shall be accepted by defined employee of the registry of the organisational unit.

(2) Out of working time, as exception, the packages shall be accepted by employee on duty of the organisational unit and shall be registered in a book according to a model, approved by the employee for security. The packages shall be preserved at a place, meeting the requirements for physical security (premises, case, safe) and delivered immediately, without unsealing at the start of the working time to the to the employee of para 1 against signature.

(3) At the receiving of the packages the employee of the registry shall check the compliance of the numbers of the packages (the envelopes) with those, pointed out in the description, the address, the intactness of the seals and the packing, after which he shall certify with a signature the copy of the description for the carrier, writing legibly his family name, the date and the hour of receiving and put seal of the organisational unit.

(4) Upon established defects or non compliance in the form of the external packing or the accompanying descriptions they shall be removed on the place or the packages are not accepted. The not accepted packages shall crossed in the description in a way, allowing the crossed to be read, after which the description shall be certified with the signature of the courier, with seal and data.

(5) The packages, received with inscription "To be opened by …", shall not be opened by a person, different from the one, pointed out in the inscription. The employee from the registry shall register them not opened in register under art. 70, item 1 (appendix No 2) and deliver them in the quickest way to the recipient.

(6) If there are no instructions of para 5 the employee of para 1 shall be obliged to open each package, to compare the numbers of the materials with the numbers from the expedition letter and to check the numbers of the sheets of the documents and the appendices.

(7) Upon established defects and/or non compliance the employee for security of information shall immediately be informed and a record shall be prepared. A copy of the record shall be sent to the sender.

(8) If after the opening of the package it is found, that the material has been designated for other recipient, the wrong recipient shall immediately return it to the sender. On the new packing of the material shall be written "Arrived by mistake" and shall be added the name and the address of the organisational unit, which has received the material by mistake, the date and the signature of the employee of para 1.

Art. 99. It shall not be permitted, except in the cases, provided in these Rules, the delivering and the accepting of:

1. materials, containing classified information, out of the zone for security of the respective organisational unit as well as in

dark and not lighted premises;

2. packages with arms, explosives and easy inflammable substances as well as cutting objects;

3. packages with incorrect and unclear addresses of the sender and the recipient;

4. packages with low quality or damaged packing or seals;

5. packages with dimensions and weight below or above the established according to appendix No 9;

6. packages, stamped with seals, which are not of the sender.

Art. 100.(1) All materials, containing classified information, received at the registry, shall immediately be registered in the register of art. 70, item 1 (appendix No 2).

(2) Materials, containing classified information, shall not be reported and delivered for fulfilment before being registered.

(3) If necessary to the documents shall be attached control sheets of art. 70, item 5 (appendix No 5).

Section VI.
Obligations of the employees, received permissions for access to classified information

Art. 101.(1) The employees of the organisational unit, received permissions for access to classified information, shall observe rules for work with classified information.

(2) At creating, preservation and work with materials, containing classified information, the employee of para 1 shall be responsible for their availability, submitting them at the end of the work with them personally to the registry.

(3) At loss of materials, containing classified information, the employees of para 1 shall immediately inform the chief of the registry and the employee for security of information.

Art. 102. It shall be prohibited to the employees of art. 101, para 1:

1. to divulge classified information in breach of the order, established with law;

2. (amend. - SG 79/20, in force from 08.09.2020) to submit classified information on communication means without the respective measures for protection, as well as to record classified information on carriers not registered in advance;

3. to take materials, containing classified information out of the organisational unit and in violation of the order, established for that;

4. to submit materials, containing classified information, to other services and departments in violation of the order, established for that;

5. to leave after working time materials, containing classified information, in the working premises (desks, cases etc.) if they do not comply with the respective measures for security of information;

6. to copy, photograph and destroy materials, containing classified information, in violation of the order, established for that;

7. to use materials, containing classified information, for open publications, diploma theses, dissertations, reports, presentations etc.

Art. 103. The submitting and the receiving of materials, containing classified information, by the employees of art. 101, para 1, shall be implemented personally against signature in a notebook (appendix No 4), kept in the registry, or in a card – substitute (appendix No 6).

Art. 104. The acquainting and the work with materials, containing classified information, shall be implemented at the registry or at the working premises of the employees of art. 101, para 1, if they are in the respective zones for security.

Art. 105.(1) The employee, received material, containing classified information, or who prepares such material, shall note it in his personal notebook (appendix No 4). The noting shall be made immediately after the accepting of the material or after the giving of registration number for newly created material, containing classified information.

(2) The employee, who is only acquainting with material, containing classified information, without receiving it for work, shall not make note in his personal notebook (appendix No 4), and only sign in the control sheet (appendix No 5), created for the material.

(3) After finishing the work with the document the employee shall write on the first page the nomenclature number of the collection of documents, to which it shall be attached, and sign.

Art. 106. Upon official need against a signature in the personal notebook (appendix No 4) the employee can give for temporary use materials, containing classified information, to other employees of the same organisational unit, who have the respective permission for work with classified information.

Art. 107. Notes or records, containing classified information, shall be recorded:

1. in working notebooks or jotters, which are duly bound, with consequently numbered sheets and registered at the registry;

2. (amend. - SG 79/20, in force from 08.09.2020) on carriers, used in CIS with an issued certificate as per Art. 14, item 2 of the CIPA and registered at the registry.

Art. 108.(1) After the ultimate preparing of a document, containing classified information, it shall be registered in the respective register (appendix No 2) and shall be printed in the defined number of copies.

(2) The order for accounting and destroying of the working versions of documents shall be determined by the chief of the organisational unit upon proposal of the employee for security.

Art. 109.(1) Persons, who are not employees of the organisational unit, can acquaint with the content of documents, registered in it, only after permission by the chief of the organisational unit or by the employee for security of information, if they have respective permission for access to classified information and observing the principle "Need to know".

(2) If necessary the chief of the organisational unit or the employee for security of information shall have right to check in the organisational unit, from which is the person, whether he has permission for access to classified information and to what level.

Section VII.
Copying or making excerpts from documents, containing classified information

Art. 110.(1) Documents, containing classified information, shall be multiplied in premises, which are located in zones for security, corresponding to the level of classification, and with corresponding measures for protection of information.

(2) The employees, who can multiply documents, containing classified information, must have permission for access to the respective level of classified information.

Art. 111. (Amend. - SG 79/20, in force from 08.09.2020) The multiplication of documents, containing classified information, shall be done:

1. if there is no explicit order prohibiting the multiplication of the document;

2. (amend. - SG 79/20, in force from 08.09.2020) after an order for reproduction, given by the Head of the organizational unit or by a person determined by a Head’s order;

3. (amend. - SG 79/20, in force from 08.09.2020) the documents with level of classification "Top secret" shall be reproduced only after preliminary written permission of the person of Art. 31, Para. 1 of the CIPA or of the organizational unit, from which the document originates, which is attached to it;

4. for documents with level of classification "For official use" - after permission of the direct Head of the person, performing the reproduction.

Art. 112. (Repealed - SG 79/20, in force from 08.09.2020)

Art. 113.(1) On the document, containing classified information, copies of which are made, shall be noted: the date of their preparation; the number of the copies; the reason for the multiplication; the name of the person, who has given permission for multiplication, and the name and the signature of the person, who has made the copies.

(2) On the first page of each copy at the upper left part shall be put the designation of art. 39, item 1, letter "c".

(3) In the respective registration diary (register) of appendix No 2 in column "Note" next to the registration number of the document, from which copies are made, shall be recorded the date and the number of the copies made.

Art. 114.(1) The making of excerpts form documents, containing classified information, shall be implemented:

1. if there is no explicit order, prohibiting the copying or making excerpts from the document, and

2. only in registered at the registry working notebooks or jotters with respective level of classification, or

3. by creating of new document, which shall be marked and registered by the order of section IV.

(2) At creating of new document, containing excerpts from other documents, the newly created document shall receive level of classification, corresponding to the highest level of classification among the documents, from which the excerpts are made.

Section VIII.
Collections of materials

Art. 115. Documents, containing classified information, with which the work has finished and verbal instruction is given in the sense of art. 105, para 3, can be collected according to certain topic in collection of documents.

Art. 116.(1) Each organisational unit shall prepare nomenclature of the collections of documents, which shall be described in nomenclature list of the collections of documents.

(2) The nomenclature list of para 1 shall be approved by the employee for security of information and it shall contain table with the following columns:

1. nomenclature number of the collection of documents;

2. topic (designation) of the collection of documents;

3. (amend. - SG 91/08) level of classification of the collection of documents under art. 30, para 3 of the PCIA;

4. the administrative – structural division of the organisational unit, which activity is connected with the topic of the collection of documents.

Art. 117.(1) In each collection of documents shall be prepared and put description, which shall contain:

1. the identification number of the registry;

2. the nomenclature number of the collection of documents under art. 116, para 2, item 1;

3. the number of the volume of the collection of documents;

4. table with the following columns:

a) consecutive number;

b) the unique registration number of the document;

c) name and short description of the contents of the document;

d) number of sheets of the document; in case the document has appendices, the total number of pages shall be recorded,

including the appendices, the number of the appendices and the total number of pages of the appendices in format "total number of pages, including the appendices, and number of the appendices/total number of pages of the appendices";

5. signature, first and family name of the chief of the registry.

(2) With each collection of documents can be put a list of those, who have right to receive and to work with the collection of documents and the level of classified information, to which they have permission for access.

(3) (amend. - SG 91/08) To each collection of documents shall be attached the card – substitute under art. 70, item 6.

(4) The using of the collections of documents or of separate documents from them shall be implemented against signature in the card – substitute by the order of art. 57.

Art. 118.(1) The documents shall be arranged in the collections of documents by the order of their preparation, complementing the description.

(2) The first copies (originals) of the documents, prepared in the organisational unit, shall be put in the collections of documents.

Art. 119. (amend. and suppl. – SG 44/08, amend. – SG 27/16, in force from 05.04.2016) The order for registering, movement, preservation and using of files, connected with the operational and/or the operational – investigation activity of the services for security and the services for public order, shall be determined by the Minister of Interior – for the services, subordinated to him, by the Chairman of the State Agency "National Security" – for the agency, by the directors of service "Military police" and of service "Military information" at the Minister of Defence – for these services, by the directors of the State Intelligence Agency and of the National service for guarding.

Section IX.
Destroying of materials or submitting them to archive

Art. 120.(1) (amend. - SG 91/08) The chief of the organisational unit shall appoint with an order a commission for preparing of proposal for destroying of materials – carriers of classified information, or their submitting to archive in compliance with the requirements of art. 33, para 2 of the PCIA.

(2) The commission of para 1 shall consist of at least three members.

(3) The commission of para 1 shall at least once in two years:

1. make assessment and give conclusion which information with expired term for protection has historic, practical or reference significance and propose it to be submitted to archive;

2. make proposal for destroying of materials with expired term of classification, which shall not be submitted to archive under item 1;

3. make assessment and proposal for destroying of materials, containing classified information, under art. 121, para 1, items 2, 3 and 4.

(4) (New - SG 79/20, in force from 08.09.2020) The destruction of the cryptograms in the representations abroad shall be carried out under the conditions and by the order of the ordinance of Art. 42, Para. 3 of the Act on the State Agency "National Security".

Art. 121. (1) The following materials shall be destroyed:

1. first copies (originals) of materials – carriers of classified information with expired term of protection;
2. second and following copies of materials, containing classified information;
3. personal working notebooks and jotters of the employees, containing notes and data, being state or official secret;
4. account documents of section IV of this chapter.

(2) The materials of para 1, item 1 shall be destroyed at least one year after the expiry of the term for protection upon proposal by the commission of art. 120 and after decision of SCSI.

(3) The destroying of materials under para 1, item 2 shall be prohibited in the cases when the person of art. 31, para 1 of the PCIA has explicitly recorded such ruling on the document.

(4) (New - SG 79/20, in force from 08.09.2020) In critical situations in the specialized units under Art. 52, Para. 2, for the purpose of protection from unregulated access to classified information, stored in them, the same shall be destroyed in observance of the requirements of Art. 125 and the rules for action during critical situations in the respective unit, approved by the Head of the organizational unit.

(5) (New - SG 79/20, in force from 08.09.2020) The employee, who has carried out the destruction under Para. 4, shall prepare a protocol, in which the events are described - the reason for the critical situation, as well as details regarding the level of classification, the type of carriers of classified information, the number of pages and manner of destruction. The protocol shall be presented to the Head of the organizational unit.

(7) (Previous Para. 5 - SG 79/20, in force from 08.09.2020) Account documents shall be destroyed after all the materials, registered in them are destroyed or submitted to archive.

Art. 122. (1) The commission of art 120 shall prepare written proposal to SCSI for destroying of first copies (originals) of materials – carriers of classified information, with expired term of protection, which has no historic, practical or reference significance.

(2) The proposal of para 1 shall contain description of the materials, proposed for destroying, as well as the factual and the legal grounds for this.

(3) (Amend. - SG 79/20, in force from 08.09.2020) The State commission for security of information shall issue a written decision allowing or refusing to allow the destruction of the proposed materials, which is an individual administrative act in the sense of the the Administrative-Procedure Code.

Art. 123.(1) After receiving of permission from SCSI, respectively by the chief of the organisational unit, the materials shall be destroyed in the presence of all members of the commission of art. 120, about which a record shall be compiled.

(2) The record of para 1 shall be signed by all the members of the commission and approved by the chief of the organisational unit.

(3) At destroying of materials under art. 121, para 1, item 1 in the record of para 1 shall be reflected the number of the written decision of SCSI

Art. 124. A copy of the record of art. 121, para 1, item 1 shall be sent to SCSI by the organisational unit.

Art. 125. The destroying of materials under art. 121, para 1, items 2, 3 and 4 shall be implemented in a way not allowing entire or partial restoring of the material and reproduction of the information.

Art. 126. (1) Documents under art. 33, para 2 of the PCIA shall be submitted to archive.

(2) (amend. – SG 84/07, in force from 19.10.2007) Before the submitting of the documents to archive they shall be formed in duly bound collections of documents with internal descriptions according to the requirements, determined by the Act on the National Archive Fund (ANAF).

Art. 127. (1) (amend. – SG 84/07, in force from 19.10.2007) The collections of documents, prepared for submitting to archive, shall be entered in inventory description, which form is to be defined by State Agency "Archives".

(2) A copy of the inventory description of para 1, together with the prepared collections, shall be submitted to the respective archive.

(3) A copy of the inventory description of para 1 shall also be preserved at the organisational unit.

Art. 128.(1) The records of art. 123, para 1 and the inventory descriptions of art. 127, para 3 shall be formed in collections of documents, which shall not be finished and submitted to archive.

(2) Corrections and crossing on the records and the inventory descriptions of para 1 shall not be permitted.

Section X.
Control over the registries

Art. 129. The management of the organisational unit, the employee for security of information and the persons, determined by the order of art. 12 of the PCIA, shall implement control over the whole activity and the status of the registry.

Art. 130.(1) The control of art. 129 shall be current and periodical.

(2) The current control shall be organised by the chief of the organisational unit and by the employee for security of information and it shall include planned and off plan, annual, partial and overall checks.

(3) The periodic control shall be direct control and it shall be implemented by the persons of art. 12 of the PCIA.

(4) The control of para 3 shall be implemented by order, defined with the ordinance of art. 13 of the PCIA.

Art. 131 The overall check of the registry shall be implemented upon change of the chief of the registry or established unregulated access to material – carrier of classified information, registered at the same registry.

Art. 132. (1) Out of the cases of art. 130 shall be implemented also monthly internal checks by the chief of the registry, when shall be checked:

1. the availability of the worked out and the received materials, containing classified information;
2. the availability of the materials, containing classified information, being with the employees of art. 101, para 1;
3. the keeping of the account documents, and
4. the status of the registry.

(2) The chief of the registry shall prepare a record about the results of the check of para 1, which shall be conceded to the employee for security of information.

Art. 133. The chief of the organisational unit shall every year appoint commission for implementing annual check of the registry with an order.

Art. 134. (1) The annual check of the registry shall be implemented by comparing the accounted documents about the factual availability of the materials and also with the acts for destroying of materials for the current year and with the descriptions for receiving and sending of materials.

(2) A record shall be worked out about the results of the checks of para 1 by the commission, which shall be conceded to the employee for security of information and to the competent service for security under art. 12 of the PCIA.

Art. 135. (1) Upon change of the chief of the registry all the materials, containing classified information, shall be submitted/accepted with a commission, appointed with an order by the chief of the organisational unit.

(2) The commission of para 1, the one submitting and the one accepting shall check the availability of all the materials, containing classified information.

(3) The commission shall prepare a record for delivery and accepting, in which shall be reflected the availability of the materials, the status of the registry and the found breaches, if there are such.

(4) The delivery and the accepting shall be considered accomplished after approval of the record of para 3 by the chief of the organisational unit.

(5) (New - SG 79/20, in force from 08.09.2020) In the specialized units under Art. 52, Para. 2, the activities under Para. 1-4 shall be carried out in case of change of employees in them.

Section XI.
Marking and account of classified information in communication and information systems (Title amend. - SG 79/20, in force from 08.09.2020)

Art. 136. (Amend. - SG 79/20, in force from 08.09.2020) Classified information, created, processed, preserved and exchanged in certified CIS, shall be marked with the respective level of classification for security and shall be accounted by the order of art. 90, para 1 of the PCIA and not by the order of the Rules.

Art. 137. (Amend. - SG 79/20, in force from 08.09.2020) At exit of documents, containing classified information, from certified CIS:

1. the printed out documents must have grading for security and be registered at the registry;

2. (amend. - SG 79/20, in force from 08.09.2020) recording of documents must be done only on physical carriers for multiple recording of classified information registered at the registry.

Section XII.
Registering, marking, account and destroying of physical carriers for multiple recording of classified information and of classified information in the area of cryptographic security (Title amend. - SG 79/20, in force from 08.09.2020)

Art. 138. (1) (Amend. - SG 79/20, in force from 08.09.2020) The physical carriers for multiple recording of classified information shall beregistered as a unique copy, shall be kept in account in a separate register under art. 72, para 1, item 4 and shall be marked with a registration number and grading for security.

(2) (Amend. - SG 79/20, in force from 08.09.2020) The markings as per Para. 1 shall be put before the initial use of the carriers.

(3) (New - SG 79/20, in force from 08.09.2020) The markings under Para. 1 shall be placed in a visible place by stamping, printing, writing, depicting, affixing labels, stickers or otherwise, permanently, clearly, legibly, intelligibly and without abbreviations, in a way that does not damage the carriers.

Art. 138a. (New - SG 79/20, in force from 08.09.2020) Materials and information recorded on paper, that provide access to the CIS, shall be destroyed by the order of the ordinance under Art. 90 of the CIPA.

Art. 139. (amend. - SG 91/08) On a carrier of art. 138, para 1 shall be prohibited the recording of classified information with level of classification higher than the designated on the carrier.

Art. 140. (1) The level of classification of a carrier under art. 138, para 1, can be lowered only after special deleting of the classified information with level of classification higher than the new level of classification of the carrier.

(2) (Amend. - SG 91/08, amend. - SG 79/20, in force from 08.09.2020) Special deleting of information under para 1 shall be such deleting, upon which is impossible or very difficult the obtaining of residual information, whereby:

1. the methods and means of special deleting must be approved by the security services for the respective or higher level;

2. for information with a level of classification up to "Confidential" inclusive, after coordination with the State Agency "National Security", it shall be admissible to use methods and means approved by the EU and/or NATO for the respective or higher level.

(3) The level of classification of the carrier of art. 138, para 1, can be removed only after special deleting of the entire classified information, recorded on it.

(4) (Amend. - SG 79/20, in force from 08.09.2020) Special deleting of the information shall be done only after a copy of the classified information is ensured, if necessary and not preserved on another carrier.

(5) The lowering or the removal of the level of classification of carrier of art. 138, para 1 with level of classification "Top secret" shall be prohibited.

Art. 141. (1) (Amend. - SG 79/20, in force from 08.09.2020) The destroying of carriers of art. 138, para 1 shall be done:

1. (amend. - SG 79/20, in force from 08.09.2020) after a copy of the classified information is ensured, if it is needed and not preserved on another carrier;

2. after special deleting of the classified information on the carrier, and

3. in a way, not allowing the use of the carrier or parts of it and the extracting of residual information.

(2) (Amend. - SG 79/20, in force from 08.09.2020) In case the reason for destroying is any physical damage of the carrier, due to which the information cannot be deleted, or the carrier is for one-time recording, it shall be destroyed without special deleting being

done.

Art. 142.(1) Special deleting of information or destroying of carriers under art. 138, para 1, shall be implemented by a commission, appointed with an order by the chief of the organisational unit, about which a record shall be made.

(2) The record of para 1 shall be signed by the members of the commission, conceded to the employee for security of information and preserved at the registry.

(3) The record of para 1 shall be ground for bringing out of account of the carriers in the registry also as material means.

Art. 143. All carriers of art. 138, para 1 shall be periodically reconsidered in order to be guaranteed, that no information is preserved with higher level of classification than the designated on the carrier.

Art. 144. Control over the availability of the carriers under art. 138, para 1 in the organisational unit shall be implemented at the checks, implemented by the order of section X of this chapter.

Art. 144a. (New - SG 79/20, in force from 08.09.2020) (1) Cryptographic means and materials for protection of classified information, as well as key materials, shall be marked, stored, accounted for, archived and destroyed under the order of the ordinance under Art. 85 of the CIPA.

(2) The marking, storage and accounting under Para. 1 shall be performed in a cryptographic registry, which is part of the registry of the organizational unit under Art. 51, Para. 1, or in a separate registry established on the grounds of Art. 51, Para. 3.

(3) In the foreign representations, the activities under Para. 1 shall be carried out in the specialized units under Art. 52, Para. 2.

Chapter six.
PERSONAL SECURITY
Section I.
Measures for protection of the classified information in the field of the personal security

Art. 145.(1) The measures for protection of the classified information in the field of the personal security shall guarantee the access to classified information only for persons, which official obligations or concrete assigned tasks impose such access, observing

the principle "Need to know".

(2) The implementing of the measures of para 1 shall be accomplished by investigation for reliability of the persons, issuing of permission for access to the respective level of classification (appendix No 10), termination (access No 12) and refusal (access No 13) for issuing of permission for access, as well as training and implementing of control.

(3) The persons shall have right to access to classified information, being official secret, after their appointment to the respective positions and passing of training in the field of protection of the classified information.

Section II.
Investigation of the persons for reliability

Art. 146. All persons, applying for positions or for concrete assigned tasks, included in the list of art. 37 of the PCIA shall obligatory be investigated for reliability according to art. 41 and 42 of the PCIA.

Art. 147. (1) For implementing of simple investigation under art. 46, item 1 of the PCIA the candidate shall submit:

1. application to the chief of the organisational unit for taking of position or for fulfilment of concrete assigned task, which shall contain the written consent of the person of art. 43, para 2 of the PCIA with attached to it:

a) diploma for graduated education;

b) (repealed - SG 79/20, in force from 08.09.2020)

c) medical certificate under art. 42, para 2 of the PCIA when such is required;

d) (repealed - SG 79/20, in force from 08.09.2020)

e) (amend. – SG 56/06, amend. - SG 79/20, in force from 08.09.2020) a declaration under art. 74, para 2, item 1 of the Tax-insurance Procedure Code or consent of the tax subject for the respective tax body, and

(2) The candidates for taking of position or fulfilment of concrete task shall submit the filled in questionnaire of para 1, item 2 for the employee for the security of information against a receipt;

(3) The employee for the security of information shell be obliged immediately to register the received questionnaire, to require the documents of para 1, item 1 and to start the procedure of investigating of the candidate after the receiving of the written order by the chief of the organisational unit, which shall open a file for investigation, called hereinafter "file for investigation"

Art. 148. (1) The procedures of extended investigation of art. 46 items 2 and 3 of the PCIA shall start after a written requirement (appendix No 14) of the chief of the management unit of art. 51 of the PCIA, where the person applies and has submitted the necessary documents of art. 147, para 1.

(2) The candidate for taking of position or for fulfilment of concrete task shall submit the filled in questionnaire under art. 147, para 1, item 2 to the employee for the security of information of the respective organisational unit against receipt.

(3) The employee for security of information shall be obliged immediately to register the received questionnaire, to require the documents of art. 147, para 1, item 1 and to attach them to the written request for investigation.

(4) (amend. – SG 44/08) The written request for investigation and the documents, attached to it shall be sent to by the employee for security of information To the State Agency "National Security".

(5) (amend. – SG 44/08) The State Agency "National Security" shall immediately start the procedure for investigation after receiving of the written request and the documents, attached to it, for this purpose opening a file for investigating of the person.

Art. 149. (Repealed - SG 79/20, in force from 08.09.2020)

Art. 150.(1) At conducting of competition for taking of position or for fulfilment of concrete task, which require access to classified information, the chief of the organisational unit, conducting the competition, shall make request or issue order for investigation for reliability only to the candidates, meeting the preliminary announced conditions of the competition.

(2) To participation in the competitions shall be admitted the persons, received permission for access.

(3) (new, SG 6/04) In holding a competition for occupying a position by a civil servant, requiring access to classified information, the body of employment shall extend a request or shall order investigation of reliability only of rated applicants.

Art. 151.(1) The files of art. 70 and 71 of the PCIA shall be preserved by the body, who has implemented the investigation.

(2) If there are additional data about then person, different from these collected in the progress of the investigation, the data in the files shall be updated.

Art. 152. The registration of the files for investigation shall be implemented not later than 3 working days after receiving of the written request or of the written order in a register (appendix No 15).

Art. 153.(1) The documents of the files for investigation shall be arranged and systematised by the competent body in two section in the following consequence:

1. section I, containing:

a) description of the documents, which shall be registered in a diary (appendix No 2);

b) list of the employees, being acquainted with the file, and the cause for acquainting;

c) registration form of the file (appendix No 16);

d) materials under art. 71, para 1 of the PCIA;

e) information about implemented checks in the registers of SCSI, the services for security and the services for public order (appendix No 17);

f) information about implemented checks in the information funds;
g) other documents, information and data about the person, and
2. section II, containing:
a) permissions, certificates and confirmations for access to classified information;
b) withdrawn or terminated permissions, certificates and confirmations, the refusals for their issuing or their terminating.
(2) The documents about applied and used intelligence techniques, as well as about applied and used special intelligence means, which are arranged in separate files for the case by the order of their receiving

Art. 154. Taking out and destroying of separate documents or collection of documents, registered in the description of the case shall not be admitted.

Art. 155. At opening of procedure for new investigation under art. 55, para 2 of the PCIA the old case shall be closed and a new case shall be opened for investigation of the person. The old case shall be attached and it shall be part of the new case for investigation.

Art. 156.(1) The cases for investigation for reliability of a person, who has received refusal for issuing of permission for access to classified information, who's such permission has been withdrawn or the effect of who's permission has been terminated, shall be preserved for a term up to 5 years after the refusal, the withdrawal or the termination enters into force.
(2) Upon opening of new procedure for investigation the cases of para 1 shall be attached and become part of the respective new cases for investigation.

Art. 157. (1) (amend. - SG 91/08) In the cases of art. 43, para 4 of the PCIA and upon falling away of the need for access to classified information, the materials and documents, presented by the investigated person, shall be returned by the person to the body, implementing the investigation, against a receipt.
(2) The data, collected in the progress of the investigation, shall be immediately destroyed by a commission, appointed by the body of para 1 and in the way, pointed out in art. 125, about which a record shall be compiled.
(3) The record of para 2 shall be registered in the register of the cases for investigation with a number, corresponding to the number of the case being destroyed.

Section III.
Training of the persons in the field of protection of the classified information

Art. 158. The training in the field of protection of the classified information shall be activity for acquiring of knowledge, skills

and experience for work with classified information.

Art. 159.(1) Before receiving permission for access to classified information the persons shall obligatory pass initial training for protection of the classified information.

(2) The training for protection of classified information shall include:

1. initial studying of the rules for protection of the classified information;

2. current training for increase of the qualification and the experience of the persons with permitted access to classified information.

(3) The persons, passed training, shall sign a declaration (appendix No 18), that they know the rules for protection of classified information and that they will preserve it till the elapse of the terms for its protection of under art. 34 of the PCIA, after which a certificate shall be issued to them (appendix No 19).

(4) The training shall include also acquainting of the person with the risk factors, which could create danger for damaging of the interests of the Republic of Bulgaria.

(5) The rules for training in the services for security and the services for public order shall be determined by the chief of the respective service

(6) In the organisational units a register shall be kept about the carried out training of the persons, admitted to work with classified information (appendix No 20).

Section IV.
Personal security in regime divisions and sites

Art. 160. The chiefs of the organisational units (sections), which divisions and sites are included in the list of appendix No 1 of art. 25 of the PCIA, shall require issuing of permission for access of all persons in the following cases:

1. (amend. – SG 44/08) accepting at regular and military service;

2. occurrence or change of official or employment legal relations;

3. need of access to classified information or change of the level of classification of the information;

4. implementing of activity for the needs of the Ministry of Defence and the Bulgarian army;

5. accepting at training, specialisation, training practice etc. at the organisational units.

Art. 161. (revoked – SG 44/08)

Art. 162.(1) The regime divisions and sites in the armed forces of the Republic of Bulgaria and their level of classification shall be announced with an order by the Minister of Defence.

(2) After the announcement of the order of para 1 SCSI shall be informed.

(3) The chiefs of the organisational units, in which structures there are sites, connected with the defence and the security of the country, shall announce their level of classification in co-ordination with the Minister of Defence and also notify SCSI.

Section V.
Personal security at international visits

Art. 163.(1) (amend. – SG 44/08, amend. – SG 27/16, in force from 05.04.2016) At international visits except visits to the State Intelligence Agency, conformation for access to classified information of foreign individuals shall be issued after written request for visit (appendix No 21) by the chief of the organisational unit, in which the visit will be implemented, to the State Agency "National Security", received not later than 10 working days before the date of the visit.

(2) The request for the visit of para 1 shall contain information about:

1. the purpose of the visit;
2. the working topics, which will contain classified information and the respective level of classification;
3. the site for visit and the working programme;
4. the foreign participants in the visit.

Art. 164. Before accepting the visitors the chief of the organisational unit – subject of the visit, shall check:

1. whether the body of art. 163, para 1 has issued confirmation;
2. is there compliance of the confirmation with the documents for identification of the visitors.

Art. 165. The not issuing of confirmation shall not be ground for refusal of the visit but only for not conceding access to classified information, being state secret.

Section VI.
Control for reliability of the persons, received access to classified information

Art. 166.(1) The control for reliability of the persons, received access to classified information, shall be implemented by the competent bodies through the use of the methods and the means of art. 11, para 4, items 1, 3, 4, 5 and 6 of the PCIA

(2) The control of para 1 shall be implemented from the moment of starting of the procedure for investigation of the person and it shall continue till this is necessary according to the terms for protection of the classified information.

Chapter seven.
INDUSTRIAL SECURITY

Art. 167. The system of principles and measures in the field of the industrial security shall guarantee, that access to classified information – state secret, can have only individuals and corporate bodies, who meet the requirements for security, who are economically stable, reliable from point of view of the security and have received certificate or confirmation for security.

Art. 168.(1) Upon necessity to be concluded contract, which subject contains or imposes access to classified information, being state secret, such contract can be concluded only with persons, to whom are issued certificates or confirmations for security.

(2) The conditions and the order for admitting to the procedures for conducting of negotiations and determining of contractor for concluding and fulfilment of contract shall refer also for all sub-contractors.

Art. 169. The organisational unit – assignor of a contract, shall determine the subject of the task and the level of its classification before the starting of the procedures for conducting negotiations and determining of contractor, for concluding and fulfilment of contract.

Art. 170. (amend. - SG 91/08) (1) The organisational unit – assignor of a contract, shall assign to the competent body of art. 95, para 3 of the PCIA written request for the investigation of the candidates for contractors under the contract before starting of the procedures for conducting of negotiations and determining of contractor unless in case of previously issued valid security certificate.

(2) The validity shall be approved by the body that has issued the security certificate on the basis of a written inquiry by the organisational unit - contractual assignor.

Art. 171. The competent body of art. 95, para 3 of the PCIA shall start procedure for investigation by the order of art. 97 of the PCIA after receiving:

1. written request for investigation of the candidate from the organisational unit – assignor under the contract, or from the organisational unit, creating classified information , being state secret, and

2. (amend. - SG 91/08) written consent (appendix No 22) for implementing of the investigation by the persons, who manage and represent the candidate for contractor.

Art. 172. The written request for investigation, submitted by the organisational unit – assignor under the contract, shall contain:

1. the subject of the task, which fulfilment will be assigned to the candidate;

2. the ground for assigning of the task;

3. the level of classification for security and the amount of the classified information, being state secret, to which the candidate will have access at the stage of negotiations and determining of contractor under the contract;

4. the level of classification for security and the amount of the classified information, being state secret, to which the candidate will have access in the process of fulfilment of the contract;

5. name, BULSTAT, headquarters and address of management, addresses for correspondence of the candidate, for whom the investigation is required.

Art. 173. (1) The persons, who manage and represent the candidate for fulfilment of contract, shall present to the chief of the organisational unit assignor written consent for starting of the investigation, filling in the questionnaires of appendix No 2 of art. 47 and 48 of the PCIA and according to appendix No 23.

(2) The chief of the organisational unit assignor shall direct written request to the body of art. 95, para 3 of the PCIA for investigation of the candidate and attach the filled in questionnaires with the explicit written consent for investigation of the candidate and the documents, required for them

Art. 174. The competent body shall open immediately a case for investigation of the reliability by the way and the order, regulated in art. 152 – 157.

Art. 175.(1) After carrying out the investigation under art. 97 of the PCIA depending on the results the body, implemented the investigation, shall issue or refuse to issue certificate for security.

(2) The certificate for security shall determine the right to access to the explicitly pointed out level of classification of the information.

(3) The certificate for security shall be issued after to all persons of art. 97, para 1 of the PCIA is issued permission for access to classified information, being state secret, according to the requirements of chapter V of the PCIA by the body, implementing the investigation of the candidate of art. 95, para 3 of the PCIA.

(4) Certificate for security shall be issued to Bulgarian corporate bodies or individuals – traders.

(5) In the cases of art. 108, para 3 of the PCIA the certificate for security shall be withdrawn by the body, who have issued it (appendix No 24).

Art. 176.(1) Individuals, who are not traders, can candidate for concluding and fulfilment of contracts under this section if there is permission for access or confirmation.

(2) In the cases of art. 1 the activities for fulfilment of the contract shall be implemented only within the framework of the organisational unit assignor, by order, time and place, determined by it.

(3) The bodies of chapter V of the PCIA shall be competent to conduct the procedure for investigation of the persons of para 1.

Art. 177. (1) (amend. – SG 44/08) Confirmation of the candidates – foreign individuals or corporate bodies (appendix No 25), shall be issued by the State Agency "National Security" if access is necessary to classified information, being state secret. on the basis of issued permission or certificate by the respective competent body of other state or international organisation and after implementing of investigation in the Republic of Bulgaria.

(2) Confirmation shall be issued only to persons, which permissions or certificates are issued by a competent body of a state or international organisation, with which the Republic of Bulgaria has concluded international contract for protection of the classified information.

(3) The provision of para 2 shall be applied also in the cases when the persons, are pointed out by a state or international organisation for implementing of tasks, connected with fulfilment of obligations, ensuing from international agreement, entered into force, to which the Republic of Bulgaria is a party.

Art. 178. To the procedures for determining of contractor and conducting of negotiations for concluding of contracts, connected with access to classified information, being state secret, shall be admitted only persons, having permission for access and/or certificate for security or confirmation.

Art. 179. The data, contained in the files, being official secret, if not subject to higher level of classification for security, shall be used for the purposes of the PCIA.

Art. 180.(1) The files for investigation shall be preserved for a term according to art. 110, para 3 of the PCIA.

(2) If the files for investigation for reliability contain documents with grading of secrecy, requiring longer term for protection of the classified information than the term of para 1, the files shall be preserved according to the longest of the terms for these documents.

(3) After the expiry of the terms of para 1 or 2 the chief of the body, implemented the investigation, shall appoint a commission, which after reviewing of the documents in the file, shall propose its destroying, submitting to archive or continuing of the preservation.

Art. 181.(1) Unless an international agreement, entered into force, to which the Republic of Bulgaria is a party, provides other, international visits in organisational units – contractors of contracts, connected with access to classified information – state secret, can be implemented after:

1. submitting of written request for visit within the term and according to the model of art. 163;
2. grounded opinion by the organisational unit to SCSI about the need of making the visit;

3. grounded opinion to SCSI by the body, issued the certificate for security of the organisational unit;

4. permission for visit, issued by SCSI.

(2) When the visit is not connected with access to classified information, the chief of the organisational unit can permit visit only in the zones, where no activities are done, connected the fulfilment of contract, referring to access to classified information. In these cases the chief of the organisational unit shall notify in writing SCSI through then body, issued the certificate for security, attaching also the requests for visit.

(3) The request for visit of para 1 shall be submitted to the organisational unit – site or organiser of the visit. The employee for security of information in the organisational unit shall send the request for visit to SCSI through the body, issued the certificate for security.

(4) Request for visit and notification shall be submitted for each separate visit

Art. 182.(1) Carrying of materials – carriers of classified information in connection with fulfilment of contract, providing access to classified information, can be implemented by the conditions the order of chapter five, section V and by special couriers, certified by SCSI

(2) (amend. SG 22/03) The carrying of para 1 shall be implemented observing the following requirements for security:

1. guaranteeing of the security of the consignment at all stages of its carrying till reaching of its final destination;

2. compliance of the level of protection of the whole consignment with the highest level of classification of the information in the consignment;

3. supplying of the consignment along the shortest and the safest route from point of view of security and in the fastest possible way, as far as the circumstances allow this.

Art. 182a. (new – SG 22/03) The special courier shall be a person of art. 81, para 1, item 2, who is an employee in the organisational unit – party in the contract of art. 95, para 1 of the PCIA, and:

1. has permission for access to the respective level of classification for security of the information;

2. has passed the training of art. 89 and has passed the examination;

3. has received special official card of art. 90;

4. has received certificate, issued by SCSI.

(2) The certificate of para 1, item 4 shall be issued to the special courier for each separate carrying of materials, containing classified information, and it shall be subject to returning after submitting them.

(3) In case at carrying occur circumstances, connected with the requirements for security of art. 182, para 2, the courier shall note them on the certificate before returning it.

Art. 182b. (new – SG 22/03) Before implementing of concrete carrying of materials, containing classified information, the

special courier shall be instructed about the respective requirements for security and sign a declaration, which is preserved by the employee for security at the organisational unit for a term not less than 12 months after implementing of the carrying of the materials.

Art. 182c. (new – SG 22/03) (1) In the cases of art. 87, para 1 materials, containing classified information, shall be carried by using a carrier.

(2) Before implementing of the carrying of para 1 the supplier and the recipient shall prepare and approve a transport plan.

(3) The transport plan of para 2 shall be prepared by the party in the contract, which sends the material, containing classified information, and shall be accepted by the recipient.

Art. 182d. (new – SG 22/03) The transport plan shall contain:

1. description of the consignment;
2. description of the separate materials and description of the levels of their classification;
3. the person, determined under art. 105 of the PCIA, who implements control over observing of the provisions of the law and the acts for its implementation and consults the contractor at fulfilment of the contract;
4. the person, who is in charge for the implementation of the measures for protection of the classified information at the fulfilment of the contract and render co-operation to the person of item 3;
5. the place for supply and the way of submitting;
6. security measures;
7. places for preservation, processing and submitting;
8. route, including the initial point and the final destination;
9. detailed description of the movement of the consignment;
10. the couriers and the carriers, as well as other elements depending on the specifics of the transported material and the route.

Art. 182e. (new – SG 22/03) (1) When the carrying of materials. containing classified information, imposes the using of a carrier, he must meet the following minimum requirements:

1. to be registered as trader according to his national legislation;
2. to have issued certificate for security for the respective level of classification for security of information, and
3. to dispose with due document for implementing of activity as carrier according to his national legislation.

(2) The specific requirements to the carrier shall be determined in the contract for carriage according to the kind of the transport.

Art. 183. At implementing of the authorities under this chapter and if necessary the competent bodies can make international

visits in foreign organisational units.

Additional provisions

§ 1. In the context of these Rules:

1. "Management of data" is activity, connected with the work with information funds, and it includes collecting, recording, organising, storage, adapting or changing, updating, use, combining, temporary stopping of the processing, conceding (entirely or partially) or ensuring of other opportunities for conceding access, preservation, deleting or destroying of the data.

2. "National system for protection of classified information" is a complex of competent bodies and measures for implementing of specific information, analytical and control activities, which give opportunity for uniting of the information from the organisational units in a way, allowing making of assessments and prognoses of the quality of protection of the classified information on the territory of the country and abroad, in explicitly determined cases with objective assessment of the updated status of the quality of the system for protection of the classified information, assessment and prognosis of the risk. timely identification of the negative processes, connected with the threat for classified information or its damaging, prognosis of their development, prevention of the harmful processes and determining the degree of effectiveness of the implemented measures for protection of the classified information.

3. "Marking in the information funds and systems" is putting of code word or another expression or other kind order for collecting of data, the physical carrier being determined depending on the kind of the information fund or system, allowing collecting of data with subject or object characteristic or with regard to certain activity.

4. "Irretrievably lost material" is a physical carrier of classified information, which cannot be restored due to its nature or cannot be found due to reasons, connected with unregulated access, insurmountable force or other unpredictable circumstances, which has lead to destroying of the classified information or have made it not secret through unregulated access or about which can be made grounded assumption, that it has been destroyed or that it cannot be used in whatever way.

5. (new - SG 79/20, in force from 08.09.2020) "Physical carrier for multiple recording" shall mean a medium that allows multiple recordings or additions to information already recorded on a medium (e.g. magnetic media, optical media, magneto-optical media, memory cards, tape media, etc.).

6. (new - SG 79/20, in force from 08.09.2020) "Critical situation" shall be a situation, occurred as a result of any sudden and unforeseen event which may lead or has led to unregulated access to classified information.

Transitional and concluding provisions

§ 2. The contracts in the field of the industrial security, concluded before the PCIA enters into force, which fulfilment is connected with access to classified information, shall preserve their effect. The chief of the organisational unit – assignor of the

contract, or the persons, who manage and represent the contractor, shall be obliged in 6 months term after the Rules enters into force to require issuing of certificates or confirmations for security.

§ 3.(1) After opening of the registries of art. 54 the organisational units shall register and account the materials, containing classified information under the conditions and by the order of chapter five, section IV, with which shall be terminated the previous order for registering and accounting of secret documents and materials.

(2) The materials with grading for secrecy, registering and accounting by the previous order, shall be brought in compliance with the requirements of the PCIA under the conditions and by the order of § 9, para 2 of the transitional and concluding provisions of the same Act.

§ 4. In 3 months term after the Rules enters into force the chiefs of the organisational units shall undertake the necessary activities for bringing the existing normative provisions in compliance with the PCIA and with the Rules.

§ 5. (amend. - SG 5/10) The fulfilment of the Rules shall be assigned to SCSI, to the Minister of Interior, the Minister of Defence, the Minister of Foreign Affairs and to the chiefs of services for security and the services for public order as well as to the chiefs of the organisational units of art. 20, para 1 in connection with § 1, item 3 of the additional provisions of the PCIA.

§ 6.The Rules shall be issued pursuant to § 3 of the transitional and concluding provisions of the PCIA.

Transitional and concluding provisions

TO DECREE NO 246 OF 10 OCTOBER 2007 CONCERNING ADOPTION OF STRUCTURAL REGULATION OF STATE AGENCY "ARCHIVES", APPROVAL OF TARIFF FOR THE TAXES, COLLECTED BY OF STATE AGENCY "ARCHIVES" AND FOR DETERMINATION OF PRICES OF THE SERVICES, PROVIDED BY STATE AGENCY "ARCHIVES"

(PROM. – SG 84/07, IN FORCE FROM 19.10.2007)

§ 23. The Decree shall enter into force from the date of its promulgation in the State Gazette.

Concluding provisions
TO DECREE № 66 of March 28, 2016, ON THE ADOPTION OF RULES ON IMPLEMENTATION OF THE STATE INTELLIGENCE AGENCY ACT

(PROM. - SG 27/16, IN FORCE FROM 05.04.2016)

§ 6. In the Rules on Implementation Of The Protection Of Classified Information Act, adopted by Decree № 276 of the Council of Ministers of 2002 (prom. SG 115 of 2002; amend. and suppl., SG 22 of 2003, SG 6 of 2004, SG 56 of 2006, SG 84 of 2007, SG 44 and 91 of 2008, SG 7 of 2009, SG 5 of 2010), everywhere the words "National intelligence service" shall be replaced by State Intelligence Agency.

.....

§ 17. The Decree shall enter into force on the day of its promulgation in the State Gazette.

Concluding provisions

TO DECREE № 205 OF AUGUST 11, 2016, ON SUPPLEMENTING THE RULES ON IMPLEMENTATION OF THE PROTECTION OF CLASSIFIED INFORMATION ACT, ADOPTED BY DECREE № 276 OF THE COUNCIL OF MINISTERS IN 2002

(PROM. - SG 64/16, IN FORCE FROM 16.08.2016)

§ 2. The Decree shall enter into force on the day of its promulgation in the State Gazette.

Transitional and concluding provisions

TO DECREE № 251 OF 4 SEPTEMBER 2020 AMENDING AND SUPPLEMENTING THE RULES FOR THE IMPLEMENTATION OF THE PROTECTION OF CLASSIFIED INFORMATION ACT, ADOPTED BY DECREE № 26 OF THE COUNCIL OF MINISTERS IN 2002

(PROM. - SG 79/20, IN FORCE FROM 08.09.2020)

§ 52. The Decree shall enter into force on the day of its promulgation in the State Gazette.