MONITORUL OFICIAL AL ROMÂNIEI

Anul XIV — Nr. 315

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ȘI ALTE ACTE

Luni, 13 mai 2002

SUMAR

HOTĂRÂRI ALE GUVERNULUI ROMÂNIEI

GUVERNUL ROMÂNIEI

HOTĂRÂRE
pentru aprobarea Normelor privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România

În temeiul prevederilor art. 107 din Constituția României,

Guvernul României adoptă prezenta hotărâre.

Art. 1. — Se aprobă Normele privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România, prevăzute în anexa care face parte integrantă din prezenta hotărâre.

Art. 2. — În termen de 60 de zile de la intrarea în vigoare a prezentei hotărâri instituțiile care utilizează informații clasificate ale Organizației Tratatului Atlanticului de Nord au obligația de a elabora dispoziții interne pentru aplicarea normelor prevăzute la art. 1.

PRIM-MINISTRU
ADRIAN NĂSTASE

Contrasemnează:
p. Ministrul afacerilor externe,
Mihnea Motoc,
secretar de stat
p. Ministrul apărării naționale,
Sorin Encuțescu,
secretar de stat
Directorul Serviciului Român de Informații,
Radu-Alexandru Timofte
p. Directorul Serviciului de Informații Externe,
Alexandru Marcel

București, 15 aprilie 2002.
Nr. 353.

ANEXĂ

NORME
privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România

A. PRINCIPII GENERALE

1. În calitate de candidată la aderare și țară parteneră la Consiliul de Cooperare Nord-Atlantic (Parteneriatul pentru pace), România a semnat la data de 8 iulie 1994 Acordul de securitate cu Organizația Tratatului Atlanticului de Nord, denumită în continuare *NATO*, iar la data de 10 septembrie 1994 Codul de conduită.

2. Prin semnarea documentelor menționate mai sus România și-a luat angajamente clare de a proteja și apăra informațiile și materialele clasificate ale Alianței Nord-Atlantice și membrilor acesteia, în conformitate cu documentul „Securitatea în cadrul NATO—C-M (55) 15 (Final)“ și cu actele normative naționale.

3. În baza obligațiilor bine definite ce revin României prin Hotărârea Guvernului nr. 864 din 10 octombrie 2000 a fost înființată Autoritatea Națională de Securitate, denumită în continuare *ANS*, instituție învestită cu atribuții de reglementare, autorizare și control în conformitate cu standardele minime privind protecția informațiilor clasificate ale NATO.

4. ANS reprezintă organismul național de legătură cu Oficiul de Securitate NATO, denumit în continuare *NOS,* și cu celelalte structuri de securitate ale Alianței Nord-Atlantice și asigură aplicarea și coordonarea unitară a activității de protecție a informațiilor clasificate NATO pe teritoriul României.

5. Domeniile principale în care ANS își exercită atribuțiile sunt securitatea fizică, securitatea personalului, securitatea documentelor, protecția informațiilor stocate în cadrul sistemelor de prelucrare automată a datelor, denumită în continuare *INFOSEC,* securitatea industrială, precum și alte domenii care implică protecția informațiilor clasificate ale NATO, pentru care elaborează instrucțiuni și proceduri interne, cu respectarea strictă a prevederilor legale din România și a standardelor NATO.

6. Pentru îndeplinirea atribuțiilor în domeniul protecției informațiilor clasificate ale NATO au competențe următoarele instituții: Serviciul Român de Informații, Serviciul de Informații Externe, Ministerul Apărării Naționale — Direcția generală de informații a apărării și Ministerul Afacerilor Externe. De asemenea, îndeplinesc atribuții specifice, conform competențelor legale, și Serviciul de Telecomunicații Speciale, Ministerul de Interne și Serviciul de Protecție și Pază.

B. DEFINIȚII

7. *Informație* semnifică acea noțiune care poate fi comunicată în orice formă.

8. *Informație clasificată* semnifică acea informație sau material care necesită protecție împotriva dezvăluirii neautorizate, atribuindu-i-se în acest scop o clasificare de securitate.

9. *Material* include documente și orice elemente ale unui echipament, mecanism sau armament prelucrat ori în curs de prelucrare.

10. *Informații clasificate NATO* se referă la toate informațiile clasificate de natură politică, militară și economică, vehiculate în cadrul NATO, elaborate în cadrul structurilor NATO sau primite de la statele membre ori de la alte organizații internaționale.

11. *Document* semnifică toate tipurile de medii de stocare a informațiilor, cum ar fi: documentele pe suport hârtie (documentele tipărite, copii, traduceri, schițe, hărți, planșe, fotografii, desene, note, hârtii de indigo, listinguri etc.), mediile de stocare ale calculatoarelor (suporturi optice, benzi magnetice, casete, dischete, hard-discuri, memorii PROM și EPROM etc.), microfilme, riboane de printare, dispozitivele de procesare portabile (agende electronice, laptop) la care hard-discul este folosit pentru stocarea informațiilor clasificate NATO.

12. *Document clasificat NATO* semnifică acel document care conține informații clasificate NATO.

13. *Securitatea documentelor clasificate NATO* reprezintă ansamblul procedurilor, instrucțiunilor și măsurilor privind gestionarea și controlul documentelor clasificate NATO.

14. *Gestionarea informațiilor clasificate NATO* reprezintă totalitatea activităților de primire, de evidență a elaborării și consultării, verificare, evidență, distribuție, transmitere, transport, multiplicare, distrugere, inventariere și arhivare a informațiilor clasificate NATO.

15. *Controlul informațiilor clasificate NATO* reprezintă totalitatea activităților de verificare a modului în care sunt gestionate documentele clasificate NATO.

C. ACCESUL LA INFORMAȚIILE CLASIFICATE NATO

16. Accesul la informațiile clasificate NATO se acordă în baza certificatului de securitate eliberat de ANS și a respectării principiului nevoii de a ști (need-to-know).

17. Conform Hotărârii Guvernului nr. 864/2000, ANS eliberează certificate de securitate, documente în baza cărora

se acordă accesul la informații și la documente clasificate NATO.

18. Acestea sunt de două tipuri:

— certificat de securitate tip A, cu o valabilitate de 3 ani, care permite accesul la informații și documente clasificate NATO;

— certificat de securitate tip B, care autorizează participarea persoanei la activități organizate de Alianța Nord-Atlantică în cadrul cărora se vehiculează informații clasificate NATO și pentru care Alianța Nord-Atlantică solicită astfel de documente. Acest tip de certificat este valabil doar pe durata desfășurării activității respective. Certificatele de securitate tip B nu se eliberează în absența certificatelor de securitate tip A.

19. Nivelul de acces acordat prin certificatul de securitate eliberat trebuie să fie similar cu nivelul de clasificare a informațiilor la care persoana necesită acces în îndeplinirea sarcinilor sale de serviciu.

20. Accesul la informații clasificate NATO pe baza certificatului de securitate trebuie să respecte principiul nevoia de a ști (need-to-know), care are următorul înțeles: nici o persoană nu este îndreptățită doar prin rang, funcție sau certificat de securitate să aibă acces la informații clasificate NATO. Numărul persoanelor care au acces la informații și documente clasificate NATO trebuie restrâns la cele ale căror activitate și îndatoriri profesionale impun lucrul cu astfel de informații.

21. Persoanele cărora le-au fost eliberate certificate de securitate și urmează să li se acorde accesul la informații clasificate NATO vor fi instruite de către funcționarul de securitate al instituției cu privire la reglementările și normele de protecție a acestora. Acestea se vor angaja, sub semnătură, să asigure securitatea informațiilor clasificate NATO și să respecte prevederile reglementărilor specifice pe linia protecției informațiilor clasificate/planurilor de securitate în îndeplinirea atribuțiilor de serviciu.

D. SISTEMUL NAȚIONAL DE REGISTRE

22. *Structura instituțională* se referă la ministere, organisme centrale, instituții, autorități, agenții, agenți economici etc, în care sunt sau vor fi utilizate informații clasificate NATO.

23. *Componentă a sistemului național de registre (CSNR)* se referă la acea componentă din cadrul unei structuri instituționale, responsabilă cu gestionarea și consultarea informațiilor clasificate NATO. Acestea sunt: Registrul Central, registrele externe, registrele interne, subregistrele și punctele de lucru.

24. *Sistemul național de registre* reprezintă ansamblul tuturor CSNR.

25. În cadrul sistemului național de registre sunt aplicate unitar reglementările privind securitatea fizică, securitatea personalului, securitatea documentelor, securitatea industrială și INFOSEC pentru a se asigura cadrul adecvat gestionării informațiilor clasificate NATO în conformitate cu standardele NATO de securitate.

26. Fiecare structură instituțională (militară sau civilă) care utilizează informații clasificate NATO are obligația să își înființeze propria CSNR, forma de organizare a acesteia depinzând de volumul și de nivelul de clasificare a informațiilor vehiculate, în concordanță cu structura administrativă existentă.

27. *Registrul Central* reprezintă CSNR care este constituită și funcționează în cadrul ANS și răspunde, la nivel național, de gestionarea și controlul tuturor informațiilor clasificate NATO.

28. *Registrul extern* reprezintă CSNR aflată în exteriorul țării, subordonată Registrului Central, care gestionează informațiile clasificate NATO primite/transmise de la/la NATO și de la/la celelalte structuri de securitate ale Alianței Nord-Atlantice.

29. *Registrul intern* reprezintă CSNR care gestionează și controlează, la nivelul unei structuri instituționale, informațiile clasificate NATO.

30. *Subregistrul* reprezintă CSNR subordonată unui registru intern și care gestionează și controlează, la nivel departamental, informațiile clasificate NATO.

31. *Punctul de lucru* reprezintă CSNR care are doar atribuții de evidență, consultare, distribuție, păstrare și control al informațiilor clasificate NATO.

32. Modul de organizare a unei CSNR este determinat în principal de volumul informațiilor clasificate NATO pe care le gestionează și de nivelul de clasificare a informațiilor vehiculate, precum și de atribuțiile funcționale pe care trebuie să le îndeplinească. O CSNR se compune din:

A. Secțiunea de documente care, la rândul ei, se compune din:

- componenta de evidență;
- componenta de distribuție.

B. Secțiunea de curierat

33. Secțiunea de documente are următoarele atribuții principale:

— primirea, evidența elaborării și consultării, verificarea, evidența, transmiterea, transportul, multiplicarea, distrugerea, inventarierea, arhivarea și controlul informațiilor clasificate NATO;

— distribuția — colectarea, verificarea, ambalarea, predarea/primirea la/de la secțiunea de curierat.

34. Secțiunea de curierat are următoarele atribuții principale:

— colectarea, verificarea și transportul documentelor clasificate NATO, în conformitate cu reglementările naționale

privitoare la transportul documentelor naționale cu nivel de clasificare echivalent și cu respectarea standardelor minime de securitate NATO.

35. Fiecare CSNR trebuie să își organizeze Secțiunea de documente. Secțiunea de curierat poate fi inclusă/asigurată de structura instituțională de care aparține.

36. Atribuțiile Registrului Central se referă la:

a) coordonarea activității tuturor structurilor CSNR din subordine;

b) aplicarea metodologiilor specifice elaborate de către ANS în cadrul structurii proprii, transmiterea acestora CSNR subordonate și urmărirea modului în care sunt aplicate;

c) gestionarea informațiilor clasificate NATO;

d) asigurarea organizării și funcționării arhivei cu informații clasificate NATO, la nivel național;

e) efectuarea inventarierii anuale a tuturor documentelor proprii și centralizarea rezultatelor inventarierii la toate CSNR din cadrul Sistemului național de registre;

f) gestionarea originalelor tuturor certificatelor de securitate tip A eliberate de ANS;

g) evidența tuturor CSNR aflate în subordine;

h) controlul periodic privind gestionarea informațiilor clasificate NATO în cadrul CSNR din subordine;

i) pregătirea și instruirea personalului propriu.

37. Atribuțiile registrelor externe se referă la:

a) aplicarea metodologiilor specifice, elaborate de către ANS în cadrul structurii proprii, transmiterea acestora CSNR subordonate și urmărirea modului în care sunt aplicate;

b) primirea/transmiterea documentelor clasificate de la/la NATO sau de la/la alte structuri de securitate ale Alianței Nord-Atlantice;

c) gestionarea informațiilor clasificate NATO primite/transmise de la/la Registrul Central;

d) asigurarea organizării și funcționării arhivei proprii cu informații clasificate NATO;

e) efectuarea inventarierii anuale a tuturor documentelor proprii și centralizarea rezultatelor inventarierii la toate CSNR din subordine;

f) gestionarea originalelor certificatelor de securitate tip B ale persoanelor care își desfășoară activitatea în cadrul propriei structuri;

g) evidența tuturor CSNR din subordine;

h) controlul periodic privind informațiile clasificate NATO în cadrul CSNR din subordine și centralizarea rezultatelor;

i) pregătirea și instruirea personalului propriu;

j) sprijinirea activităților organizate de NATO pe linia protecției informațiilor clasificate;

k) transmiterea la NOS a materialelor specifice pe linia protecției informațiilor clasificate NATO, elaborate de ANS.

38. Atribuțiile registrelor interne se referă la:

a) coordonarea activității tuturor CSNR din subordine, subregistrelor sau punctelor de lucru;

b) aplicarea metodologiilor specifice elaborate de către ANS în cadrul structurii proprii, transmiterea acestora CSNR subordonate și urmărirea modului în care sunt aplicate;

c) gestionarea informațiilor clasificate NATO și asigurarea fluxului informațional de la/la CSNR subordonate, precum și transmiterea către Registrul Central a documentelor naționale;

d) asigurarea organizării și funcționării arhivei cu informații clasificate NATO la nivelul structurii instituționale din care face parte;

e) efectuarea inventarierii anuale a tuturor documentelor proprii și centralizarea rezultatelor inventarierii la toate CSNR din subordine;

f) gestionarea tuturor originalelor certificatelor de securitate (tip A și tip B) eliberate de ANS pentru personalul din structura sa proprie și păstrarea listei actualizate cuprinzând toate persoanele din cadrul tuturor CSNR din subordine, care au acces la informații clasificate NATO;

g) evidența tuturor CSNR aflate în subordine;

h) controlul periodic privind gestionarea informațiilor clasificate NATO în cadrul CSNR din subordine;

i) pregătirea și instruirea personalului propriu și a subregistrelor/punctelor de lucru subordonate.

39. Atribuțiile subregistrelor se referă la:

a) coordonarea activității tuturor CSNR din subordine (puncte de lucru);

b) aplicarea metodologiilor specifice elaborate de către ANS în cadrul structurii proprii;

c) gestionarea informațiilor clasificate NATO și asigurarea fluxului informațional de la/la CSNR subordonate, precum și transmiterea către Registrul intern a documentelor naționale;

d) asigurarea organizării și funcționării arhivei proprii cu informații clasificate NATO;

e) efectuarea inventarierii anuale a tuturor documentelor proprii și centralizarea rezultatelor inventarierii la toate CSNR din subordine;

f) gestionarea originalelor certificatelor de securitate (tip A și tip B) eliberate de ANS pentru personalul din competență;

g) evidența tuturor CSNR din subordine;

h) controlul periodic privind gestionarea informațiilor clasificate NATO în cadrul CSNR din subordine;

i) pregătirea și instruirea personalului propriu și al punctelor de lucru subordonate.

40. Atribuțiile punctelor de lucru se referă la:

a) aplicarea metodologiilor specifice elaborate de către ANS și transmise prin intermediul CSNR căreia îi este subordonat;

b) gestionarea tuturor originalelor certificatelor de securitate (tip A și tip B) eliberate de ANS;

c) asigurarea organizării și funcționării arhivei proprii cu informații clasificate NATO;

d) efectuarea inventarierii anuale a tuturor documentelor proprii;

e) asigurarea evidenței, consultării, distribuției, controlului și păstrării informațiilor clasificate NATO, precum și transmiterea către CSNR imediat superioară a documentelor naționale.

41. Gestionarea informațiilor clasificate NATO se efectuează exclusiv în cadrul Sistemului național de registre.

42. Documentele primite de către Registrul extern de la NATO, SHAPE sau de la alte structuri de securitate ale Alianței Nord-Atlantice sunt gestionate conform procedurilor elaborate de ANS și sunt transmise la Registrul Central care constituie unicul canal de transmitere a informațiilor clasificate NATO de la/la NATO.

43. Registrul central va transmite/primi informațiile clasificate NATO la/de la CSNR direct subordonate, în conformitate cu procedurile existente, iar acestea la rândul lor le vor transmite/primi la/de la CSNR din subordinea lor directă, cu respectarea acelorași proceduri.

44. Registrul Central, în conformitate cu procedurile existente, va transmite la NATO, prin intermediul Registrului extern, toate documentele primite.

45. Fiecare structură instituțională care în desfășurarea activității sale gestionează sau urmează să gestioneze informații clasificate NATO trebuie să își înființeze o CSNR proprie.

46. Înființarea unei CSNR se realizează printr-o procedură unică ce se finalizează prin eliberarea unei autorizații de înființare și funcționare, document eliberat de către ANS, care certifică faptul că sunt îndeplinite standardele de securitate privind protecția informațiilor clasificate NATO.

47. ANS, prin Registrul Central, păstrează evidența tuturor CSNR, precum și evidența tuturor documentelor referitoare la înființarea/transformarea/desființarea acestora și are obligația de a efectua controlul periodic asupra modului în care sunt îndeplinite condițiile de securitate.

48. Fiecare structură instituțională va păstra la rândul său evidența la zi asupra tuturor înființărilor/transformărilor/desființărilor CSNR din sfera lor de competență.

49. ANS are obligația de a prezenta Oficiului de Securitate NATO, cu ocazia controalelor anuale efectuate, situația la zi a tuturor CSNR care există la nivel național și de a informa ori de câte ori este necesar instituțiile naționale cu atribuții în materie de protecție a informațiilor clasificate asupra modului în care se desfășoară activitatea în acest domeniu.

50. În situațiile în care atribuțiile unei CSNR se modifică în sensul extinderii/diminuării activității sale se impune transformarea acesteia.

51. Transformarea unei CSNR se efectuează la solicitarea instituției, cu aprobarea ANS, și se materializează prin eliberarea unei noi autorizații de înființare și funcționare.

52. Desființarea unei CSNR are loc atunci când nu se mai justifică funcționarea acesteia și se face la solicitarea în scris a respectivei instituții.

53. ANS va analiza solicitarea și va aproba desființarea respectivei CSNR.

54. O dată pe an și ori de câte ori este necesar ANS are obligația să efectueze controlul la Registrul Central, care se desfășoară conform unei grile de control și se finalizează cu un raport de control.

55. Echipa care efectuează controlul va fi alcătuită din persoane desemnate de Consiliul de coordonare al ANS.

56. Raportul de control va fi analizat de Consiliul de coordonare al ANS, iar concluziile desprinse vor fi consemnate în decizia acestuia. Consiliul de coordonare al ANS va stabili măsurile necesare a fi întreprinse și termene precise pentru rezolvarea problemelor apărute ca urmare a controlului.

57. În cazul apariției unor evenimente deosebite conducerea ANS are obligația să informeze operativ NOS, iar pe plan național, instituțiile abilitate pe linia protecției informațiilor clasificate și să prezinte măsurile întreprinse pentru reglementarea situației.

58. O dată pe an și ori de câte ori este necesar ANS, prin intermediul Registrului Central, are obligația să verifice registrele interne/externe și să întocmească raportul de control care va fi prezentat conducerii ANS.

59. Echipa care efectuează controlul va fi alcătuită din persoane desemnate de Consiliul de coordonare al ANS.

60. Raportul de control va fi elaborat în termen de 7 zile de la data efectuării controlului.

61. Concluziile și recomandările cuprinse în raportul de control vor fi prezentate spre analiză și aprobare Consiliului de coordonare al ANS, care va decide asupra celor constatate. Secretariatul tehnic al ANS va informa în termen de 7 zile conducerea instituției respective asupra rezultatelor controlului și va prezenta recomandările Consiliului de coordonare al ANS, împreună cu măsurile care se consideră că trebuie întreprinse pentru reglementarea situației.

62. Raportul de control împreună cu măsurile/recomandările consemnate vor fi păstrate la Registrul Central,

constituind documente de evidență, o copie de pe acestea fiind trimisă și la registrul respectiv.

63. În cazul apariției unor evenimente deosebite conducerea ANS are obligația să informeze operativ NOS, iar pe plan național, instituțiile abilitate pe linia protecției informațiilor clasificate și să prezinte măsurile întreprinse pentru reglementarea situației.

64. O dată pe an și ori de câte ori este necesar structurile instituționale care dețin subregistre, prin intermediul registrelor interne, au obligația să verifice toate subregistrele din subordine și să întocmească raportul de control.

65. Echipa care efectuează controlul va fi alcătuită din persoane desemnate de conducerea instituției din cadrul Registrului intern în a cărui subordine directă se află.

66. Concluziile și recomandările cuprinse în raportul de control vor fi analizate și aprobate de conducerea Registrului intern. Rezultatul controlului împreună cu măsurile întreprinse vor fi transmise conducerii instituției, în termen de 7 zile de la data efectuării controlului.

67. Raportul de control împreună cu măsurile/recomandările consemnate vor fi păstrate la CSNR care are în subordine respectivul subregistru, constituind documente de evidență, o copie de pe acestea fiind trimisă și la subregistrul care a fost controlat.

68. În cazul apariției unor evenimente deosebite conducerea ANS are obligația să informeze operativ NOS, iar pe plan național, instituțiile abilitate pe linia protecției informațiilor clasificate și să prezinte măsurile întreprinse pentru reglementarea situației.

69. O dată pe an și ori de câte ori este necesar CSNR care are în subordine respectivul punct de lucru are obligația să îl controleze și să întocmească raportul de control.

70. Echipa care efectuează controlul va fi alcătuită din persoane desemnate de conducerea CSNR căreia i se subordonează direct respectivul punct de lucru.

71. Concluziile și recomandările cuprinse în raportul de control vor fi analizate și aprobate de conducerea CSNR. Rezultatul controlului împreună cu măsurile întreprinse vor fi transmise conducerii instituției în termen de 7 zile de la data efectuării controlului.

72. Raportul de control împreună cu măsurile/recomandările consemnate vor fi păstrate la CSNR căreia i se subordonează respectivul punct de lucru, constituind documente de evidență, o copie de pe acestea fiind trimisă și la punctul de lucru care a fost controlat.

73. În cazul apariției unor evenimente deosebite conducerea ANS are obligația să informeze operativ NOS, iar pe plan național, instituțiile abilitate pe linia protecției informațiilor clasificate și să prezinte măsurile întreprinse pentru reglementarea situației.

E. SECURITATEA FIZICĂ

74. *Securitatea fizică* reprezintă ansamblul reglementărilor, normelor și măsurilor care au drept scop prevenirea accesului neautorizat la informații clasificate NATO, precum și a oricăror situații, împrejurări sau fapte de natură să pericliteze ori să compromită securitatea și integritatea acestora.

75. ANS răspunde de stabilirea reglementărilor specifice în domeniu, precum și de elaborarea măsurilor de protecție a obiectivului propriu, asigurând aplicarea corectă a acestora.

76. Conducătorii instituțiilor asigură punerea în aplicare și respectarea măsurilor de protecție fizică a informațiilor clasificate NATO prin desemnarea unei structuri/unui funcționar de securitate.

77. Nivelurile de protecție fizică se stabilesc în funcție de următorii parametri:

a) nivelul de clasificare a informațiilor;

b) volumul și suportul fizic de prezentare a informațiilor clasificate NATO;

c) nivelul de acces conferit de certificatul de securitate, cu aplicarea principiului nevoii de a ști (need-to-know);

d) situația din zona de localizare a obiectivului.

78. Termenul *obiectiv* definește totalitatea zonelor de securitate în care sunt gestionate informații clasificate NATO.

79. Zonele de securitate sunt împărțite în 3 clase definite, organizate și administrate conform următoarelor criterii:

a) Zona de securitate clasa I presupune că orice persoană aflată în interiorul acesteia are acces la informații clasificate NATO. În această zonă se pot gestiona informații clasificate NATO până la nivelul SECRET. O asemenea zonă necesită:

1. perimetru clar definit și protejat, în care toate intrările și ieșirile sunt supravegheate;

2. controlul sistemului de intrare, care să permită numai accesul persoanelor verificate corespunzător și autorizate în mod special;

3. indicarea clasei și a nivelului de securitate a informațiilor existente.

b) Zona de securitate clasa II presupune gestionarea informațiilor clasificate NATO prin aplicarea unor măsuri specifice de protecție a acestora împotriva accesului persoanelor neautorizate. În această zonă se pot gestiona informații clasificate NATO până la nivelul CONFIDENTIAL. O asemenea zonă necesită:

1. perimetru clar definit și protejat, în care toate intrările și ieșirile sunt supravegheate;

2. controlul sistemului de intrare, pentru a permite accesul numai persoanelor verificate și autorizate să pătrundă

în această zonă. Pentru toate celelalte persoane trebuie să existe reguli de însoțire, supraveghere și prevenire a accesului neautorizat în această zonă.

c) Zona administrativă. În jurul zonelor de securitate clasa I sau clasa II poate fi stabilită o zonă administrativă cu perimetru vizibil definit, în interiorul căreia să existe posibilitatea de control al personalului și vehiculelor. În zona administrativă sunt gestionate numai informații NATO/RESTRICTED.

80. Incintele în care nu se lucrează zilnic 24 de ore vor fi inspectate imediat după orele de program pentru a verifica dacă informațiile clasificate NATO sunt protejate corespunzător.

81. Intrările în zonele de securitate clasa I și clasa II vor fi controlate prin permis de intrare sau printr-un sistem de recunoaștere personală aplicat personalului permanent. De asemenea, trebuie instituit un sistem de control al vizitatorilor în vederea interzicerii accesului neautorizat la informații clasificate NATO.

82. Permisul de intrare nu va specifica în clar identitatea organizației emitente sau locul în care deținătorul are acces. Controlul intrărilor și ieșirilor poate fi completat de un sistem automatizat de identificare, care nu se substituie sistemului de pază și apărare.

83. Inopinat sau la ordin, la intrarea sau la ieșirea din zonele de securitate clasa I sau clasa II, va fi efectuat controlul bagajelor (incluzând colete, genți și alte containere în care s-ar putea transporta informații și materiale clasificate NATO).

84. Personalul care asigură sistemul de pază și apărare pentru zonele de securitate și informațiile clasificate NATO, gestionate în interiorul obiectivului, trebuie să dețină certificat de securitate și să fie instruit permanent cu privire la modul de îndeplinire a atribuțiilor specifice.

85. În afara orelor de program și în zilele nelucrătoare se vor organiza patrulări în perimetrul obiectivului, la intervale care vor fi stabilite prin instrucțiuni elaborate pe baza planului de securitate al obiectivului.

86. Pentru eficientizarea sistemelor de pază și apărare trebuie asigurată detectarea pătrunderii neautorizate prin folosirea unor modalități adecvate (televiziune cu circuit închis, sisteme de alarmă sau pentru inspectare vizuală). Se va constitui în mod obligatoriu o forță de intervenție pentru situații de urgență. Timpul de reacție a personalului de pază și apărare în situații de urgență va fi testat periodic.

87. Atunci când se folosesc sisteme de alarmă, televiziune cu circuit închis sau alte dispozitive destinate supravegherii zonelor de securitate ori protecției informațiilor clasificate NATO trebuie să existe o sursă de alimentare de rezervă (generator de avarie).

88. Informațiile clasificate NATO sunt păstrate în containere speciale care se împart în 3 clase:

— clasa A: seifuri (containere cu cifru) aprobate de ANS pentru depozitarea informațiilor NATO/TOP SECRET;

— clasa B: fișete metalice prevăzute cu cifru pentru depozitarea informațiilor NATO/SECRET și NATO/CONFIDENTIAL;

— clasa C: mobilier de birou adecvat numai pentru păstrarea informațiilor NATO/RESTRICTED.

89. În situații de urgență, dacă documentele clasificate NATO trebuie evacuate, se vor utiliza lăzi metalice.

90. Încuietorile folosite la containerele în care sunt păstrate informații clasificate NATO nu trebuie scoase din obiectiv. Ele se împart în 3 grupe, astfel:

— grupa A: aprobate de ANS pentru containerele din clasa A;

— grupa B: pentru containerele din clasa B;

— grupa C: indicate numai pentru mobilierul de birou pentru clasa C.

91. Combinațiile încuietorilor containerelor vor fi cunoscute numai de persoanele abilitate.

92. În afara orelor de program cheile de serviciu de la încăperile și containerele din cadrul obiectivului vor fi păstrate în cutii sigilate la personalul care asigură paza și apărarea. Acestea vor fi utilizate pentru intervenție în situații de urgență. Cutiile vor fi predate/primite, pe bază de semnătură, într-un registru special destinat.

93. Cheile de rezervă și combinațiile încuietorilor vor fi păstrate în plicuri mate, sigilate, la șeful structurii/funcționarul de securitate. Evidența fiecărei combinații trebuie păstrată în plic separat. Cheilor și plicurilor trebuie să li se asigure un nivel de protecție corespunzător nivelului de clasificare a informațiilor clasificate NATO la care acestea permit accesul.

94. Cunoașterea combinațiilor containerelor de securitate va fi restrânsă la un număr minim de persoane. Cheile și combinațiile vor fi schimbate:

a) ori de câte ori are loc o schimbare în rândul personalului care le manipulează;

b) în cazul în care se constată existența unui risc de securitate;

c) la intervale regulate, de preferință o dată la 6 luni (fără a se depăși 12 luni).

95. Copiatoarele și dispozitivele telefax vor funcționa în încăperi special destinate, în care vor avea acces doar persoanele autorizate să le utilizeze.

96. Pe baza prezentelor reglementări, a normelor și reglementărilor proprii fiecărei instituții structura/funcționarul de securitate va elabora planul de securitate al obiectivului, aprobat de conducătorul instituției și avizat de instituțiile

abilitate prin lege. Elementele obligatorii care trebuie cuprinse în planul de securitate sunt următoarele:

a) delimitarea și marcarea zonelor de securitate;

b) sistemul de control al accesului;

c) sistemul de avertizare și alarmare;

d) sistemul de pază și apărare;

e) planul de evacuare a documentelor în caz de urgență;

f) modul de acțiune în situații de urgență (măsuri de evacuare/distrugere a documentelor);

g) modul de raportare, investigare și evidență a încălcărilor măsurilor de securitate;

h) modalitățile de realizare a pregătirii și instruirii personalului;

i) responsabilitățile privind verificarea sistemului de securitate al obiectivului;

j) modalitățile de realizare a inspecțiilor asupra măsurilor de securitate aplicate în cadrul obiectivului.

F. SECURITATEA PERSONALULUI

97. *Securitatea personalului* reprezintă ansamblul procedurilor de securitate care se aplică persoanelor care urmează să aibă acces la informații clasificate NATO.

98. Măsurile de securitate a personalului sunt menite:

a) să prevină accesul persoanelor neautorizate la informații clasificate NATO;

b) să garanteze că informațiile clasificate NATO sunt distribuite pe baza existenței certificatului de securitate, exclusiv pe baza principiului nevoii de a ști (need-to-know);

c) să permită identificarea persoanelor care, prin acțiunile lor, pot pune în pericol securitatea informațiilor clasificate NATO și să interzică accesul acestor persoane la astfel de informații.

99. Asigurarea securității personalului se realizează prin următoarele elemente: selecționarea, verificarea, avizarea și autorizarea accesului la informațiile clasificate NATO, revalidarea, retragerea certificatului, controlul și instruirea personalului.

100. Persoanele care fac obiectul verificărilor de securitate sunt cele care prin natura funcției sau activității lor necesită ori urmează să aibă acces la informațiile clasificate, trebuie să participe la activitățile NATO sau să lucreze în cadrul unui contract clasificat NATO.

101. Accesul la informații clasificate NATO, obținut în baza certificatului de securitate emis ca rezultat al procedurii de verificare a personalului, este restricționat de principiul nevoia de a ști (need-to-know).

102. Procesul de verificare are ca obiectiv reducerea riscurilor de securitate, sustragere sau divulgare neautorizată a informațiilor și materialelor clasificate NATO.

103. Verificarea în vederea avizării pentru accesul la informații clasificate NATO se efectuează cu respectarea legislației în vigoare privind responsabilitățile în domeniul protecției informațiilor clasificate naționale, după cum urmează:

A. Serviciul Român de Informații, pentru:

— personalul propriu;

— personalul autorităților și instituțiilor publice;

— personalul agenților economici cu capital integral sau parțial de stat și al persoanelor juridice de drept public, altele decât cele date în competența instituțiilor menționate la lit. B, C și D ale acestui punct.

B. Ministerul Apărării Naționale — Direcția generală de informații a apărării, pentru:

— personalul militar și civil propriu;

— angajații din unitățile productive și de afaceri, din unitățile științifice, de cercetare sau dezvoltare, înființate de/în colaborare cu Ministerul Apărării Naționale, precum și din alte unități organizatorice, în măsura producției sau serviciilor angajate prin contracte de furnizare de tehnică, aparatură și utilități militare în cadrul unor contracte, colaborări sau programe de asistență cu NATO.

C. Serviciul de Informații Externe, pentru:

— personalul militar sau civil propriu;

— personalul român al reprezentanțelor diplomatice, misiunilor permanente, consulare, centrelor culturale, organismelor internaționale etc., care își desfășoară activitatea în străinătate și care are acces la date clasificate NATO;

— cetățenii români aflați în străinătate în cadrul unor contracte, stagii de perfecționare, programe de cercetare sau în calitate de angajați la firme, societăți de stat sau private care derulează contracte de producție, servicii ori cooperare cu NATO ori cu structuri ale Alianței Nord-Atlantice.

D. Ministerul de Interne, Serviciul de Protecție și Pază, Serviciul de Telecomunicații Speciale, pentru personalul propriu.

104. Atunci când se impune, structurile competente în realizarea verificărilor de securitate cooperează, pe baza protocoalelor, în îndeplinirea sarcinilor și obiectivelor propuse.

105. Principalele criterii de evaluare a compatibilității unei persoane în acordarea avizului de securitate, pe baza căruia se eliberează de către ANS certificatul de securitate, vizează trăsăturile circumstanțiale și de caracter care pot genera riscuri de securitate. Deși aceste criterii se referă la persoana care trebuie avizată, conduita, caracterul, concepțiile sau împrejurările de viață ale soțului/soției ori concubinului/concubinei pot fi, de asemenea, relevante și trebuie luate în considerare.

106. Factorii ce trebuie analizați pentru titular și soțul/soția sau coabitantul:

a) dacă a comis sau a intenționat să comită, a fost complice, a ajutat ori a instigat pe altcineva să comită (sau să intenționeze să comită) acte de spionaj, terorism, trădare ori revoltă;

b) dacă a încercat, susținut, participat, cooperat sau sprijinit acțiuni de spionaj, terorism ori persoane suspectate de a se încadra în această categorie ori de a fi membre ale unor organizații sau puteri străine inamice securității țărilor membre ori partenere NATO sau complice ale reprezentanților acestora;

c) dacă este sau a fost membru al unei organizații care susține ori încearcă să răstoarne guvernul dintr-o țară membră sau parteneră NATO ori să schimbe forma de guvernământ dintr-o țară membră sau parteneră NATO prin mijloace violente, subversive ori prin alte forme ilegale;

d) dacă este sau a fost un susținător al vreunei organizații descrise în subparagraful c) de mai sus, este sau a fost recent în relații apropiate cu membrii unor astfel de organizații, într-o formă care să ridice suspiciuni temeinice cu privire la siguranța persoanei.

107. Factorii suplimentari ce trebuie analizați numai pentru titular:

a) dacă în mod deliberat a ascuns, a interpretat eronat sau a falsificat informații cu relevanță în planul securității ori a mințit prin completarea formularelor-tip ori în cursul interviului de securitate;

b) dacă a fost condamnat pentru infracțiuni de drept comun sau delicte care indică tendințe infracționale de comportament; are serioase probleme financiare sau există o diferență frapantă între nivelul său de trai și veniturile legal realizate; este dependent de folosirea alcoolului în exces sau de uzul de droguri; are sau a avut comportamente promiscue ori alte forme de deviații sexuale, care pot genera riscul ca persoana să fie vulnerabilă la șantaj sau presiuni; a demonstrat prin fapte sau vorbe nesiguranță, necinste, incorectitudine ori indiscreție; a încălcat regulile de securitate;

c) dacă suferă sau a suferit de boli fizice ori mintale, care pot cauza deficiențe de discernământ sau pot transforma persoana, în mod neintenționat, într-un factor de risc. În toate aceste cazuri se va solicita, cu acordul persoanei, un aviz medical competent;

d) dacă poate fi supus la presiuni din cauza rudelor sau a persoanelor apropiate, care ar putea genera o vulnerabilitate exploatabilă de către serviciile de informații străine, ale căror interese sunt ostile pentru interesele de securitate ale NATO și/sau ale țărilor membre și partenere.

108. Accesul la informațiile clasificate NATO/RESTRICTED se va face la nivelul instituțiilor angajatoare, pe baza avizului dat de structura/funcționarul de securitate, cu aprobarea șefului instituției.

109. Pentru acces la informații clasificate NATO/RESTRICTED nu se solicită certificat de securitate.

110. Verificarea de nivel I — pentru avizarea în vederea eliberării certificatului de securitate pentru nivelul NATO/CONFIDENTIAL (echivalent SECRET). Avizarea pentru acces la informațiile NATO/CONFIDENTIAL se va baza pe:

a) verificarea corectitudinii datelor menționate în formularul de bază;

b) referințe minime de la locurile de muncă și din mediile frecventate (cel puțin de la 3 persoane).

În situația în care este necesară clarificarea anumitor aspecte sau la solicitarea persoanei verificate investigatorul poate avea o întrevedere cu aceasta.

111. Verificarea de nivel II — pentru avizarea în vederea eliberării certificatului de securitate pentru nivelul NATO/SECRET (echivalent STRICT SECRET). Avizarea pentru acces la informații clasificate de nivel NATO/STRICT SECRET se va baza pe :

a) verificarea corectitudinii datelor personale menționate în formularul de bază și în formularul suplimentar;

b) referințe minime de la locurile de muncă și din mediile frecventate (cel puțin de la 3 persoane);

c) verificări asupra membrilor familiei în legătură cu datele prezentate în formular;

d) o discuție cu persoana verificată.

112. Verificarea de nivel III — pentru avizarea în vederea eliberării certificatului de securitate pentru nivelul NATO/TOP SECRET (echivalent STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ). Avizarea accesului la informațiile clasificate NATO/TOP SECRET se va baza pe:

a) verificarea corectitudinii datelor menționate în formularele de bază, suplimentar și financiar;

b) investigații de cunoaștere a antecedentelor la domiciliul actual și cele anterioare, la locul de muncă actual și cele anterioare, precum și la instituțiile de învățământ urmate începând de la vârsta de 18 ani. Investigațiile nu se vor limita la audierea persoanelor indicate de solicitantul avizului;

c) verificări ale mediului relațional pentru a identifica existența unor riscuri de securitate în cadrul acestora;

d) un interviu de securitate cu persoana solicitantă;

e) în cazul în care din verificările întreprinse rezultă că ar exista unele deficiențe psihice ori de comportament, cu acordul subiectului, acesta poate fi supus unui test psihologic specific, limitat la domeniul ce trebuie clarificat.

113. Dacă în cursul verificărilor, pentru orice nivel, apar informații ce evidențiază riscuri de securitate, se va realiza o verificare suplimentară de fond cu implicarea mijloacelor

specifice instituțiilor cu atribuții în domeniul siguranței naționale.

114. În funcție de nivelul de securitate investigația de cunoaștere a antecedentelor va cuprinde gradual următoarele:

a) Evidențe naționale — se va efectua o verificare în evidențele naționale de securitate și la cazierul judiciar, în evidențele centrale și locale ale poliției, precum și în baza de date a Oficiului registrului comerțului.

b) Registre de stare civilă și verificarea identității — se vor verifica datele personale și locul de naștere, iar identitatea va fi confirmată fără posibilitate de dubiu.

c) Statutul cetățeniei — se va stabili cu certitudine statutul cetățeniei și al naționalității persoanei, în prezent și în trecut.

d) Educația — în mod normal investigația va indica școlile, universitățile și alte instituții de învățământ urmate de titular de la împlinirea vârstei de 18 ani.

e) Angajări — investigațiile vor acoperi angajarea actuală și pe cele anterioare, cu referințe din surse ca: dosarele de angajare, aprecierile anuale asupra performanțelor și eficienței activității desfășurate, date furnizate de șefii instituțiilor, șefi de departamente sau de colegi.

f) Interviuri — se vor purta discuții cu persoane care pot face evaluări asupra trecutului persoanei, activității și corectitudinii sale.

g) Evidențele organelor centrale și locale de poliție — se vor verifica evidențele centrale și cele ale organelor locale de ordine din vecinătatea locurilor unde persoana a locuit sau a lucrat perioade substanțiale.

h) Serviciul militar — se va verifica serviciul efectuat de persoană în forțele armate și modalitatea în care a fost lăsată la vatră.

i) Relații în străinătate — se va verifica existența unor riscuri de securitate datorate unor presiuni exercitate de surse din străinătate.

j) Antecedente financiare — se vor verifica solvabilitatea și reputația financiară ale persoanei.

k) Organizații — în cursul investigației, așa cum a fost prezentată mai sus, se va stabili dacă persoana este sau a fost membru ori afiliat al vreunei organizații, asociații, mișcări, grupări de persoane străine sau autohtone, care au adoptat ori au manifestat o politică de sprijinire sau aprobare a comiterii de acte de forță sau violență, în scopul afectării drepturilor altor persoane, ori care caută să schimbe forma de guvernare din țările membre sau partenere NATO prin mijloace neconstituționale.

115. Eliberarea certificatului de securitate tip A are loc în baza unei solicitări scrise, semnată de șeful instituției și adresată ANS prin intermediul Registrului intern.

116. Solicitarea va fi însoțită de formularele-tip, care vor fi introduse într-un plic separat sigilat și vor fi completate de persoana selecționată.

117. Structura/funcționarul de securitate are obligația să pună la dispoziție persoanei selecționate formularele-tip corespunzătoare nivelului de acces pentru care se solicită eliberarea certificatului, să acorde asistență în vederea completării acestora și să respecte următoarele termene pentru transmiterea solicitării în raport cu data la care se preconizează accesul persoanei selecționate la informații clasificate NATO:

a) pentru acces la NATO/TOP SECRET — cu trei luni în avans;

b) pentru acces la NATO/SECRET — cu două luni în avans;

c) pentru acces la NATO/CONFIDENTIAL — cu o lună în avans.

118. În termen de 7 zile de la primirea solicitării ANS va transmite la instituția cu competență pentru efectuarea verificărilor cererea-tip de declanșare a procedurii de verificare pentru persoana selecționată, la care va anexa plicul sigilat cu formularele-tip completate.

119. După primirea formularelor instituția abilitată va efectua verificările și va transmite concluziile în scris la ANS în interiorul termenelor prevăzute mai sus. În concluzii se va preciza dacă rezultă sau nu rezultă riscuri de securitate în legătură cu persoana pentru care s-a solicitat verificarea.

120. Pentru cadrele proprii ale Serviciului Român de Informații, Ministerului Apărării Naționale, Serviciului de Informații Externe, Ministerului de Interne, Serviciului de Telecomunicații Speciale și ale Serviciului de Protecție și Pază, aceste instituții notifică ANS cu privire la declanșarea procedurii de verificare, iar eliberarea certificatului de securitate tip A are loc în baza unei solicitări scrise, semnată de șeful instituției și adresată ANS. În solicitarea scrisă se va preciza faptul că s-au efectuat verificările și se vor consemna concluziile cu privire la existența/inexistența riscurilor de securitate sau a altor elemente relevante din punct de vedere al securității.

121. Certificatele de securitate tip B sunt eliberate numai persoanelor care dețin certificate de securitate tip A.

122. Eliberarea certificatului de securitate tip B se realizează, în baza aprobării șefului instituției, de către structura/funcționarul de securitate din instituția în care persoana respectivă își desfășoară activitatea. În lipsa structurii/funcționarului de securitate respectiva instituție adresează solicitarea la ANS, care va elibera respectivul certificat. În această situație solicitarea va fi adresată ANS cu cel puțin două săptămâni înainte de data începerii

activității pentru care este necesară eliberarea certificatului de securitate.

123. Eliberarea certificatului de securitate se face pe baza analizării concluziilor verificărilor transmise de instituția abilitată să le efectueze. În cazul în care în concluziile verificărilor este evidențiată existența unor riscuri de securitate, ANS va decide dacă acestea pot fi un obstacol pentru eliberarea certificatului de securitate. Atunci când sunt semnalate elemente care nu constituie riscuri, dar sunt relevante din punct de vedere al securității, în luarea deciziei de eliberare a certificatului de securitate vor prima interesele de securitate.

124. ANS are la dispoziție un termen de 7 zile pentru emiterea certificatului de securitate sau pentru a comunica refuzul de eliberare a acestuia instituției solicitante.

125. Un exemplar al adresei de comunicare a deciziei ANS privind acordarea/neacordarea certificatului de securitate se va transmite instituției care a efectuat verificările.

126. Certificatul de securitate tip A se emite în două exemplare originale. Unul rămâne la Registrul Central, iar al doilea va fi păstrat la locul de muncă al persoanei.

127. Valabilitatea certificatului de securitate tip A eliberat unei persoane este de 3 ani.

128. O copie de pe certificatul de securitate tip B se păstrează la structura/funcționarul de securitate din cadrul instituției respective.

129. Reverificarea unei persoane se face dacă este necesară eliberarea unui nou certificat de securitate, dacă sunt evidențiate riscuri de securitate sau la cererea NATO. Eliberarea unui nou certificat de securitate poate avea loc, la solicitarea instituției, în următoarele situații:

a) dacă în îndeplinirea sarcinilor de serviciu persoana necesită acces la informații clasificate NATO de nivel superior;

b) dacă a expirat perioada de valabilitate a certificatului de securitate deținut anterior;

c) în cazul în care apar modificări în datele de identificare a persoanei care sunt prevăzute în certificat, certificatul de securitate vechi se retrage, eliberându-se un nou certificat.

130. Reverificarea se efectuează fără eliberarea unui nou certificat de securitate în următoarele situații:

a) în cazul în care există modificări ale datelor declarate în formularele completate anterior, cu excepția celor prevăzute la pct. 129 lit. c);

b) în cazul în care pe parcursul perioadei de valabilitate a certificatului de securitate se evidențiază existența unor riscuri de securitate;

c) în cazul în care structuri ale Alianței Nord-Atlantice sau ale unor autorități naționale de securitate din țări membre sau partenere NATO solicită expres reverificarea persoanei.

131. ANS este singura instituție autorizată să retragă certificatul de securitate. ANS va comunica instituțiilor decizia de retragere a certificatelor de securitate.

132. Certificatele de securitate tip A și tip B se retrag în următoarele cazuri:

a) la inițiativa ANS;

b) la cererea instituțiilor care au solicitat inițial eliberarea certificatului, inclusiv în situația expirării acestuia;

c) la plecarea din instituție sau la schimbarea locului de muncă al deținătorului, dacă noul loc de muncă nu presupune lucrul cu informații clasificate NATO;

d) la schimbarea nivelului de acces.

133. În cazul retragerii certificatului de securitate angajatului i se va interzice accesul la informații clasificate NATO.

134. După retragere certificatele de securitate tip A și tip B se distrug pe bază de proces-verbal, comunicându-se instituției care a derulat verificările acest fapt.

G. SECURITATEA DOCUMENTELOR

135. Consiliul Nord-Atlantic (denumit în continuare *NAC*) este autoritatea supremă care distribuie informațiile clasificate NATO, cu caracter oficial, către statele membre și partenere. Această autoritate funcționează după principiul consensului titularului informației.

136. Toate transferurile de documente de la NATO către statele partenere se efectuează prin Registrul NATO către Registrul Central al statului partener respectiv. Documentele care sunt transmise se referă la acțiuni, activități etc., care au fost aprobate de către NAC.

137. Organismele NATO păstrează, în calitate de deținător originar, evidența tuturor informațiilor NATO clasificate pe care le transmit statelor partenere și transmit datele de identificare a acestor documente (numărul, titlul și data transmiterii) către Registrul Central NATO de la Bruxelles. La cerere, autoritățile naționale pot obține detalii prin intermediul Registrului Central NATO de la Bruxelles.

138. Informațiile NATO neclasificate, deși nu presupun o protecție specifică, pot fi transmise și către state care nu fac parte din NATO, organizații, persoane doar atunci când se consideră că nu sunt afectate interesele NATO.

139. Informațiile clasificate NATO necesită o protecție specifică și sunt vehiculate în conformitate cu principiul nevoii de a ști (need-to-know) fără a fi menționat deținătorul originar, ci doar specificând „NATO“. Informația inițială rămâne proprietatea deținătorului originar, care este singura autoritate care decide asupra nivelului de clasificare și diseminării acesteia, și nu poate fi transmisă unui alt

stat care nu este stat membru sau unei organizații internaționale decât cu acordul acestuia.

140. Gestionarea documentelor clasificate NATO se face conform procedurilor NATO privind protecția informațiilor clasificate NATO, în cadrul Sistemului național de registre, de către persoane care trebuie să posede certificat de securitate cu nivel de clasificare corespunzător.

141. Gestionarea documentelor clasificate NATO, precum și a documentelor naționale transmise de România Alianței Nord-Atlantice se face separat de gestionarea documentelor naționale.

142. Informațiile neclasificate NATO nu fac obiectul procedurilor de securitate prin care se protejează informațiile clasificate NATO. Aceste informații vor fi gestionate în conformitate cu normele interne existente pentru informațiile naționale cu nivel echivalent, astfel încât să nu fie afectate interesele Alianței Nord-Atlantice.

143. Clasificarea informațiilor NATO este necesară pentru a indica gradul de sensibilitate al informațiilor și, în consecință, nivelul care trebuie atribuit pentru a determina complexitatea măsurilor și procedurilor care se impun în vederea protecției respectivelor informații împotriva dezvăluirii neautorizate.

144. Nivelurile de clasificare impun, pe de o parte, asigurarea măsurilor de securitate în conformitate cu standardele NATO pentru protejarea informațiilor, iar pe de altă parte, controlul accesului la respectivele informații.

145. Responsabilitatea încadrării informațiilor și a materialelor într-o categorie de clasificare revine deținătorului originar al informațiilor/materialelor și se face în funcție de importanța și conținutul acestora. Subestimarea (subclasificarea) importanței documentului este la fel de periculoasă ca și supraestimarea (supraclasificarea) acestuia.

146. Șeful ierarhic al deținătorului originar al documentului are obligația să verifice dacă acestea au fost clasificate corect și să ia măsurile care se impun pentru clasificarea corectă atunci când constată că au fost efectuate clasificări necorespunzătoare.

147. Schimbarea nivelului de clasificare a documentelor primite de la alte structuri instituționale se poate efectua numai cu acordul deținătorului originar al documentului.

148. Adresele care însoțesc documentele, în funcție de informațiile pe care le conțin, primesc nivelul de clasificare corespunzător, indiferent de nivelul de clasificare a documentului.

149. Extrasele din documentele care conțin informații clasificate NATO vor fi clasificate corespunzător conținutului informațiilor cuprinse, nivelul de clasificare fiind cel puțin egal cu cel al documentului de bază (din care s-a efectuat extragerea).

150. În funcție de importanța și sensibilitatea informațiilor există următoarele niveluri NATO de clasificare a informațiilor și care au următoarea echivalență în legislația națională:

ROMÂNIA	NATO
SECRET DE SERVICIU	RESTRICTED
SECRET	CONFIDENTIAL
STRICT SECRET	SECRET
STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ	TOP SECRET

151. Potrivit riscurilor generate de divulgarea neautorizată a informațiilor clasificate NATO, nivelurile de clasificare se atribuie în mod corespunzător importanței acestora și au următoarea semnificație:

— NATO/RESTRICTED — SECRET DE SERVICIU: nivel de clasificare care se aplică acelor informații și materiale a căror divulgare neautorizată va fi în dezavantajul intereselor NATO și al celor naționale;

— NATO/CONFIDENTIAL — SECRET: nivel de clasificare care se aplică informațiilor și materialelor a căror divulgare neautorizată va provoca prejudicii intereselor NATO și celor naționale;

— NATO/SECRET — STRICT SECRET: nivel de clasificare care se aplică doar informațiilor și materialelor a căror divulgare neautorizată va genera prejudicii grave la adresa NATO și a intereselor naționale;

— NATO/TOP SECRET — STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ: nivel de clasificare care se aplică doar informațiilor și materialelor a căror divulgare ar putea determina prejudicii extrem de grave la adresa NATO și a intereselor naționale.

152. Conform acordurilor de securitate încheiate, NATO transmite țărilor partenere informații clasificate marcate NATO până la nivelul SECRET inclusiv.

153. Informațiile NATO clasificate pot fi supuse procesului de scădere a nivelului de clasificare sau declasificării numai de către sau cu acordul deținătorului originar și numai după ce au fost consultate celelalte state membre și organizații.

154. Scăderea nivelului de clasificare se face periodic, în urma unei analize speciale care va stabili dacă nivelul de clasificare acordat inițial documentului mai concordă sau nu cu valoarea lui informațională la momentul analizei.

155. Schimbarea nivelului de clasificare a unui document va fi adusă imediat la cunoștință tuturor deținătorilor acelui document.

156. Prin *declasificare* se înțelege anularea nivelului de clasificare a unei informații clasificate NATO și astfel

scoaterea ei de sub incidența tuturor reglementărilor privind protecția informațiilor clasificate NATO.

157. Informațiile clasificate NATO de nivel CONFIDENTIAL sau SECRET vor fi sistematic revizuite pentru declasificare (numai după o perioadă de cel puțin 30 de ani).

158. Marca NATO aplicată pe un document semnifică faptul că documentul este proprietate NATO și că informația conținută rămâne proprietatea deținătorului originar. Astfel marca NATO se va aplica pe toate copiile pregătite de Alianța Nord-Atlantică spre a fi puse în circulație, inclusiv pe documentele neclasificate (de exemplu: NATO-UNCLASSIFIED).

159. Toate documentele care conțin informații NATO clasificate, inclusiv dosarele, volumele și broșurile legate sau reproducerile din acestea, vor fi marcate, scris sau tipărit, în partea de sus și de jos a primei pagini (coperta), a paginii cu titlul, pe prima pagină, pe ultima pagină și pe exteriorul copertei din spate. Fiecare dintre paginile documentului propriu-zis va avea marcat în partea de sus și în partea de jos nivelul de clasificare atribuit de deținătorul originar.

160. Documentele transmise de NATO își vor păstra nivelul de clasificare acordat de Alianța Nord-Atlantică pe toată durata existenței lor. Pe prima pagină a documentului va fi înscris numele componentei din cadrul NATO care a autorizat comunicarea, data când s-a hotărât comunicarea, precum și alte elemente care au legătura cu aceasta.

161. În situația în care un document clasificat este transmis de către NATO ca urmare a derulării unor activități comune, aprobate de către NAC, clasificarea este precedată de marca NATO și de numele unei activități, numele unei țări sau de numele unei organizații.

Exemplu: NATO/EAPC/PfP CONFIDENTIAL sau
NATO/ROMANIA CONFIDENTIAL sau
NATO/OSCE CONFIDENTIAL.

162. În situația în care titularul documentului consideră necesar să limiteze distribuția informației clasificate, acest lucru se va marca indicându-se sub linia de demarcare numele țării/țărilor căreia/cărora i/li se transmite documentul.

Exemplu: NATO/PfP CONFIDENTIAL
ROMANIA/BULGARIA only

sau

NATO/PfP CONFIDENTIAL
EXERCISE COPPERPLATE only

163. Documentele transmise Alianței Nord-Atlantice de către România vor purta marca ROMANIA, urmată de nivelul național de clasificare a documentului (echivalat cu nivelul de clasificare existent la NATO), și structura/activitatea din cadrul NATO către/în cadrul căreia se dorește transmiterea respectivului document.

Exemplu:

ROMANIA-CONFIDENTIAL	ROMANIA-SECRET
NATO only	PfP only

164. Cerințele minime pentru gestionarea informațiilor NATO clasificate se aplică în funcție de nivelul de clasificare.

165. Informațiile NATO/RESTRICTED vor fi vehiculate și păstrate în spații care nu vor fi accesibile persoanelor neautorizate.

166. Documentele vor fi transmise prin canale de comunicație autorizate de ANS în conformitate cu procedurile existente. Sistemele criptografice aprobate de un stat membru NATO sau de NAMIL COM vor fi utilizate pentru criptarea informațiilor NATO RESTRICTED care vor fi transmise prin mijloace electronice.

În situații deosebite, când viteza este elementul primordial și mijloacele de criptare nu sunt posibile, informațiile NATO RESTRICTED pot fi transmise electronic în text clar prin sistemele publice de comunicații.

167. Copierea și traducerea documentelor NATO RESTRICTED pot fi realizate în cadrul CSNR, cu respectarea strictă a principiului nevoii de a ști (need-to-know).

168. Informațiile NATO CONFIDENTIAL vor fi vehiculate și păstrate în zone în care accesul este controlat strict. Accesul va fi permis doar persoanelor care sunt în posesia certificatului de securitate corespunzător și pentru care s-a aprobat accesul.

169. Transmiterea documentelor se va face prin curier special sau sac diplomatic.

170. Sistemele criptografice aprobate de un stat membru NATO sau de NAMIL COM vor fi utilizate pentru criptarea informațiilor NATO CONFIDENTIAL care vor fi transmise prin mijloace electronice.

171. Copierea și traducerea documentelor NATO CONFIDENTIAL pot fi realizate de către persoane autorizate, cu respectarea principiului nevoii de a ști (need-to-know).

172. Informațiile NATO SECRET vor fi vehiculate și păstrate în zone pentru care accesul este strict controlat. Accesul va fi permis doar persoanelor care au certificat de securitate corespunzător și pentru care s-a stabilit necesitatea de a accesa astfel de documente în îndeplinirea sarcinilor de serviciu.

173. Transmiterea documentelor trebuie făcută prin curier special sau sac diplomatic. Pentru criptarea informațiilor vor fi utilizate numai sistemele criptografice autorizate de către NAMIL COM.

174. Copierea și traducerea documentelor NATO clasificate SECRET pot fi realizate de către posesorul acestora în conformitate cu principiul nevoii de a ști (need-to-know), numai după obținerea aprobării scrise a deținătorului originar. Copiile de pe documentele NATO clasificate SECRET

trebuie să fie marcate prin imprimarea numărului copiei. Numărul atribuit copiilor/traducerilor unor astfel de documente trebuie să existe în evidența respectivei componente a Sistemului național de registre (CSNR).

175. Activitatea de gestionare a documentelor clasificate NATO presupune:

— primirea documentelor — constă în activitatea de a desigila, dezambala documentele sosite;

— verificarea — constă în:

a) verificarea sigiliilor, a ambalajelor etc.;

b) verificarea documentelor care însoțesc documentul propriu-zis (adrese, borderouri etc.);

c) verificarea integrității documentului;

d) verificarea concordanței dintre numărul de pagini înscris pe borderou și numărul de pagini al documentului; la fel se va proceda și pentru anexe;

e) verificarea inscripționărilor obligatorii pe document;

— evidența — constă în înscrierea documentului în registrul de evidență din cadrul respectivei CSNR și inscripționarea pe document a numărului de înregistrare atribuit în cadrul registrului;

— consultarea — consultarea documentelor clasificate NATO de către persoanele autorizate se face pe bază de semnătură, cu respectarea principiului nevoii de a ști (need-to-know);

— distribuirea — constă în activitatea de repartizare a documentelor pentru rezolvarea acestora, în conformitate cu principiul nevoii de a ști (need-to-know);

— transmiterea — se referă la activitatea de circulație a documentelor clasificate NATO în cadrul Sistemului național de registre și între acesta și NATO;

— transportul — se referă la modul în care documentele clasificate NATO circulă între expeditor și destinatar;

— multiplicarea — se referă la activitatea de copiere a documentelor clasificate NATO. Evidența copiilor se păstrează în registrul special destinat;

— distrugerea — se referă la activitatea de tocare, incinerare, topire etc. a acelor documente care se consideră că nu mai sunt necesare pentru a fi păstrate; se efectuează diferit în funcție de nivelul de clasificare a documentului și, de regulă, are loc după o inventariere prealabilă a documentelor care vor fi păstrare în continuare;

— inventarierea — constă în activitatea anuală de verificare a existenței documentelor și de reînregistrare a celor care se consideră că mai sunt necesare în desfășurarea activității;

— arhivarea — constă în activitatea de păstrare în spații special amenajate a acelor documente care nu au fost distruse și care se consideră că sunt necesare în activitatea viitoare, dar pentru care nu se impune ca ele să fie păstrate în același loc cu documentele de uz curent.

H. SECURITATEA INDUSTRIALĂ

176. În îndeplinirea atribuțiilor ce îi revin pentru protecția informațiilor clasificate NATO în domeniul industrial, ANS desemnează în calitate de autorități desemnate de securitate instituțiile care, potrivit legislației, au competență națională în sfera civilă, respectiv militară, a sectorului industrial. În acest sens aceste autorități au următoarele competențe:

a) implementarea politicii de securitate națională în domeniul industrial, îndrumarea și acordarea asistenței necesare în aplicarea acestei politici;

b) impunerea respectării normelor de securitate industrială la nivel național (au dreptul să inspecteze și să aprobe măsurile pentru protecția informațiilor clasificate NATO);

c) urmărirea respectării componentelor unui contract sau subcontract clasificat NATO potrivit standardelor Alianței Nord-Atlantice. Înainte de transmiterea informațiilor clasificate NATO unui agent economic în cadrul derulării unui contract clasificat NATO, acesta trebuie să îndeplinească următoarele condiții:

— să asigure măsuri de protecție a acestora corespunzătoare prezentelor reglementări;

— să dețină certificat de securitate pentru obiectivul industrial implicat în contract;

— personalul implicat în derularea contractului clasificat NATO să dețină certificat de securitate de nivel corespunzător nivelului de clasificare a informațiilor NATO la care au acces;

— accesul la informațiile clasificate vehiculate în cadrul contractului este permis doar persoanelor care lucrează la acel contract, cu respectarea principiului nevoii de a ști (need-to-know);

d) la cererea unei autorități naționale de securitate dintr-un stat membru NATO, eliberează certificat de securitate unui agent economic implicat în negocierea sau executarea unui contract ori subcontract clasificat NATO;

e) la cererea unei autorități naționale de securitate dintr-un stat membru NATO, eliberează certificat de securitate pentru personalul implicat în negocierea sau executarea unui contract ori subcontract clasificat NATO;

f) va fi desemnată o structură/un funcționar de securitate în obiectivele implicate în derularea contractelor și subcontractelor clasificate NATO, cu atribuții specifice tipului de contract derulat.

177. În vederea eliberării certificatului de securitate pentru agenții economici implicați în derularea unui contract clasificat NATO se va verifica dacă sunt îndeplinite cerințele de securitate pentru protecția informațiilor clasificate NATO, potrivit nivelului de clasificare a informațiilor

vehiculate în cadrul contractului sau subcontractului, conform prezentelor reglementări.

178. Pentru persoanele implicate în derularea unui contract clasificat NATO se va elibera certificat de securitate conform prezentelor norme.

I. INFOSEC

179. Politica de securitate și cerințele acestei secțiuni se vor aplica tuturor sistemelor de prelucrare automată a datelor, denumite în continuare *SPAD,* și rețelelor de transmisii de date, denumite în continuare *RTD*, precum și sistemelor informatice și de comunicații, denumite în continuare *SIC*, care stochează, procesează și/sau transmit informații clasificate NATO. Aceste sisteme necesită măsuri de securitate a informațiilor, îndeosebi de control al accesului, pe baza principiului nevoii de a ști și a nivelului de securitate atribuit.

180. Protecția SPAD și/sau RTD (SIC) din compunerea sistemelor de armament și de detecție va fi definită în contextul general al sistemelor din care acestea fac parte și va fi realizată prin aplicarea prevederilor prezentei secțiuni.

181. Protecția informațiilor clasificate NATO care sunt stocate, procesate sau transmise în SPAD și/sau RTD (SIC) este asigurată de către ANS prin intermediul următoarelor autorități: Autoritatea de Acreditare de Securitate, denumită în continuare *AAS*, Autoritatea de Securitate pentru Informatică și Comunicații, denumită în continuare *ASIC,* Autoritatea pentru Distribuirea Materialului Criptografic, denumită în continuare *ADMC.*

182. AAS este responsabilă la nivel național cu acreditarea de securitate și aplicarea politicii de securitate NATO conform acreditării date pentru SIC.

183. AAS este responsabilă pentru aprobarea dată unui SPAD și/sau RTD (SIC) de a stoca, de a procesa sau de a transmite informații clasificate NATO până la nivelul de clasificare acordat (incluzând, unde este cazul, unele categorii cu destinație specială) în mediul său operațional. AAS este responsabilă cu evaluarea și certificarea sistemelor SPAD și/sau RTD (SIC) sau a unor elemente componente ale acestora.

184. AAS este o structură de acreditare la nivel național, subordonată ANS, cu reprezentanțe delegate/desemnate din cadrul departamentelor implicate, în funcție de SPAD și/sau RTD (SIC) care trebuie acreditate. AAS este responsabilă cu procesul periodic de reacreditare a SPAD și/sau RTD (SIC).

185. AAS își exercită responsabilitatea în domeniul securității în numele ANS, este responsabilă pentru securitate în toate cazurile, cu excepția unor situații speciale, și are autoritatea de a impune standarde de securitate.

186. AAS stabilește strategia de acreditare de securitate din cadrul politicii generale de securitate a ANS și formulează explicit condițiile în care poate fi solicitată să acrediteze SPAD și/sau RTD (SIC).

187. ASIC este structura care activează la nivel național, subordonată ANS, cu reprezentanțe delegate/desemnate de către ANS în cadrul departamentelor implicate. ASIC își exercită autoritatea pe plan local prin intermediul Autorității Operaționale a SIC, denumită în continuare *AOSIC*. Este responsabilă cu conceperea și implementarea mijloacelor și metodelor de protecție a informațiilor clasificate NATO, care sunt stocate, procesate sau transmise prin intermediul SIC, și are în principal următoarele responsabilități:

a) coordonarea tuturor activităților de protecție a informațiilor clasificate NATO, care sunt stocate, procesate sau transmise prin intermediul SIC;

b) inițiativa elaborării și promovării de reglementări și standarde specifice;

c) analiza cauzelor provocatoare de incidente de securitate și gestionarea bazei de date privind vulnerabilitățile din sistemele de comunicație și informatice, necesare pentru managementul riscurilor asupra securității SIC;

d) semnalarea către AAS a incidentelor de securitate;

e) integrarea măsurilor privind protecția fizică de personal, de documente, administrativă, COMPUSEC, COMSEC, TEMPEST, criptologică;

f) executarea inspecțiilor periodice asupra SPAD și/sau RTD (SIC) în vederea reacreditării acordate de către AAS;

g) supunerea certificării și autorizării a sistemelor de securitate specifice SIC;

h) cooperarea cu AAS, ADMC și cu alte structuri de securitate implicate.

188. ADMC este o structură națională subordonată ANS și are următoarele responsabilități:

— managementul materialelor și echipamentelor criptografice specifice NATO;

— distribuirea materialelor și echipamentelor criptografice specifice NATO;

— raportarea periodică la ASIC a incidentelor de securitate cu care s-a confruntat;

— cooperarea cu AAS, ASIC și cu alte structuri de securitate implicate.

189. Amenințarea poate fi definită ca o posibilitate de compromitere accidentală sau deliberată a securității SPAD și/sau RTD (SIC) prin pierderea confidențialității, a integrității sau disponibilității informațiilor în formă electronică. Vulnerabilitatea poate fi definită ca fiind o slăbiciune sau lipsă de control care ar permite sau ar facilita o manevră de amenințare împotriva unei valori ori ținte specifice și ea poate fi de natură tehnică, procedurală sau operațională.

190. Măsurile de securitate prevăzute în această secțiune se aplică SIC care stochează, procesează sau transmit informații clasificate NATO, începând cu nivelul CONFIDENTIAL.

191. Crearea mediului de securitate în care trebuie să opereze SPAD și/sau RTD (SIC) presupune definirea și implementarea unui set echilibrat de măsuri de securitate (fizice, de personal, administrative, de tip TEMPEST, privind tehnica de calcul și comunicațiile).

192. Măsurile de securitate destinate protecției SIC trebuie să asigure controlul accesului pentru prevenirea sau detectarea divulgării neautorizate a informațiilor. Procesul de certificare și acreditare va stabili dacă aceste măsuri sunt corespunzătoare.

193. Cerințele de securitate specifice, denumite în continuare *CSS*, se constituie într-un document încheiat între AAS și AOSIC, fiind o listă completă de principii de securitate care trebuie respectate și de măsuri de securitate detaliate ce trebuie implementate, care stau la baza procesului de certificare și acreditare a SPAD și/sau RTD (SIC).

194. CSS se elaborează pentru toate SPAD și/sau RTD (SIC) care stochează, procesează sau transmit informații clasificate NATO. Aceste cerințe sunt stabilite de către AOSIC și sunt aprobate de către AAS.

195. CSS vor fi formulate încă din faza de proiectare a SPAD și/sau RTD (SIC) și vor fi dezvoltate de-a lungul întregului ciclu de viață al sistemului.

196. CSS au la bază principiile politicii NATO de securitate și de evaluare a riscurilor, promovate de către ANS, ținând seama de parametrii esențiali ai mediului operațional, de nivelul minim de autorizare a personalului, de nivelul de clasificare a informațiilor și de modul de operare a sistemului care urmează să fie acreditat.

197. SPAD și/sau RTD (SIC) care stochează, procesează sau transmit informații clasificate NATO vor fi certificate și acreditate să opereze pe anumite perioade și în diverse moduri de operare, astfel:

a) dedicat;

b) de nivel înalt;

c) multinivel.

198. În modul de operare „dedicat“ toate persoanele cu drept de acces la SPAD și/sau RTD au certificat de securitate pentru cel mai înalt nivel de clasificare a informațiilor stocate, procesate sau transmise în cadrul SPAD și/sau RTD (SIC). Necesitatea de cunoaștere pentru aceste persoane se referă la toate informațiile stocate, procesate sau transmise în cadrul SPAD și/sau RTD (SIC).

1. În acest mod de operare principiul nevoii de a ști (need-to-know) nu impune o cerință expresă de separare a informațiilor, în cadrul SPAD și/sau RTD, ca mijloc de securitate a SIC.

2. Celelalte elemente de securitate (de exemplu: securitatea fizică, de natură procedurală sau la nivel de personal) vor satisface cerințele impuse de cel mai înalt nivel de clasificare și de toate categoriile de informații cu destinație specială stocate, procesate sau transmise în cadrul SPAD și/sau RTD.

199. În modul de operare „de nivel înalt“ toate persoanele cu drept de acces la SPAD și/sau RTD (SIC) au certificat de securitate pentru cel mai înalt nivel de clasificare a informațiilor stocate, procesate sau transmise în cadrul SPAD și/sau RTD (SIC), dar accesul la informații se face diferențiat, conform principiului nevoii de a ști (need-to-know).

1. Faptul că în acest mod accesul la informații se face diferențiat, conform principiului nevoii de a ști (need-to-know), înseamnă că trebuie să existe în compensație facilități de securitate care să asigure un mod de acces selectiv la informațiile din cadrul SPAD și/sau RTD (SIC).

2. Celelalte facilități de securitate (de exemplu: securitatea fizică, de natură procedurală sau de personal) vor satisface cerințele de protecție pentru cel mai înalt nivel de clasificare și pentru toate categoriile de informații cu destinație specială stocate, procesate, transmise în cadrul SPAD și/sau RTD (SIC).

3. Toate informațiile stocate, procesate sau vehiculate în cadrul unui SPAD și/sau RTD (SIC) sub acest mod de operare vor fi protejate ca informații cu destinație specială și ca informații cu nivel maxim de clasificare.

200. În modul de operare „multinivel“ nu toate persoanele cu drept de acces SPAD și/sau RTD (SIC) au certificat de securitate pentru acces la informații de cel mai înalt nivel de clasificare, care sunt stocate, procesate sau transmise prin SPAD și/sau RTD (SIC). De asemenea, nu toate persoanele cu acces la SPAD și/sau RTD (SIC) au acces la toate informațiile stocate, procesate, transmise în cadrul SPAD și/sau RTD, accesul la informații făcându-se diferențiat, conform principiului nevoii de a ști (need-to-know).

1. Acest mod de operare protejat permite stocarea, procesarea sau transmiterea informațiilor cu diferite niveluri de clasificare și de diverse destinații.

2. Faptul că nu toate persoanele sunt autorizate pentru cel mai înalt nivel de clasificare, combinat cu faptul că accesul la informații se face diferențiat, conform principiului nevoii de a ști (need-to-know), înseamnă că trebuie să existe în compensație facilități de securitate care să asigure un mod selectiv de acces la informațiile din cadrul SPAD și/sau RTD.

201. AOSIC este persoana sau compartimentul având responsabilitatea, delegată de către ASIC, asupra SPAD și/sau RTD (SIC) pentru implementarea metodelor și mijloacelor necesare protecției informațiilor, precum și pentru

exploatarea operațională a SPAD și/sau RTD (SIC) în condiții de securitate. Responsabilitatea AOSIC cuprinde întregul ciclu de viață al SPAD și/sau RTD (SIC), începând cu proiectarea, continuând cu elaborarea specificațiilor, testarea instalării, acreditarea, testarea periodică în vederea reacreditării, exploatarea operațională, modificarea și sfârșind cu scoaterea din uz. În anumite situații speciale rolul AOSIC poate fi preluat de către diverse componente ale organizației, în decursul ciclului de viață. Este important ca rolul AOSIC să fie de la început identificat și exercitat fără întrerupere în decursul ciclului de viață.

202. AOSIC coordonează cooperarea dintre organismul care exercită autoritatea asupra SIC al unei organizații și organismul care asigură acreditarea de securitate, atunci când organizația:

a) planifică dezvoltarea sau achiziția de SPAD și/sau RTD;

b) propune schimbări ale unei configurații de sistem existente;

c) propune conectarea unui SPAD și/sau a unei RTD (SIC) cu un alt SPAD și/sau RTD (SIC);

d) propune schimbări ale modului de operare de securitate ale SPAD și/sau RTD (SIC);

e) propune schimbări în programele existente sau propune utilizarea de noi programe care au impact asupra securității SPAD și/sau RTD (SIC);

f) propune modificarea nivelului de clasificare a securității pentru SPAD și/sau RTD (SIC) care au fost deja acreditate;

g) planifică, propune sau intenționează să întreprindă orice altă activitate care poate afecta securitatea SPAD și/sau RTD (SIC) deja acreditate (de exemplu, creșterea substanțială a numărului de utilizatori).

203. AOSIC, îndrumat de către AAS și în cooperare cu cel care exercită autoritatea asupra SIC, stabilește standardele și procedurile de securitate care trebuie respectate de către furnizorul de echipamente pe parcursul dezvoltării, instalării și testării SPAD și/sau RTD (SIC). AOSIC este responsabilă pentru justificarea, selecția, implementarea și controlul componentelor tehnice de asigurare a securității care constituie parte a SPAD și/sau RTD (SIC).

204. AOSIC atribuie structurilor de securitate și management ale SPAD și/sau RTD (SIC), încă de la înființare, responsabilitățile necesare pe care să le exercite pe tot ciclul de viață al SPAD și/sau RTD (SIC).

205. AOSIC sau structura delegată competentă desemnează administratorul de securitate al obiectivului SIC, care răspunde de asigurarea implementării și menținerii măsurilor de securitate fizică aplicabile obiectivului respectiv.

206. Un obiectiv SIC reprezintă un amplasament specific sau un grup de amplasamente în care funcționează un SPAD și/sau o RTD. Responsabilitățile pentru fiecare zonă de amplasare a unui terminal/a unei stații de lucru care funcționează la distanță trebuie explicit determinate. Responsabilitățile unui administrator de securitate de obiectiv sunt îndeplinite de funcționarul de securitate din cadrul structurii de securitate a obiectivului, ca parte a îndatoririlor profesionale.

207. AOSIC desemnează un administrator de securitate al SPAD (SIC), care este responsabil cu supervizarea dezvoltării, implementării și administrării măsurilor de securitate dintr-un SPAD (SIC), inclusiv cu participarea la elaborarea procedurilor operaționale de securitate. La recomandarea AAS, AOSIC desemnează persoane suplimentare (de exemplu, pentru compartimente specifice unei organizații) care îndeplinesc atributele de securitate în conformitate cu măsurile stabilite de administratorul de securitate al SPAD în cadrul procedurilor operaționale de securitate (*PrOpSec*).

208. Pentru un SIC de mari dimensiuni sau în cazul interconectării SPAD, AOSIC nominalizează un administrator de securitate al rețelei, care are responsabilități în ceea ce privește managementul securității comunicațiilor.

209. Toți utilizatorii de SPAD și/sau RTD (SIC) poartă responsabilitatea în ceea ce privește securitatea acestora (raportate, în principal, la drepturile acordate) și sunt îndrumați de către administratorii de securitate. Informarea și conștientizarea utilizatorilor asupra îndatoririlor lor de securitate asigură o eficacitate sporită a sistemului de securitate.

210. Pregătirea și instruirea cu privire la securitatea SIC sunt asigurate adecvat la diferite niveluri și pentru clasele de personal diferite ale unei organizații, cum ar fi: nivelul superior de conducere, personalul autorității de securitate, administratorii de securitate, utilizatorii etc., și sunt în conformitate cu planul general de instruire elaborat de către ANS.

211. Utilizatorii SPAD și/sau RTD (SIC) sunt autorizați și li se permite accesul la informații clasificate, pe baza principiului nevoii de a ști (need-to-know) și în funcție de nivelul de clasificare a informațiilor stocate, procesate sau transmise în cadrul SPAD și/sau RTD.

212. Datorită vulnerabilității informațiilor față de accesarea neautorizată, interzicerea accesului, divulgare, alterare, modificare sau ștergere, se prevăd măsuri speciale pentru instruirea și supravegherea personalului, incluzând aici și personalul de proiectare a sistemului, care are acces la SPAD și/sau RTD.

213. SPAD și/sau RTD (SIC) trebuie proiectate astfel încât să permită atribuirea sarcinilor și răspunderilor personalului de o așa manieră încât să nu existe o persoană care să aibă cunoștință de sau acces la toate cheile de

securitate (parole, mijloace de identificare personală etc.) și la toate programele.

214. Procedurile de lucru ale personalului din SPAD și/sau RTD (SIC) trebuie să asigure separarea dintre operațiunile de programare și cele de exploatare a sistemului sau a rețelei. Este interzis, cu excepția unor situații speciale, ca personalul să facă atât programarea, cât și operarea sistemelor sau rețelelor și trebuie instituite proceduri speciale pentru detectarea acestor situații.

215. Pentru orice fel de modificare aplicată unui SPAD și/sau RTD (SIC) este obligatorie colaborarea a cel puțin două persoane. Procedurile de securitate trebuie să prevadă explicit situațiile în care regula de lucru cu două persoane (two men rule) este implementată.

216. Pentru asigurarea și implementarea corectă a măsurilor de securitate personalul SPAD și/sau RTD (SIC) și personalul care răspunde de securitatea SPAD și/sau RTD (SIC) este instruit și informat în așa fel încât să își cunoască reciproc responsabilitățile.

217. Zonele în care sunt amplasate SPAD și/sau RTD (SIC) și cele cu terminale la distanță, unde sunt prezentate, stocate, procesate sau transmise informații clasificate NATO ori în care este posibil accesul potențial la astfel de informații, se declară zone de securitate ale obiectivului.

218. În zonele în care sunt amplasate SPAD și terminale la distanță (stații de lucru), unde se procesează și/sau pot fi accesate informații clasificate NATO, se aplică următoarele măsuri generale de securitate:

a) intrarea personalului și a materialelor, precum și plecarea în/din aceste zone sunt controlate prin mijloace bine stabilite;

b) zonele și locurile în care securitatea SPAD și/sau RTD (SIC) ori a terminalelor la distanță poate fi modificată nu trebuie să fie niciodată ocupate de o singură persoană;

c) persoanelor care solicită acces temporar sau cu intermitențe în aceste zone trebuie să li se autorizeze accesul ca vizitatori de către responsabilul pe probleme de securitate al zonei, desemnat de către administratorul de securitate al SPAD, conform atribuțiilor. Vizitatorii sunt însoțiți permanent pentru a avea garanția că nu pot avea acces la informații clasificate NATO și nici la echipamentele utilizate.

219. În funcție de riscul de securitate și de nivelul de clasificare a informațiilor stocate, procesate și transmise, poate să se impună cerința de aplicare a regulii de lucru cu două persoane (two men rule) și în alte zone. Acestea se stabilesc în stadiul inițial al proiectului și sunt specificate în cadrul cerințelor de securitate specifice ale SIC.

220. Când un SPAD este exploatat în mod autonom, deconectat în mod permanent de alte SPAD, atunci, ținând seama de condițiile specifice, de alte măsuri de securitate tehnice sau procedurale și de rolul pe care îl joacă respectivul SPAD în funcționarea de ansamblu, AAS poate să renunțe la cerințele pct. 218 lit. b). În asemenea cazuri AAS trebuie să stabilească reguli, adaptate la structura SPAD, conform nivelului de clasificare a informațiilor procesate, și să identifice caracteristicile speciale.

221. Toate informațiile și materialele care controlează accesul la SPAD sau la RTD (SIC) sunt controlate și protejate de reglementări corespunzătoare nivelului de clasificare cel mai ridicat și specificului categoriei de informații la care respectivul SPAD și/sau RTD (SIC) permite accesul.

222. Când nu mai sunt utilizate, informațiile și materialele de control trebuie să fie distruse.

223. Titularul informațiilor are obligația de a identifica și de a clasifica toate documentele purtătoare de informații, indiferent de suportul pe care se află (copie pe hârtie sau medii de stocare specifice tehnologiei informației). Fiecare document, indiferent de suport, trebuie marcat cu nivelul său de clasificare. Suportul pe care se află documentele va căpăta același nivel de clasificare ca și nivelul cel mai înalt de clasificare a informațiilor utilizate pentru elaborarea documentelor. De asemenea, acestea se pot clasifica și conform nivelului cel mai înalt de clasificare a unui SPAD și/sau RTD (SIC) funcționând în modul „dedicat“ sau de „nivel înalt“, cu excepția situației în care titularul sau autoritatea care răspunde de punerea la dispoziție a respectivelor informații a stabilit, după verificare, o altă clasificare.

224. Titularii de informații au obligația să analizeze aspectele privind agregarea informațiilor și consecințele asupra nivelului de clasificare ce pot rezulta din aceasta, pentru a decide eventual acordarea unui nivel de clasificare mai ridicat pentru informația rezultată în urma agregării.

225. Modul în care este prezentată informația în clar (chiar dacă se utilizează codul prescurtat sau de transmisie, reprezentarea binară) nu asigură nici un fel de protecție de securitate și nu trebuie, prin urmare, să influențeze nivelul de clasificare acordat informațiilor respective.

226. Documentele conținând informații clasificate NATO trebuie să fie controlate, conform reglementărilor de securitate în vigoare, înainte de a fi transmise din zonele SPAD și/sau RTD (SIC) ori din cele cu terminale la distanță.

227. Când informațiile sunt transferate de la un SPAD sau RTD (SIC) către alt SPAD sau RTD (SIC), ele trebuie să fie protejate atât în timpul transferului, cât și în SPAD sau RTD (SIC) care le primește, corespunzător clasificării originale a informațiilor.

228. Toate mediile de stocare a informațiilor se păstrează într-o modalitate care să fie în concordanță cu

cel mai înalt nivel de clasificare a informațiilor stocate pe acestea, fiind protejate permanent.

229. Mediile refolosibile de stocare a informațiilor, utilizate pentru înregistrarea informațiilor clasificate NATO, își mențin cea mai înaltă clasificare pentru care au fost vreodată utilizate, până când respectivelor informații li se reduce nivelul de clasificare sau sunt declarate neclasificate, moment în care mediile menționate mai sus se reclasifică în mod corespunzător sau sunt distruse în conformitate cu prevederile PrOpSec.

230. Evidența automată sau manuală a accesului la informațiile clasificate NATO de la nivelul SECRET în sus se ține sub forma registrelor de acces. Aceste registre se păstrează pe o perioadă stabilită de comun acord între AAS și AOSIC. În ceea ce privește registrele de acces la informațiile clasificate NATO nivel NATO TOP SECRET sau cele din categoria specială, perioada minimă de păstrare este de 10 ani; în cazul informațiilor clasificate NATO nivel SECRET perioada minimă de păstrare pentru aceste registre nu va fi mai mică de 3 ani.

231. Mediile de stocare care conțin informații clasificate NATO ce sunt utilizate în interiorul unei zone SPAD pot fi manipulate ca un unic material clasificat, nefiind nevoie să fie înregistrate în Registrul Central sau în subregistre, cu condiția ca materialul să fie identificat, marcat cu nivelul său de clasificare și controlat în interiorul zonei SPAD, până în momentul în care este distrus, redus la o copie de arhivă sau pus într-un dosar permanent. Evidențele și controlul materialelor clasificate vor fi menținute în cadrul zonei SPAD până când acestea sunt supuse controlului de evidență sau sunt distruse.

232. În cazul în care un material este generat într-un CIS, iar apoi este transmis într-o zonă cu terminal/stație de lucru îndepărtat, se stabilesc proceduri adecvate de securitate, agreate de către AAS. Procedurile trebuie să cuprindă și instrucțiuni specifice privind evidența informațiilor.

233. Toate mediile de stocare amovibile, clasificate de la nivelul NATO CONFIDENTIAL în sus, se identifică și se controlează în mod corespunzător (pentru nivelurile NATO UNCLASSIFIED și NATO RESTRICTED se aplică regulamentele de securitate locale, aprobate de către ANS). Identificarea și controalele trebuie să includă cel puțin următoarele cerințe:

a) pentru nivelul NATO CONFIDENTIAL și mai sus:

— un mijloc de identificare (număr de serie și marcajul nivelului de clasificare) pentru fiecare astfel de mediu, în mod separat (cu precizarea că marcarea nivelului de clasificare trebuie să indice cel mai înalt nivel de clasificare stocat vreodată pe acel mediu, în cazul în care nu a fost declasificat conform procedurilor aprobate);

— proceduri complete pentru emiterea, primirea sau retragerea mediului de memorare, pentru a fi distrus sau pentru alte scopuri;

— înregistrări manuale sau tipărite la imprimantă, indicând conținutul general, clasificarea și precizarea categoriei informației;

b) pentru nivelul NATO SECRET și mai sus informațiile detaliate asupra mediului de stocare amovibil, incluzând conținutul și nivelul de clasificare, se țin într-un registru adecvat.

234. Controlul punctual (spot-checking) și de ansamblu al mediilor de stocare amovibile, pentru a asigura compatibilitatea cu procedurile de identificare și control în vigoare, astfel:

a) pentru nivelul NATO CONFIDENTIAL controalele punctuale ale prezenței fizice și ale conținutului mediilor de stocare amovibile se efectuează periodic, pentru a garanta că acele medii de stocare nu conțin informații cu un nivel de clasificare superior;

b) pentru nivelul NATO SECRET toate mediile amovibile se inventariază periodic, controlând punctual prezența lor fizică și conținutul (pentru a garanta că pe acele medii nu sunt stocate informații cu un nivel de clasificare superior);

c) pentru nivelul NATO COSMIC TOP SECRET și Categoria Specială de informații toate mediile amovibile se verifică anual și se controlează punctual (spot-checked), periodic, în legătură cu prezența lor fizică și cu conținuturile lor (pentru a garanta că pe acele medii nu sunt stocate în mod necorespunzător informații din Categoria Specială).

235. Utilizatorii trebuie să își asume responsabilitatea pentru a garanta că informațiile clasificate NATO sunt stocate pe medii de stocare având marcarea și protecția corespunzătoare. Procedurile trebuie stabilite pentru a se garanta că, pentru toate nivelurile de clasificare a informațiilor NATO, stocarea acestora se realizează în conformitate cu reglementările de securitate.

236. Informațiile clasificate NATO înregistrate pe medii de stocare refolosibile sunt șterse doar în conformitate cu procedurile PrOpSec.

237. Când un mediu de stocare urmează să iasă din uz, trebuie să fie declasificat, după care poate fi eliberat și utilizat ca mediu de stocare neclasificat. Dacă acesta nu poate fi declasificat, trebuie distrus printr-o procedură aprobată. Mediile de stocare care conțin informații NATO COSMIC TOP SECRET sau Categorie Specială pot fi distruse, dar nu pot fi declasificate și refolosite.

238. Informațiile clasificate NATO, stocate pe un mediu nereutilizabil pentru procesul de scriere (cartele sau benzi

perforate, tipărituri etc.), vor fi distruse conform prevederilor cap. G „Securitatea documentelor".

239. Toate mijloacele folosite pentru transmiterea electromagnetică a informațiilor clasificate NATO se supun instrucțiunilor NATO de securitate a comunicațiilor, instrucțiuni promovate de către ANS.

240. Într-un SPAD (SIC) trebuie să se asigure mijloace de interzicere categorică a accesului la informațiile clasificate NATO de la toate terminalele/stațiile de lucru îndepărtate, atunci când se solicită acest lucru, prin deconectare fizică sau prin proceduri software speciale, aprobate de către AAS.

241. Instalarea inițială a SIC și orice modificare majoră adusă acestuia sunt executate de persoane autorizate. Acestea sunt sub supravegherea permanentă a unui personal tehnic calificat, care are acces la informații clasificate NATO de cel mai înalt nivel de clasificare a informațiilor, pe care respectivul SIC le va stoca, le va procesa sau le va transmite.

242. Toate echipamentele vor fi instalate în conformitate cu reglementările NATO specifice în vigoare, promovate de către ANS. Se vor folosi și directive naționale echivalente pe plan tehnic.

243. Sistemele SIC care stochează, procesează și/sau transmit informații clasificate NATO nivel CONFIDENTIAL și mai sus vor fi protejate corespunzător față de vulnerabilitățile de securitate cauzate de radiațiile compromițătoare (TEMPEST).

244. Procesarea informațiilor se realizează în conformitate cu PrOpSec.

245. Transmiterea informațiilor NATO CONFIDENTIAL și mai sus către instalații automate (a căror funcționare nu necesită prezența unui operator uman) este interzisă, cu excepția cazului în care se aplică reglementări speciale aprobate de către AAS, iar acestea au fost specificate în PrOpSec.

246. În SIC care au utilizatori existenți sau potențiali fără certificate de securitate nu se pot stoca, procesa și transmite informații clasificate NATO COSMIC TOP SECRET sau din Categoria Specială.

247. PrOpSec reprezintă o descriere a implementării politicii de securitate ce urmează să fie adoptată, a procedurilor operaționale de urmat și a responsabilităților personalului.

248. PrOpSec sunt elaborate de către ASIC în colaborare cu AOSIC și AAS, care coordonează și alte elemente de securitate implicate. AAS va aproba procedurile de operare înainte de a autoriza stocarea, procesarea sau transmiterea informațiilor de nivel NATO CONFIDENTIAL și mai sus.

249. AOSIC stabilește controale care vor garanta că toate produsele software originale (sisteme de operare generale, subsisteme și pachete soft), aflate în folosință, sunt protejate în condiții conforme cu nivelul de clasificare a informațiilor pe care acestea trebuie să le proceseze. Protecția programelor (software) de aplicație se stabilește în primul rând pe baza unei evaluări a nivelului de clasificare de securitate a acestora și apoi se va ține seama de nivelul de clasificare a informațiilor pe care acestea urmează să le proceseze.

250. Versiunile software care sunt în uz trebuie să fie verificate la intervale regulate pentru a garanta integritatea și funcționarea lor corectă. Versiunile noi sau modificate ale software nu vor fi folosite pentru procesarea informațiilor de nivel NATO CONFIDENTIAL și mai sus, până când procedurile de securitate software nu sunt testate și aprobate de către administratorul de securitate al SPAD. Versiunile noi sau modificate ale software mai depind și de condițiile reacreditării prezentate în cerințele de securitate specifice ale sistemelor, aprobate de către AAS. Un software care modifică posibilitățile sistemului sau care îi conferă posibilități noi și care nu conține nici o procedură de securitate nu poate fi folosit înainte de a fi verificat de către AOSIC.

251. Verificarea prezenței virușilor și a software nociv se face în conformitate cu cerințele impuse de către AAS.

252. Versiunile de software noi sau modificate (sisteme de operare, subsisteme, pachete de software și software de aplicație), stocate pe diferite medii, care se introduc într-o instituție/structură/organizație, trebuie verificate (obligatoriu pe sisteme de calcul izolate) în vederea depistării software nociv sau a virușilor de calculator, înainte de a fi folosite în SPAD și/sau RTD (SIC). În plus, periodic se va proceda la verificarea software instalat; aceste verificări trebuie făcute mai frecvent dacă SPAD și/sau RTD (SIC) sunt conectate la alt SPAD și/sau RTD (SIC) ori la o rețea publică de comunicații de date sau la o rețea telefonică publică.

253. În contractele de întreținere a SPAD și/sau RTD (SIC), care stochează/procesează/transmit informații clasificate de nivel NATO CONFIDENTIAL sau mai sus, se vor specifica cerințele care trebuie îndeplinite pentru ca personalul de întreținere și aparatura specifică a acestuia să poată fi introduse în zona de operare a unui SPAD și/sau RTD (SIC); personalul de întreținere trebuie să dețină certificate de securitate, deoarece prin executarea operațiunilor de întreținere există posibilitatea de a accesa informații clasificate NATO.

254. Cerințele menționate la pct. 75 trebuie stipulate foarte clar în CSS, iar procedurile de desfășurare a activității respective trebuie stabilite în PrOpSec. Nu se acceptă tipurile de întreținere care constau în aplicarea unor proceduri de diagnosticare ce implică accesul de la distanță la sistem, decât dacă activitatea respectivă se desfășoară sub control strict și numai cu aprobarea AAS.

255. Achiziționarea de sisteme SIC este limitată pe cât posibil la cele proiectate și realizate în țări membre NATO. Hardware și/sau software proiectate și/sau realizate în țări ce nu sunt membre NATO pot fi achiziționate numai după aprobarea AAS.

256. Pentru SIC care stochează, procesează și/sau transmit informații clasificate NATO, de la nivelul SECRET în sus, și/sau informații din Categoria Specială respectivele sisteme SIC sau componentele lor de bază (cum ar fi: sisteme de operare de scop general, produse de limitare a funcționării în scopul realizării securității și produse pentru comunicare în rețea) se pot achiziționa doar dacă sunt sau urmează să fie evaluate și certificate de către AAS, conform criteriilor NATO (AC/35 — D/1012 revăzut) sau criteriilor naționale echivalente.

257. Pentru SIC care stochează, procesează și/sau transmite informații clasificate NATO CONFIDENTIAL sistemele și componentele lor de bază vor respecta pe cât posibil criteriile prevăzute la pct. 256.

258. Decizia de a prefera închirierea în loc de cumpărarea unui echipament, în special medii de stocare, trebuie luată ținându-se seama de faptul că astfel de echipamente, o dată utilizate pentru stocarea sau procesarea informațiilor clasificate NATO, nu mai pot fi scoase în medii neprotejate fără a fi în prealabil declasificate, conform aprobării AAS, și de faptul că acest lucru nu este întotdeauna posibil.

259. Toate SPAD și/sau RTD (SIC), înainte de a fi utilizate pentru stocarea, procesarea sau transmiterea informațiilor clasificate de la categoria NATO CONFIDENTIAL în sus, trebuie acreditate de către AAS pe baza datelor furnizate de către CSS, PrOpSec și de alte documentații relevante. Subsistemele SPAD și/sau RTD și stațiile de lucru cu acces la distanță sau terminalele vor fi acreditate ca parte integrantă a sistemelor SIC la care sunt conectate. În cazul în care un sistem SPAD și/sau RTD (SIC) deservește atât NATO, cât și organizațiile, structurile interne ale țării, acreditarea se va face de către ANS de comun acord cu autoritățile NATO de securitate.

260. Modul de operare de securitate multinivel impune în unele situații ca, înainte de acreditarea propriu-zisă a SPAD și/sau RTD (SIC), hardware, firmware și software să fie evaluate și certificate de către AAS, conform criteriilor stabilite la nivel NATO, în ceea ce privește posibilitatea acestora de a proteja informațiile NATO de toate categoriile și nivelurile de clasificare și de a deține mecanisme de partajare/clasificare a utilizatorilor, bazate pe autorizarea accesului la sisteme.

261. Cerințele de evaluare și certificare sunt incluse în planificarea sistemului SIC și sunt stipulate explicit în CSS imediat după ce modul de operare de securitate a fost stabilit.

262. Există următoarele situații în care se impun evaluarea și certificarea de securitate într-un mod de operare de securitate multinivel:

a) pentru SPAD și/sau RTD (SIC) care stochează/procesează/transmit informații clasificate NATO COSMIC TOP SECRET și/sau cele din Categorie Specială;

b) pentru SPAD și/sau RTD (SIC) care stochează, procesează sau transmit informații clasificate NATO SECRET, în următoarele cazuri:

(i) SPAD și/sau RTD (SIC) este interconectat cu un alt SPAD și/sau RTD (SIC);

(ii) SPAD și/sau RTD (SIC) are un număr de utilizatori posibili care nu poate fi definit exact.

263. Procesul de evaluare și certificare trebuie să se desfășoare conform principiilor/instrucțiunilor aprobate, evaluarea și certificarea făcându-se de către echipe formate din experți cu pregătire tehnică adecvată și autorizați corespunzător, iar aceste echipe vor acționa ca reprezentanți ai AAS. Aceasta va selecta echipele de experți care urmează să realizeze evaluarea și certificarea.

264. Echipele pot fi formate din experți din cadrul AAS, din reprezentanți desemnați ai acestei autorități sau din experți din cadrul unor organisme specializate ale NATO.

265. În procesul de evaluare și certificare se va stabili în ce măsură un anumit SPAD și/sau RTD (SIC) îndeplinește condițiile de securitate specificate prin CSS. Este posibil ca după încheierea procesului de evaluare și certificare anumite secțiuni (paragrafe/capitole) din CSS să fie modificate sau actualizate. Procesul de evaluare și certificare trebuie să înceapă din stadiul de definire a SPAD și/sau RTD (SIC) și continuă de-a lungul întregului ciclu de implementare.

266. Gradul de evaluare și certificare poate fi redus în cazurile în care SPAD și/sau RDT (SIC) respective au la bază produse de securitate evaluate și certificate deja pe plan național.

267. Pentru toate SIC care stochează, procesează sau transmit informații clasificate NATO CONFIDENTIAL sau mai sus AOSIC stabilește proceduri de control care vor garanta că toate schimbările ulterioare intervenite în SIC sunt verificate în ceea ce privește implicațiile lor de securitate.

268. Tipurile de modificări care implică reacreditarea sau care solicită aprobarea anterioară a AAS trebuie să fie identificate cu claritate și expuse în CSS. După orice modificare, reparare sau eroare care ar fi putut afecta dispozitivele de securitate ale SIC, AOSIC trebuie să garanteze realizarea unei verificări care să asigure funcționarea corectă a dispozitivelor de securitate. Menținerea acreditării SIC trebuie să depindă de satisfacerea criteriilor de verificare.

269. Toate SIC care stochează, procesează sau transmit informații clasificate NATO CONFIDENTIAL sau mai sus sunt inspectate și reexaminate periodic de către AAS. Pentru SIC care stochează, procesează sau transmit informații clasificate NATO COSMIC TOP SECRET sau din categoria specială inspecția se va face cel puțin o dată pe an.

270. Microcalculatoarele sau calculatoarele personale având discuri fixe sau alte medii nevolatile de stocare a informației, operând autonom sau ca parte a unei rețele, precum și calculatoarele portabile cu discuri fixe sunt considerate medii de stocare a informațiilor în același sens ca și celelalte medii amovibile de stocare a informațiilor.

271. Acestor echipamente trebuie să li se acorde nivelul de protecție pentru acces, manipulare, stocare și transport, corespunzător cu cel mai înalt nivel de clasificare a informațiilor care au fost vreodată stocate sau procesate pe ele, până la declasarea sau declasificarea acestora în conformitate cu procedurile aprobate.

272. Este interzisă utilizarea mediilor de stocare amovibile, a software și hardware, aflate în proprietate privată, pentru stocarea, procesarea și transmiterea informațiilor clasificate NATO CONFIDENTIAL și mai sus. Pentru informațiile NATO RESTRICTED sau NATO UNCLASSIFIED se aplică reglementările naționale corespunzătoare.

273. Este interzisă introducerea mediilor de stocare amovibile, a software și hardware, aflate în proprietate privată, în zonele în care se stochează, se procesează sau se transmit informații clasificate NATO, fără aprobarea șefului unității.

274. Utilizarea echipamentelor și a software contractorilor în unități, în sprijinul activității oficiale NATO, este permisă cu aprobarea șefului unității. Utilizarea echipamentelor și software puse la dispoziție de alte instituții naționale poate fi permisă; în acest caz echipamentele sunt evidențiate în inventarul unității. În ambele situații, dacă echipamentele sunt folosite pentru stocarea, procesarea și transmiterea informațiilor clasificate NATO, trebuie obținut avizul de securitate al AAS locale.

275. Marcarea informațiilor cu destinație specială se aplică în mod obișnuit informațiilor clasificate care necesită o distribuție limitată și o manipulare specială, în plus față de caracterul atribuit, prin clasificarea de securitate (de exemplu: ATOMAL, US-SIOP-ESI, Crypto, EXCLUSIVE FOR etc.).

276. Definițiile furnizate la punctele următoare reprezintă concepte importante în terminologia specifică NATO și pot în unele cazuri să difere de definițiile vehiculate pe plan intern.

277. *Informație în formă electronică* reprezintă texte, date, imagini, sunete înregistrate pe suporturi magnetice, optice, electrice sau transmise, sub formă de curenți, tensiuni sau câmp electromagnetic, în eter sau în rețele de comunicații.

278. *Regula de lucru cu două persoane* („Two men rule“) presupune obligativitatea colaborării a două persoane pentru îndeplinirea unei activități specifice.

279. *Securitatea SPAD și/sau RTD (SIC)* reprezintă aplicarea măsurilor de securitate la SPAD și/sau RTD (SIC) cu scopul de a preveni sau împiedica atât extragerea și/sau modificarea informațiilor clasificate NATO stocate, procesate, transmise prin intermediul SPAD și/sau RTD (SIC) — prin interceptare, alterare, distrugere, accesare neautorizată cu mijloace electronice—, cât și invalidarea de servicii/funcții, prin mijloace specifice.

280. *Asigurarea securității SPAD și/sau RTD (SIC)* presupune aplicarea unui cumul de măsuri mixte: măsuri de securitate specifice SPAD și/sau RTD (respectiv, la nivel de calculator), măsuri de securitate din domeniul comunicațiilor, măsuri de ordin procedural, fizice, la nivel de personal și de securitate a documentelor.

281. *Securitatea calculatoarelor (COMPUSEC)* constă în aplicarea la nivel de calculator a facilităților de securitate hardware, software și firmware, pentru a preveni divulgarea, manevrarea, modificarea/ștergerea neautorizată a informațiilor sau invalidarea neautorizată a unor funcții.

282. *Produs informatic de securitate* reprezintă o componentă de securitate care se încorporează într-un SPAD și/sau RTD (SIC) și care servește la asigurarea, menținerea și sporirea confidențialității, integrității sau disponibilității/valabilității informațiilor.

283. *Securitatea comunicațiilor (COMSEC)* reprezintă aplicarea măsurilor de securitate în telecomunicații; scopul măsurilor este de a proteja mesajele dintr-un sistem de telecomunicații, care pot fi interceptate, studiate, analizate și care, prin reconstituire, pot conduce la dezvăluiri de informații clasificate.

COMSEC reprezintă un set complex de proceduri, incluzând:

a) măsuri de securitate a transmisiilor;

b) măsuri de securitate împotriva emisiilor (radiațiilor);

c) măsuri de acoperire criptologică;

d) măsuri de securitate fizică, procedurală, de personal și a documentelor;

e) măsuri COMPUSEC.

284. *TEMPEST* reprezintă măsuri de testare și de realizare a securității împotriva scurgerii de informații prin intermediul emisiilor electromagnetice parazite.

285. *Evaluarea* constă în examinarea detaliată, din punct de vedere tehnic și funcțional, a aspectelor de securitate ale SPAD și/sau RTD (SIC) sau a produselor de securitate, de către o autoritate abilitată în acest sens.

1. Prin procesul de evaluare se verifică prezența facilităților (funcțiilor) de securitate cerute, absența efectelor secundare compromițătoare care ar putea decurge din implementarea facilităților de securitate și se estimează funcționalitatea globală a sistemului de securitate.

2. Prin evaluare se constată în ce măsură cerințele de securitate specifice pentru un SPAD și/sau RTD (SIC) sunt satisfăcute. De asemenea, se evaluează performanțele de securitate ale produsului de securitate destinat calculatorului și se stabilește nivelul de încredere al SPAD și/sau RTD (SIC) sau al produsului de securitate implementat.

286. *Certificarea* constă în emiterea, în urma etapei de evaluare, a unui document de constatare, la care se atașează unul de analiză, în care sunt prezentate modul în care a decurs evaluarea și rezultatele acesteia; în documentul de constatare se menționează măsura în care SPAD și/sau RTD (SIC) verificate satisfac cerințele de securitate și măsura în care produsul de securitate destinat protecției acestora răspunde exigențelor în materie de securitate.

287. *Acreditarea* este etapa de acordare a autorizării și aprobării unui SPAD și/sau RTD (SIC) de a prelucra informații clasificate NATO, în spațiul/mediul operațional propriu. Etapa de acreditare trebuie să se desfășoare după ce s-au implementat toate procedurile de securitate și după ce s-a atins un nivel suficient de protecție a resurselor de sistem. Acreditarea se face în principal pe baza CSS și include următoarele:

a) o lucrare justificativă despre obiectivul acreditării sistemului; alte detalii cuprinse în lucrare: nivelul/nivelurile de clasificare a informațiilor care urmează să fie procesate și vehiculate, modul/modurile de operare protejată propuse;

b) o lucrare despre managementul riscurilor (modul de tratare/gestionare/rezolvare a riscurilor), în care se specifică pericolele și punctele vulnerabile, precum și măsurile adecvate de contracarare a acestora;

c) o descriere detaliată a procedurilor propuse, a facilităților de securitate destinate SPAD și/sau RTD (SIC). Această descriere va reprezenta elementul esențial pentru finalizarea procesului de acreditare;

d) planul de implementare și de întreținere a facilităților de securitate;

e) planul de desfășurare a etapelor de testare, evaluare și certificare a securității SPAD și/sau RTD (SIC);

f) certificatul și, acolo unde este necesar, elemente de acreditare suplimentare.

288. Prin *SPAD (sistem de prelucrare automată a datelor)* se înțelege un ansamblu de elemente interdependente, în care se includ: echipamentele de calcul, produsele software de bază și aplicative, metodele, procedeele și, dacă este cazul, personalul, organizate astfel încât să asigure îndeplinirea funcțiilor de stocare și prelucrare automată a informațiilor în formă electronică. Astfel de sisteme pot fi utilizate în aplicații specifice din domeniile: industrial, economic, militar, cercetare, proiectare, administrativ-organizatoric etc.

1. Pentru stabilirea limitelor până la care se întinde un SPAD, acesta se definește ca fiind un ansamblu de elemente care se află sub coordonarea și controlul unei singure autorități AOSIC.

2. Un SPAD poate să cuprindă subsisteme, iar unele dintre acestea pot fi ele însele SPAD.

289. *Facilitățile de securitate specifice unui SPAD* se referă la:

— funcții și caracteristici hardware/firmware/software;
— proceduri/moduri de operare;
— proceduri și mijloace de evidență;
— controlul accesului;
— definirea zonei de operare a SPAD;
— definirea zonei de operare a posturilor de lucru/a terminalelor la distanță;
— restricții impuse de politica de management;
— mijloace și structuri fizice, personal;
— mijloace de control ale comunicațiilor.

Toate acestea sunt necesare asigurării unui nivel acceptabil de protecție pentru informațiile clasificate care urmează să fie stocate sau procesate într-un SPAD.

290. *RTD* este un ansamblu de elemente interdependente, în care se includ: dispozitive și echipamente de comunicație, tehnică de calcul hardware și software, metode și proceduri pentru transmisie-recepție date, precum și pentru controlul rețelei. Dacă este cazul, este inclus și personalul aferent. Toate acestea sunt organizate astfel încât să asigure îndeplinirea funcțiilor de teletransmisie a

informațiilor în formă electronică între două sau mai multe SPAD (SIC) sau să permită interconectarea cu alte RTD. RTD poate utiliza serviciile unui singur sistem de comunicații sau ale mai multor sisteme de comunicații; mai multe RTD pot utiliza serviciile unuia și aceluiași sistem de comunicații.

291. *Facilitățile de securitate specifice unei RTD* sunt specifice și cuprind: rețeaua, împreună cu toate componentele și facilitățile auxiliare unei rețele (facilități de comunicații ale rețelei, mecanisme și proceduri de identificare și etichetare, controlul accesului, programe și proceduri de control și revizie), necesare pentru a asigura un nivel acceptabil de protejare pentru informațiile clasificate.

292. Structural un *sistem informatic și de comunicații (SIC)* reprezintă o conexiune alcătuită din cel puțin un SPAD și/sau o RTD. Prin intermediul SIC se stochează, se procesează și/sau se transmit informații sub formă electronică.

293. *Zona SPAD* reprezintă o zonă de lucru în care se găsesc și operează unul sau mai multe calculatoare, unități periferice locale și de stocare, mijloace de control și echipament specific de rețea și specific comunicațiilor. Zona SPAD nu include acea zonă separată în care sunt amplasate terminale, echipamente periferice sau stații de lucru la distanță, chiar dacă aceste echipamente sunt conectate la echipamentul central de calcul din zona SPAD.

294. *Zona terminal/stație de lucru* reprezintă o zonă, separată de zona SPAD, în care se găsesc:

— echipamentele periferice locale sau terminalele asociate echipamentului de calcul central;

— stațiile de lucru la distanță;

— echipamente de comunicații RTD.

J. STRUCTURA/FUNCȚIONARUL DE SECURITATE

295. Pentru implementarea măsurilor de securitate și organizarea activității specifice protecției informațiilor clasificate NATO, la nivelul fiecărui minister sau autorități administrative autonome și în structurile subordonate, care prin natura activității lor vehiculează informații clasificate NATO, se va desemna o structură/funcționar de securitate. Personalul care încadrează structura de securitate este desemnat în funcție de volumul activității specifice.

296. Desemnarea structurii/funcționarului de securitate este obligatorie în toate instituțiile, societățile, firmele, întreprinderile de stat sau private, care, prin natura activității lor sau prin contractele, acordurile, înțelegerile ce le încheie, vehiculează informații clasificate NATO.

297. Structura/funcționarul de securitate reprezintă punctul de contact dintre instituție și ANS.

298. Structura/funcționarul de securitate este numită/numit de către șeful instituției și se subordonează direct acestuia. Aceasta/acesta răspunde de aplicarea procedurilor și normelor de securitate pentru protecția informațiilor clasificate NATO în cadrul instituției respective, precum și în cele subordonate, pentru toate domeniile de securitate reglementate de ANS: organizarea securității, securitatea fizică, securitatea personalului, securitatea documentelor, securitatea industrială și INFOSEC.

299. Responsabilitatea pentru implementarea reglementărilor privind protecția informațiilor clasificate NATO revine șefului instituției respective, iar structura/funcționarul de securitate este principalul colaborator al acestuia și componentă executivă.

300. Conform reglementărilor privind accesul la informații clasificate NATO personalul care încadrează structura/funcționarul de securitate trebuie să dețină, anterior desemnării, certificat de securitate de tip A, corespunzător celui mai înalt nivel de clasificare a informațiilor clasificate NATO gestionate.

301. Responsabilitățile structurii/funcționarului de securitate sunt:

Responsabilități generale:

a) coordonează activitatea CSNR din instituția respectivă și din cele subordonate;

b) elaborează norme interne de aplicare a reglementărilor privind protecția informațiilor clasificate NATO;

c) monitorizează implementarea normelor interne de securitate a informațiilor clasificate NATO, precum și modul de respectare a acestora în cadrul instituției;

d) elaborează planul de securitate pentru protecția informațiilor clasificate NATO la nivelul instituției;

e) îl consiliază pe șeful instituției pentru toate aspectele privind securitatea informațiilor clasificate NATO;

f) îl informează pe șeful instituției cu privire la vulnerabilitățile, riscurile și încălcările reglementărilor de securitate și ANS și propune măsurile ce se impun pentru soluționarea acestora.

Responsabilități privind securitatea personalului:

a) asigură implementarea normelor interne privind securitatea personalului;

b) inițiază procesul de solicitare a eliberării certificatelor de securitate, din dispoziția șefului instituției;

c) are obligația să pună la dispoziție persoanei pentru care se solicită eliberarea certificatului de securitate formularul-tip corespunzător nivelului de acces solicitat;

d) acordă asistență în vederea completării formularelor de verificare, cu respectarea termenului de transmitere a solicitării;

e) acordă sprijinul necesar instituțiilor cu atribuții în efectuarea verificărilor asupra personalului ce urmează să aibă acces la informații clasificate NATO;

f) ține evidența actualizată a tuturor persoanelor din cadrul instituției, care au acces la informații clasificate NATO, o copie de pe certificatele de securitate tip A și ia măsurile necesare pentru revalidarea sau retragerea certificatelor de securitate;

g) reanalizează periodic și actualizează normele interne de implementare a reglementărilor privind protecția informațiilor clasificate NATO.

Responsabilități privind securitatea documentelor:

a) coordonează și urmărește punerea în aplicare a normelor interne privind securitatea documentelor clasificate NATO în cadrul instituției sale;

b) inspectează activitatea CSNR din instituție privind modalitățile de gestionare a informațiilor documentelor clasificate NATO;

c) pregătește și transmite către ANS solicitarea și documentația necesară înființării în cadrul instituției sale a unei CSNR.

Responsabilități privind securitatea fizică:

a) stabilește măsurile de securitate fizică pentru controlul accesului în zonele de securitate, pentru a preveni accesul persoanelor neautorizate;

b) verifică condițiile de securitate ale spațiilor, birourilor, încăperilor, containerelor, în care sunt manipulate sau păstrate informații clasificate NATO;

c) adoptă măsurile necesare pentru a asigura un nivel de protecție fizică corespunzător în toate încăperile în care se desfășoară activități în cadrul cărora sunt vehiculate informații clasificate NATO;

d) pregătește și execută programele de inspecție a măsurilor de securitate fizică în cadrul CSNR, din competență, și îl informează pe șeful instituției cu privire la vulnerabilitățile constatate;

e) realizează verificări inopinate ale sistemelor de protecție fizică;

f) stabilește planul de cooperare cu alte formațiuni cu responsabilități în asigurarea protecției fizice.

Responsabilitățile pe linia INFOSEC sunt prevăzute în cap. I „INFOSEC".

Responsabilitățile privind pregătirea personalului sunt prevăzute în cap. L „Pregătirea personalului".

K. ACTIVITATEA DE CONTROL

302. Controlul reprezintă activitatea de verificare a modului în care fiecare CSNR asigură protecția informațiilor clasificate NATO.

303. Activitatea de control se desfășoară în mod planificat, pe baza Planului unic de control.

304. Toate structurile și persoanele care gestionează informații clasificate NATO vor fi incluse în programe de control, urmând să fie notificate cu privire la obiectivele controlului.

305. Fiecare acțiune de control se va încheia printr-un raport de control întocmit de echipa care a efectuat acțiunea.

306. Activitatea de control are drept scop identificarea, eliminarea și contracararea oricăror riscuri de securitate care ar duce la compromiterea, divulgarea, distrugerea sau sustragerea informațiilor clasificate NATO.

307. Activitatea de control vizează structura/funcționarul de securitate, CSNR și personalul care are acces la informații clasificate NATO.

308. Finalitatea acțiunilor de control se constituie într-un ansamblu de măsuri și recomandări menit să asigure operaționalizarea și perfecționarea cadrului organizatoric și funcțional la toate structurile și nivelurile de activitate, cu responsabilități în protecția informațiilor clasificate NATO.

309. ANS organizează și coordonează acțiunile de control la nivel național.

310. ANS verifică implementarea recomandărilor și a măsurilor necesare realizării obiectivelor asumate, la nivelul CSNR direct subordonate.

311. Desemnarea experților care formează echipa de control și inspecție se face de către Consiliul de coordonare al ANS și se aprobă de președintele ANS.

312. Rolul coordonator al ANS se manifestă prin întocmirea Planului unic de control, precum și prin asumarea responsabilităților la nivel național, față de solicitările și activitățile de control ale Oficiului de Securitate NATO în România.

313. ANS va integra propunerile înaintate de structurile de securitate din subordine și de cele ale Oficiului de Securitate NATO, în vederea stabilirii, planificării și desfășurării tematicilor de control. Ca urmare a controalelor și ori de câte ori se constată fapte și elemente de disfuncționalitate care ar putea să reprezinte riscuri de securitate pentru protecția informațiilor clasificate NATO, ANS are obligația de a informa operativ Oficiul de Securitate NATO, concomitent cu întreprinderea, împreună cu structurile de securitate responsabile, a măsurilor necesare de contracarare/diminuare și evaluare a incidentelor de securitate constatate.

314. ANS va efectua controale, în conformitate cu Planul unic de control, la CSNR direct subordonate și va superviza activitățile desfășurate pe această linie de toate CSNR din Sistemul Național de Registre.

315. Anual sau ori de câte ori este nevoie ANS va întocmi o evaluare cu privire la rezultatele controalelor desfășurate, modul de implementare a măsurilor concrete de remediere a deficiențelor care au fost constatate și la modalitățile practice de eficientizare a activității de protecție a informațiilor clasificate NATO.

316. Pe baza Planului unic de control fiecare CSNR își va întocmi propriul Plan specific de control, care trebuie să se adreseze, în mod diferențiat, CSNR din subordine. Elaborarea tematicii, planificarea și raportarea acțiunilor de control prevăzute în Planul specific de control se înscriu în Planul unic de control, fiind adaptate la condițiile specifice fiecărei CSNR.

317. ANS va fi informată cu privire la rezultatele, propunerile și măsurile de eficientizare a activității de protecție a informațiilor clasificate NATO, stabilite la finalizarea acțiunilor de control.

318. În situația în care se evidențiază riscuri de securitate referitoare la compromiterea, divulgarea, distrugerea sau sustragerea unor informații clasificate NATO, se va efectua o investigație de securitate ale cărei rezultate vor fi comunicate ANS. Membrii comisiei de investigare vor fi desemnați de șeful structurii instituționale.

319. CSNR au obligația să țină evidența acțiunilor de control desfășurate, a domeniilor care au făcut obiectul controalelor, cât și a personalului care a fost verificat.

320. Planul unic de control se întocmește anual de către ANS, în conformitate cu atribuțiile în domeniu ale acesteia și în concordanță cu propunerile Oficiului de Securitate NATO.

321. Domeniile, tematica, etapele și formele de control sunt parte integrantă a acestui Plan unic de control și stau la baza întocmirii, la nivelul structurilor de securitate subordonate, a planurilor specifice de control.

322. Planul unic de control va fi aprobat de către președintele ANS în cadrul Consiliului de coordonare al ANS, iar responsabilitatea punerii în aplicare a măsurilor și activităților stabilite revine Secretariatului tehnic.

323. Pe baza Planului unic de control structura/funcționarul de securitate își va întocmi propriul plan specific de control, care se adresează, în mod diferențiat, CSNR din subordine.

324. Planul specific de control va fi aprobat de către șeful structurii instituționale din care face parte respectiva CSNR.

325. La finalizarea acțiunilor cuprinse în Planul specific de control structura/funcționarul de securitate va prezenta ANS în termen de două săptămâni rapoartele cu privire la controlul efectuat.

326. Acțiunile de control sunt planificate și anunțate, planificate și neanunțate, neplanificate, precum și datorate unor situații de urgență. Acestea pot lua forma unor:

1. controale de fond, care au drept obiectiv verificarea în plan organizatoric, structural și funcțional a activităților de protecție a informațiilor clasificate NATO;

2. controale tematice, care se realizează în baza unor tematici specifice și vizează unul sau mai multe domenii ale activității de securitate protectivă și/sau programe de pregătire și educație de securitate;

3. controale în situații de urgență, care se adresează strict verificării și soluționării unor evenimente/solicitări exprese transmise ANS sau structurii de securitate ca urmare a identificării unui risc de securitate.

L. PREGĂTIREA PERSONALULUI

327. Pregătirea personalului constituie o formă a educației de securitate, obligatorie pentru toate persoanele care gestionează sau vor gestiona informații clasificate NATO, și reprezintă activitatea specifică de informare și instruire pe linia protecției informațiilor clasificate NATO. Persoanele angajate în locuri de muncă unde sunt gestionate informații clasificate NATO și pentru care s-au eliberat certificate de securitate vor fi instruite înaintea începerii activității.

328. Activitatea de pregătire se efectuează planificat și are caracter permanent, în scopul prevenirii, contracarării și eliminării riscurilor de securitate, precum și a amenințărilor la adresa securității informațiilor clasificate NATO.

329. Pregătirea personalului se va realiza diferențiat, în funcție de atribuțiile personalului și de nivelul certificatului de securitate deținut.

330. Fiecare formă de pregătire se va înscrie în fișa individuală de pregătire a persoanei.

331. Pregătirea personalului urmărește înțelegerea și însușirea corectă a standardelor de securitate, precum și a modului de implementare eficientă a măsurilor de protecție a informațiilor clasificate NATO, în vederea eliminării disfuncțiilor.

332. În cadrul Planului unic de pregătire a personalului ANS stabilește tematici de pregătire pe domenii, forme și metode de desfășurare a activităților, diferențiate în funcție de atribuțiile personalului și de nivelul certificatului de securitate deținut, în strânsă colaborare cu structurile de securitate din cadrul instituțiilor care gestionează informații clasificate NATO.

333. Pentru stabilirea Planului unic de pregătire a personalului ANS conlucrează în permanență cu Oficiul de Securitate NATO.

334. ANS este responsabilă de realizarea informării publice și a educației de securitate, care se efectuează diferențiat, pe grupuri-țintă, și are drept scop conștientizarea și informarea la nivelul întregii societăți a necesității protecției informațiilor clasificate NATO.

335. Structura/funcționarul de securitate are rolul coordonator în întocmirea, implementarea și controlul modului de aplicare a propriilor programe de pregătire a personalului.

336. Structura/funcționarul de securitate va întocmi Planul specific de pregătire a personalului, înscris în Planul unic de pregătire a personalului, în baza căruia va organiza și va desfășura activități specifice de pregătire la nivelul structurii instituționale și al structurilor din subordinea acesteia.

337. Periodic structura/funcționarul de securitate va informa ANS asupra formelor de pregătire desfășurate și va comunica lista persoanelor care au participat la acestea.

338. Structura/funcționarul de securitate are obligația să țină o evidență a tuturor persoanelor din cadrul structurii instituționale, care au participat la forme de pregătire organizate de NATO, de structuri de securitate ale Alianței Nord-Atlantice sau la forme de pregătire organizate la nivel național.

339. Planul unic pe pregătire a personalului este întocmit și aprobat de ANS pe baza propunerilor înaintate de structurile de securitate din cadrul instituțiilor care gestionează informații clasificate NATO, a proiectelor bilaterale de cooperare internă și internațională și a propunerilor formulate de Oficiul de Securitate NATO. El se întocmește pentru o perioadă de un an și se transmite tuturor structurilor instituționale.

340. Planul specific de pregătire a personalului este elaborat la începutul fiecărui an de către fiecare structură instituțională, adaptat la condițiile proprii, pornind de la prevederile Planului unic de pregătire a personalului. Planul specific de pregătire a personalului va fi aprobat de către șeful structurii instituționale.

341. Trimestrial structurile instituționale vor informa ANS asupra modului de îndeplinire a Planului specific de pregătire a personalului și vor prezenta propuneri de acțiuni posibil să fie incluse în Planul unic de pregătire a personalului.

342. Pregătirea generală cuprinde obiectivele, sarcinile și responsabilitățile care revin fiecărei structuri, în vederea aplicării măsurilor de protecție a informațiilor clasificate NATO. La acest nivel sunt prezentate principiile generale de protecție a informațiilor clasificate NATO, modalitățile de implementare a prezentelor norme, formele și metodele de armonizare a acestora cu cerințele NATO în domeniu.

343. Pregătirea specifică se realizează în baza principiului nevoii de a ști (need to know), a domeniului de activitate specific, în funcție de nivelul certificatului de securitate deținut și de atribuțiile personalului.

344. Pregătirea individuală se realizează în mod obligatoriu de întregul personal care gestionează informațiile clasificate NATO, conform atribuțiilor specifice.

345. Tematica generală și cea specifică pot fi prezentate sub formă de lecții, informări, prelegeri, simpozioane, mese rotunde, grupuri de lucru, seminarii, ședințe demonstrative cu caracter aplicativ, discuții libere, care se pot finaliza prin verificări sau certificări ale nivelului cunoștințelor.

346. Activitățile de pregătire se desfășoară, pe baza Planului unic de pregătire a personalului, de către structurile de securitate, precum și de alte autorități, instituții, organizații guvernamentale sau neguvernamentale și organisme, care sunt autorizate de ANS să desfășoare astfel de activități, în baza unor protocoale încheiate cu acestea.

347. Pe plan extern, în baza acordurilor existente între ANS și instituții internaționale similare, precum și alte autorități, organizații guvernamentale sau neguvernamentale, organisme, structuri, care au ca domeniu de activitate protecția informațiilor clasificate NATO, se vor derula programe comune de pregătire.

348. Desemnarea persoanelor care vor participa la astfel de forme de pregătire se va realiza de către fiecare instituție, iar solicitarea va fi făcută prin intermediul structurii de securitate. Pentru formele de pregătire organizate de către ANS solicitarea va fi transmisă acesteia tot prin intermediul structurii instituționale.

349. Formele de pregătire vor fi organizate și susținute de către experții din cadrul Secretariatului tehnic al ANS, conform tematicilor cuprinse în Planul unic de pregătire a personalului.

350. ANS organizează, anual și ori de câte ori este nevoie, instruirea funcționarilor de securitate și a responsabililor CSNR.

351. Formele de pregătire vor fi organizate și susținute de către structura/funcționarul de securitate, conform tematicilor cuprinse în propriul plan specific de pregătire a personalului. La solicitarea structurilor/funcționarilor de securitate, experții ANS vor acorda consultată de specialitate.

A N E X E*)
la protecția informațiilor clasificate NATO în România

ANS – SECRET DE SERVICIU

ROMÂNIA

Secret de serviciu
(după completare)
Exemplar nr. ____

.....
Ministerul titular
.....
Instituția solicitantă
Nr. _____ din _____

AUTORITATEA NAȚIONALĂ DE SECURITATE

Domnului .....
Preşedinte al Autorității Naționale de Securitate

Vă rugăm să dispuneți declanşarea procedurii de verificare şi avizare în vederea eliberării Certificatului de securitate pentru:

Numele:	
Prenumele:	
Data naşterii:	
Locul:	
B.I. / Carte de identitate:	Sr. Nr.
Eliberat:	

Pentru certificat de securitate tip A:

Nivelul de acces: CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐

Pentru certificat de securitate tip B:

Nivelul de acces: CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐

Acțiunea şi locul:

Perioada:

Paşaport tip: DE SERVICIU ☐ DIPLOMATIC ☐

Seria: Nr: Data eliberării:

Anexat, vă transmitem formularele de verificare nr._____din___.___.___

ŞEFUL INSTITUȚIEI SOLICITANTE,

Numele:

Semnătura:

Data:

L.S.

ANS – SECRET DE SERVICIU

*) Anexele sunt reproduse în facsimil.

ANS – SECRET DE SERVICIU

ROMÂNIA

Secret de serviciu
(după completare)
Exemplar nr. .....

AUTORITATEA NAȚIONALĂ DE SECURITATE

Nr. _____ din _____

Domnului .....

Vă rugăm să declanşaţi procedura de verificare şi avizare în baza solicitării Nr._____ din_____ emisă de _____ în vederea eliberării Certificatului de securitate pentru:

Numele:
Prenumele:
Data naşterii:
Locul:
B.I. / Carte de identitate: Sr. Nr.
Eliberat de:
La data:

Certificat de securitate tip: **A**

Nivelul de acces: CONFIDENTIAL SECRET TOP SECRET

Certificat de securitate tip: **B**

Nivelul de acces: CONFIDENTIAL SECRET TOP SECRET

Anexăm formularele de verificare cu nr. .....din data .....

Preşedintele Autorităţii Naţionale de Securitate

Numele:

Semnătura:

Data:

ANS – SECRET DE SERVICIU

ANS – SECRET DE SERVICIU

ROMÂNIA

Secret de serviciu
(după completare)
Exemplar nr. _____

.....
Ministerul titular

.....
Instituţia solicitantă
Nr. _____ din _____

AUTORITATEA NAŢIONALĂ DE SECURITATE

Domnului .....
Preşedinte al Autorităţii Naţionale de Securitate

Vă notificăm declanşarea procedurii de verificare şi avizare în vederea eliberării Certificatului de securitate pentru:

Numele:
Prenumele:
Data naşterii:
Locul:
B.I. / Carte de identitate: Sr. Nr.
Eliberat:

Pentru certificat de securitate tip A:

Nivelul de acces: CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐

Pentru certificat de securitate tip B:

Nivelul de acces: CONFIDENTIAL ☐ SECRET ☐ TOP SECRET ☐

Acţiunea şi locul:

Perioada:

Paşaport tip: DE SERVICIU ☐ DIPLOMATIC ☐

Seria: Nr: Data eliberării:

ŞEFUL INSTITUŢIEI SOLICITANTE,

Numele:
Semnătura:
Data:

L.S.

ANS – SECRET DE SERVICIU

ANS - NESECRET

Nr. 1234

AUTORITATEA NAȚIONALĂ DE SECURITATE

CERTIFICAT DE SECURITATE TIP A

1. Prin prezentul se certifică:

Domnului / Doamnei:

Paul – Doru STĂNESCU

Data şi locul naşterii:

06 Decembrie 1973, Constanța, Județul Constanța

I se acordă Certificat de Securitate în conformitate cu prevederile Acordului de Securitate dintre ROMÂNIA şi NATO ca urmare a verificărilor de securitate, pentru acces la informaţii clasificate NATO, nivel NATO SECRET.

2. Valabilitate: **14.12.2001 - 14.12.2004.**

MIHNEA MOTOC,

Preşedintele Autorităţii Naţionale de Securitate *Ştampila*

Date: 14.12.2001

ANS - NESECRET

Nr. 2345 NATO/EAPC/PfP UNCLASSIFIED

CERTIFICATE OF SECURITY CLEARANCE

Issued by

.....

Date and Place of Issue
14.12. 2001, Bucharest

Valid until
01.01.2002 - 30.11.2002

This is to certify that:

Full Name
Paul – Doru STĂNESCU

Date of Birth
December 06, 1973

Place of Birth
Constanţa, Constanţa County

Where employed
Ministry of National Defence

Purpose and Duration of Visit
Appointed to the Defence Cooperation and Partnership Directorate, NATO HQ, Bruxelles, Belgium
01.01.2002 – 30.11.2002

Holder of Passport/Identity Card No. P - 034567
Issued at Ministry of Foreign Affairs
Dated: 07.10.1999
has been cleared for access to NATO/EAPC(PfP) information classified up to and including NATO/EAPC(PfP) SECRET in accordance with current NATO security requirements and has been briefed accordingly by National Security Authority of Romania.

Signed by: .....

Title: ..... *Official Government Stamp*

Date: 14.12. 2001

ANS – SECRET DE SERVICIU

ROMÂNIA

Secret de serviciu
(după completare)

.....
Instituția titulară

Exemplar nr. .....

Nr. _____ din _____

CERTIFICAT DE CURIER NR. .....

PENTRU TRANSPORTUL DE MÂNĂ AL DOCUMENTELOR ŞI AL ECHIPAMENTELOR CLASIFICATE NATO

Prin prezenta se certifică că purtătorul:

Domnul/Doamna: _____

Născut la data de __/___/_____, în: _____

Paşaport/carte de identitate sr.___ nr. _____

Emis de : _____ la data de : ___/___/____

Angajat al : _____

Însoțitor:

Domnul/Doamna: _____

Născut la data de __/___/_____, în: _____

Paşaport/carte de identitate sr.____nr. _____

Emis de : _____ la data de : ___/___/____

Angajat al : _____

este autorizat să transporte următoarele documente/materiale clasificate:

Nr. crt.	FELUL DOCUMENTULUI / MATERIALULUI	SERIA DOCUMENTULUI / MATERIALULUI	OBS.

ANS – SECRET DE SERVICIU

ANS – SECRET DE SERVICIU

INTINERARIU:

De la (originator): _____

La (destinatar): _____

Prin: _____

Puncte de oprire:

1. _____
2. _____
3. _____
4. _____
5. _____

Data începerii misiunii: ___/___/_____

Data terminării misiunii: ___/___/_____

Semnătura funcţionarului de securitate al instituţiei

_____
(nume)

Semnătura şefului instituţiei

_____
(nume)

Ştampila instituţiei

L.S.

Declar cu bună credinţă că, pe durata exercitării misiunii de curierat în baza prezentului mandat, nu mă voi implica în nici un fel de activităţi care să aibă ca rezultat compromiterea misiunii primite.

Semnătura curierului: _____

Semnătura însoţitorului: _____

Martor : _____
(funcţionarul de securitate al instituţiei)

Data depunerii Certificatului de curier: ___/___/_____

ANS – SECRET DE SERVICIU

REGISTRUL DOCUMENTELOR NATO/PfP DE CIRCULAȚIE LIMITATĂ *)

Nr. de referință	Nr. de înregistrare la R.C.	Data înregistrării	Nr. și data documentului de la NATO	Titlul și conținutul pe scurt al documentului	Nr. file	Caracterul **)	Persoana autorizată la care se află documentul (nume - semnătură)	Alte destinații ***)			Dosarul (fichetul) unde se află documentul sau nr. P.V. de distrugere
								instituții (1)	consultare (2)	copii (3)	

*) Registrul are în anexă: caietul de transmitere a documentelor (sau copii ale acestora) la alte instituții autorizate; evidența persoanelor autorizate care au mai consultat documentul; procesele-verbale de multiplicare sau de distrugere a documentului.

**) RESTRICTED (R), CONFIDENTIAL (C), SECRET (S)

***) Se referă la transmiterea documentului către alte instituții autorizate, consultarea documentului de către alte persoane autorizate sau efectuarea de copii. În fiecare coloană se menționează (după caz) numărul de referință (de ordine) din caietul de transmitere, numărul de referință din Evidența consultării sau numărul procesului-verbal în caz de multiplicare. Atunci când se transmit copii la o altă instituție autorizată se completează atât coloana 3 cât și 1.

ANEXA I

CAIET DE TRANSMITERE A DOCUMENTELOR NATO/PfP

Nr. de referință a transmiterii	Nr. de referință în registrul central (sub registru)	Nr. și data documentului	Nr. file	Data transmiterii	Instituția autorizată la care se transmite documentul	Persoana care a preluat documentul (nume și semnătură)

ANEXA II

EVIDENŢA CONSULTĂRII DOCUMENTELOR NACC/PfP

Nr. de ordine	Nr. de referinţă în registrul central (sub registru)	Nr. şi data documentului	Data consultării	Persoana autorizată care a consultat documentul			Persoana autorizată la care se află documentul	Persoana care a autorizat consultarea
				Nume	Instituţie	Semnătură		

Formular de bază - date personale

Nr._____ din___.___.___

SECRET DE SERVICIU
(după completare)

SPAȚIU REZERVAT INSTITUȚIEI SOLICITANTE

Instituţia solicitantă:

Tipul de certificat şi nivelul de acces solicitat:

A		CONFIDENTIAL		SECRET		TOP SECRET	
B		CONFIDENTIAL		SECRET		TOP SECRET	

Motivul solicitării:

Instituţia la care se trimite avizul: **AUTORITATEA NAȚIONALĂ DE SECURITATE**

DATE GENERALE DESPRE SOLICITANT

NUME:

NUME ANTERIOARE:

PRENUME:

DATA NAŞTERII:

LOCUL NAŞTERII: sat: comună:

oraş: judeţ:

CETĂŢENIA la naştere: actuală:

CARTE/BULETIN DE IDENTITATE:

Seria: Nr.: Eliberat de: La data:

Cod numeric personal:

DOMICILIUL PERMANENT:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILII PERMANENTE ŞI FLOTANTE ÎN ULTIMII CINCI ANI:

Tipul de domiciliu: Permanent: Flotant:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

.....

Tipul de domiciliu: Permanent: Flotant:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

ADRESE ŞI REŞEDINŢE ÎN STRĂINĂTATE ÎN ULTIMII CINCI ANI:
(pentru perioade peste 3 luni)

Perioada: Ţara: Ţara: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

.....

Perioada: Ţara: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

STUDII CIVILE ŞI MILITARE:

Nr.crt.	Perioada	Instituţia emitentă	Felul studiilor

LIMBI STRĂINE CUNOSCUTE

Nr.crt.	Limba	Nivelul

(în cazul atestatelor se va indica instituţia emitentă şi data)

SITUAȚIA MILITARĂ:

Fără stagiu militar satisfăcut: ☐ Militar activ: ☐ În rezervă: ☐

Seria livretului militar: _____ Numărul livretului militar: _____

Eliberat de centrul militar: _____ la data: _____

PAȘAPOARTE:

Turistic
Seria: ☐ Numărul: _____ Eliberat de: _____ La data: _____

De serviciu
Seria: ☐ Numărul: _____ Eliberat de: _____ La data: _____

Diplomatic
Seria: ☐ Numărul: _____ Eliberat de: _____ La data: _____

CĂLĂTORII ÎN STRĂINĂTATE ÎN ULTIMII CINCI ANI:

Nr.crt.	Țara	Localitatea	Perioada	Scopul

SITUAŢIA PROFESIONALĂ:

CIVIL:

Profesia:

Ministerul:

Instituţia la care este încadrat:

De la data:

Funcţia:

De la data:

Adresa de la locul de muncă:

Telefon: Fax: E-mail:

MILITAR:

Gradul: Funcţia:

Arma de bază: Arma de încadrare:

Unitatea:

Indicativul eşalonului superior:

LOCURI DE MUNCĂ ÎN ULTIMII CINCI ANI:

Nr.crt.	INSTITUŢIA	PERIOADA	FUNCŢII DEŢINUTE

SITUAŢIA FAMILIALĂ ACTUALĂ

Celibatar(ă): ☐ Căsătorit(ă): ☐ Concubinaj ☐

Despărţit(ă) în fapt: ☐ Divorţat(ă): ☐ Văduv(ă) ☐

Recăsătorit(ă): ☐

Alte situaţii:

Date referitoare la data şi locul încheierii căsătoriei sau legate de situaţia actuală

DATE DESPRE PARTENERUL DE VIAŢĂ (SOŢ / SOŢIE, CONCUBIN / CONCUBINĂ)

NUME:

NUME ANTERIOARE:

PRENUME:

DATA NAŞTERII:

LOCUL NAŞTERII: comună: oraş: judeţ:

CETĂŢENIA: la naştere: actuală:

PROFESIA:

LOCUL DE MUNCĂ:

DOMICILIUL PERMANENT:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILII PERMANENTE ŞI FLOTANTE ÎN ULTIMII CINCI ANI:

Tipul de domiciliu: Permanent: ☐ Flotant: ☐

Localitatea: ☐ Judeţul/Sectorul: ☐

Strada: ☐ Numărul: ☐ Bloc: ☐

Scara: ☐ Etajul: ☐ Apartamentul: ☐ Codul poştal: ☐

.....

Tipul de domiciliu: Permanent: ☐ Flotant: ☐

Localitatea: ☐ Judeţul/Sectorul: ☐

Strada: ☐ Numărul: ☐ Bloc: ☐

Scara: ☐ Etajul: ☐ Apartamentul: ☐ Codul poştal: ☐

.....

Tipul de domiciliu: Permanent: ☐ Flotant: ☐

Localitatea: ☐ Judeţul/Sectorul: ☐

Strada: ☐ Numărul: ☐ Bloc: ☐

Scara: ☐ Etajul: ☐ Apartamentul: ☐ Codul poştal: ☐

COPII (inclusiv cei din alte căsătorii)

Nr.crt.	NUMELE ŞI PRENUMELE	DATA NAŞTERI	LOCUL	OCUPAŢIA	DOMICILIUL

DATE DESPRE PĂRINȚI

TATĂL

NATURA RELAȚIEI: tată natural: ☐ tată adoptiv: ☐ tată vitreg: ☐

NUME:

NUME ANTERIOARE:

PRENUME:

PROFESIA:

DATA NAȘTERII:

LOCUL NAȘTERII: comună: oraș: județ:

CETĂȚENIA la naștere: actuală:

DOMICILIUL PERMANENT:

Localitatea: Județul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poștal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Județul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poștal:

Telefon fix: Telefon mobil:

Fax: E-mail:

MAMA

NATURA RELAȚIEI: mamă naturală: ☐ mamă adoptivă: ☐ mamă vitregă: ☐

NUME:

NUME ANTERIOARE:

PRENUME:

PROFESIA:

DATA NAȘTERII:

LOCUL NAȘTERII: comună: oraș: județ:

CETĂȚENIA la naștere: actuală:

DOMICILIUL PERMANENT:

Localitatea: Județul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poștal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Județul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poștal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DATE DESPRE FRAȚI/SURORI

NUME:

PRENUME:

DATA ŞI LOCUL NAŞTERII:

DOMICILIUL:

NUME:

PRENUME:

DATA ŞI LOCUL NAŞTERII:

DOMICILIUL:

NUME:

PRENUME:

DATA ŞI LOCUL NAŞTERII:

DOMICILIUL:

NUME:

PRENUME:

DATA ŞI LOCUL NAŞTERII:

DOMICILIUL:

ANTECEDENTE ŞI CAZIER

Aţi fost vreodată reţinut, arestat preventiv, anchetat, pus sub acuzare, judecat, condamnat (inclusiv la amendă penală sau interzicerea unor drepturi), graţiat, amnistiat, eliberat pe cauţiune, eliberat condiţionat?

DA ☐ NU ☐

Aţi fost vreodată anchetat administrativ, sancţionat administrativ, amendat de către poliţie sau autorităţi civile (**nu** se menţionează amenzile pentru abateri minore, cum sunt cele pentru parcare, dar se menţionează cele pentru fapte grave, precum conducerea sub influenţa alcoolului sau tulburarea ordinii publice)?

DA ☐ NU ☐

Aţi fost vreodată judecat în Consiliul de Onoare, anchetat, judecat sau condamnat de o Curte Marţială, trimis într-o unitate disciplinară în timpul cât v-aţi aflat în serviciul militar?

DA ☐ NU ☐

Dacă aţi răspuns cu **da** la vreuna din întrebările de mai sus, detaliaţi în spaţiul de mai jos, inclusiv perioadele şi instituţiile care au sancţionat faptele dvs..[1]

Nr.crt.	FAPTA SĂVÂRŞITĂ	PERIOADA	INSTITUŢIA

[1] Datele furnizate vor fi tratate cu maximum de confidenţialitate. Autoritatea care acordă avizul va decide dacă faptele comise au vreo relevanţă la acordarea certificatului de securitate. Nu este obligatoriu ca aceste fapte să determine refuzul de acordare a certificatului. În acelaşi timp, ascunderea totală sau parţială a unor astfel de informaţii şi circumstanţe este considerată drept dovadă de nesinceritate cu consecinţe grave în planul securităţii personale şi, ca atare, determinantă la luarea deciziei privind avizul.

DATE DE SECURITATE

	Solicitantul	Partenerul de viață
Ați fost vreodată implicat în acțiuni de: spionaj, terorism, tentative de subminare a ordinii democratice prin mijloace violente?	DA ☐ NU ☐	DA ☐ NU ☐
Ați fost vreodată membru sau simpatizant al unei grupări implicate în acțiuni menționate mai sus?	DA ☐ NU ☐	DA ☐ NU ☐
Ați fost vreodată în relații apropiate cu o persoană care a activat sau a simpatizat cu astfel de grupări?	DA ☐ NU ☐	DA ☐ NU ☐

Dacă ați răspuns cu **da** la vreuna dintre întrebări detaliați mai jos.

	Solicitantul	Partenerul de viață
Ați colaborat cu organele fostei Securități care au desfășurat activități de poliție politică?	DA ☐ NU ☐	DA ☐ NU ☐
Considerați că ați atras atenția vreunui serviciu de informații sau de securitate străin?	DA ☐ NU ☐	DA ☐ NU ☐
Considerați că au fost făcute presiuni asupra dumneavoastră sau asupra membrilor familiei dumneavoastră ca urmare a unui incident survenit pe teritoriul altei țări?	DA ☐ NU ☐	DA ☐ NU ☐
Sunteți în relații permanente de natură profesională sau personală cu cetățeni străini?	DA ☐ NU ☐	DA ☐ NU ☐
Considerați că vi s-a solicitat vreodată să furnizați informații clasificate în afara atribuțiilor de serviciu?	DA ☐ NU ☐	DA ☐ NU ☐

Dacă aţi răspuns cu **da** la vreuna dintre întrebări detaliaţi mai jos.

	Solicitantul	Partenerul de viaţă
Aveţi rude apropiate, din cele menţionate mai sus, care locuiesc în străinătate sau care au locuit mai mult de trei luni în străinătate?	DA ☐	DA ☐
	NU ☐	NU ☐

Dacă aţi răspuns cu **da** detaliaţi mai jos.

Nr.crt.	NUMELE PRENUMELE	GRADUL DE RUDENIE	ŢARA	PERIOADA

DECLARAŢIE

Subsemnatul,.....

Declar că toate datele furnizate mai sus sunt exacte şi corecte;

Declar că am luat cunoştinţă de cerinţele procedurii de verificare şi avizare pentru acces la informaţiile clasificate N.A.T.O şi le accept;

Consimt ca toate datele pe care le furnizez să fie verificate, conştient fiind de consecinţele legale ale declaraţiilor false sau omisiunilor cu bună ştiinţă;

Mă angajez să furnizez orice date suplimentare care îmi vor fi solicitate în eventualitatea unor neclarităţi, precum şi să informez, din proprie iniţiativă, asupra oricărei modificări apărute în cele declarate mai sus.

Am luat notă că neacordarea avizului de securitate nu-mi va fi motivată.

Data,

Semnătura,

FORMULAR SUPLIMENTAR

(se completează pentru niveluri
NATO SECRET şi NATO TOP SECRET)
Nr._____din___.___.____

SECRET DE SERVICIU

(după completare)
Ex. unic

SPAŢIU REZERVAT INSTITUŢIEI SOLICITANTE

Instituţia solicitantă: ☐

Tipul de certificat şi nivelul de acces solicitat:

A	☐	CONFIDENTIAL	☐	SECRET	☐	TOP SECRET	☐
B	☐	CONFIDENTIAL	☐	SECRET	☐	TOP SECRET	☐

Motivul solicitării: ☐

Instituţia la care se trimite avizul: **AUTORITATEA NAŢIONALĂ DE SECURITATE**

CANDIDATUL LA AVIZARE

NUME: ☐

PRENUME: ☐

DATA NAŞTERII: ☐

LOCUL NAŞTERII: sat: ☐ comună: ☐

oraş: ☐ judeţ: ☐

CETĂŢENIA actuală: ☐

DATA COMPLETĂRII FORMULARULUI DE BAZĂ: ☐

DATE SUPLIMENTARE DESPRE SOLICITANT

În afara domiciliilor, adreselor şi reşedinţelor indicate în formularul de bază, în ultimii zece ani aţi mai avut şi altele?

ÎN ROMÂNIA

Perioada: Judeţ: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

.....

Perioada: Judeţ: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

.....

Perioada: Judeţ: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poştal:

ÎN STRĂINĂTATE

Perioada: Țara: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul poștal:

.....

Perioada: Țara: Localitatea

Strada: Numărul: Bloc

Scara: Etajul: Apartamentul: Codul poștal:

.....

Perioada: Țara: Localitatea

Strada: Numărul: Bloc

Scara: Etajul: Apartamentul: Codul poștal:

.....

Perioada: Țara: Localitatea

Strada: Numărul: Bloc

Scara: Etajul: Apartamentul: Codul poștal:

RUDE

Cumnați/cumnate

GRAD DE RUDENIE				
NUMELE ACTUAL				
NUMELE LA NAȘTERE				
NUME ANTERIOARE				
PRENUMELE				
DATA NAȘTERII				
LOCUL NAȘTERII				
CETĂȚENIA ACTUALĂ				
DOMICILIUL PERMANENT				
OCUPAȚIA ACTUALĂ				

Părinții partenerului de viață (naturali, vitregi sau adoptivi).

	TATĂL		MAMA	
GRADUL DE RUDENIE				
NUMELE ACTUAL				
NUMELE LA NAȘTERE				
NUME ANTERIOARE				
PRENUMELE				
DATA NAȘTERII				
LOCUL NAȘTERII				
CETĂȚENIA ACTUALĂ				
DOMICILIUL PERMANENT				
OCUPAȚIA ACTUALĂ				

REFERINŢE

Nominalizaţi date de identificare a minim două persoane, care sunt de acord să prezinte referinţe despre dumneavoastră, care vă cunosc de cel puţin cinci ani.

Numele şi prenumele	Ocupaţia	Locul de muncă	Domiciliul permanent	Tel/Fax	Observaţii

STARE DE SĂNĂTATE

Aţi fost vreodată diagnosticat cu boală psihică?
Dacă răspunsul este afirmativ, detaliaţi:

Aţi suferit incidente de natură medicală care au provocat pierderea temporară a cunoştinţei?
Dacă răspunsul este afirmativ, detaliaţi:

Sunteţi conştient de vreo altă problemă medicală, neacoperită de răspunsurile anterioare, care ar putea afecta protecţia informaţiile clasificate?
Dacă răspunsul este afirmativ, detaliaţi:

Aţi avut sau aveţi probleme legate de consumul de alcool?
Dacă răspunsul este afirmativ, detaliaţi:

Aţi consumat sau consumaţi substanţe care creează dependenţă sau droguri?
Dacă răspunsul este afirmativ, detaliaţi:

DECLARAŢIE

Subsemnatul,.....

Declar că toate datele furnizate mai sus sunt exacte şi corecte;

Declar că am luat cunoştinţă de cerinţele procedurii de verificare şi avizare pentru acces la informaţiile clasificate N.A.T.O şi le accept;

Consimt ca toate datele pe care le furnizez să fie verificate, conştient fiind de consecinţele legale ale declaraţiilor false sau omisiunilor cu bună ştiinţă;

Mă angajez să furnizez orice date suplimentare care îmi vor fi solicitate în eventualitatea unor neclarităţi, precum şi să informez, din proprie iniţiativă, asupra oricărei modificări apărute în cele declarate mai sus.

Am luat notă că neacordarea avizului de securitate nu-mi va fi motivată.

Data,

Semnătura,

Formular financiar

Ex. nr._____din___.___.___

SECRET DE SERVICIU
(după completare)
Ex. unic

SPAŢIU REZERVAT INSTITUŢIEI SOLICITANTE

Instituţia solicitantă:

Tipul de certificat şi nivelul de acces solicitat:

A		SECRET		STRICT SECRET		S.S.I.D.	
B		CONFIDENTIAL		SECRET		TOP SECRET	

Motivul solicitării:

Instituţia la care se trimite avizul: **AUTORITATEA NAŢIONALĂ DE SECURITATE**

DATE GENERALE DESPRE SOLICITANT

NUME:

NUME ANTERIOARE:

PRENUME:

DATA NAŞTERII:

LOCUL NAŞTERII: sat: comună:

oraş: judeţ:

CETĂŢENIA actuală:

SITUAȚIA FAMILIALĂ

➢ Cum vă apreciați situația financiară ?

Confortabilă: ☐ Acceptabilă: ☐ Dificilă: ☐ Nu pot aprecia: ☐

Locuință

➢ Locuința pe care o folosiți împreună cu ceilalți membri ai familiei este:

Proprietate: ☐ Chirie: ☐ Locuință de serviciu: ☐

PROPRIETĂȚI MOBILE/IMOBILE

➢ Detaliati:

Venituri și cheltuieli lunare tipice pentru dumneavoastră și partenerul de viață

➢ Venit anual net realizat în urma activității principale.

➢ Venituri suplimentare realizate din alte activități

➢ Total venituri anuale pe gospodărie.

➢ Evaluați care este valoarea totală a debitelor curente care vă grevează

Dumneavoastră și partenerul dumneavoastră de viață economisiți

Curent ☐ Ocazional ☐ Rar ☐

Comparativ cu anul anterior aveți obligații și datorii financiare:

Mai mult: ☐ Mai puțin ☐ Cam la fel: ☐

Sunteți interesat, dvs. sau partenerul de viață în colaborarea cu anumite societăți comerciale înregistrate în țară? DA ☐ NU ☐

Dacă da, detaliați:

- denumirea societății comerciale, adresa, domeniul de activitate
- caracterul interesului (asociere, membru în Consiliul de administrație, consilier etc.)

Aveți relații, dvs. sau partenerul de viață cu firme înregistrate în străinătate? DA ☐ NU ☐

Dacă da, detaliați:

- denumirea firmei, adresa, domeniul de activitate
- caracterul interesului (asociere, membru în Consiliul de administrație, consilier, contracte de colaborare, concesionare, comision etc.)
- țara de înmatriculare.

Împotriva dvs. sau a asociaților dvs. au fost inițiate, în ultimii 10 ani, proceduri de executare silită? DA ☐ NU ☐

Dacă da, detaliați:

- motivul procedurii
- tribunalul care a hotărât măsura
- autoritatea care a pus-o în aplicare

Aveți alte interese financiare care ar putea intra în conflict cu îndatoririle dumneavoastră de serviciu? DA ☐ NU ☐

Detaliați.

Detaliați alte aspecte care ne-ar putea ajuta să înțelegem mai bine situația dumneavoastră financiară ?

DECLARAŢIE

Subsemnatul,.....

Declar că toate datele furnizate mai sus sunt exacte şi corecte;

Declar că am luat cunoştinţă de cerinţele procedurii de verificare şi avizare pentru acces la informaţiile clasificate N.A.T.O şi le accept;

Consimt ca toate datele pe care le furnizez să fie verificate, conştient fiind de consecinţele legale ale declaraţiilor false sau omisiunilor cu bună ştiinţă;

Mă angajez să furnizez orice date suplimentare care îmi vor fi solicitate în eventualitatea unor neclarităţi, precum şi să informez, din proprie iniţiativă, asupra oricărei modificări apărute în cele declarate mai sus.

Am luat notă că neacordarea avizului de securitate nu-mi va fi motivată.

Data,

Semnătura,

GUVERNUL ROMÂNIEI

H O T Ă R Â R E
privind înființarea, organizarea și funcționarea Agenției de Acreditare de Securitate, Agenției de Securitate pentru Informatică și Comunicații și Agenției pentru Distribuirea Materialului Criptografic

În temeiul prevederilor art. 107 din Constituția României,

Guvernul României adoptă prezenta hotărâre.

Art. 1. — (1) Se înființează Agenția de Acreditare de Securitate, denumită în continuare *AAS*, Agenția de Securitate pentru Informatică și Comunicații, denumită în continuare *ASIC*, și Agenția pentru Distribuirea Materialului Criptografic, denumită în continuare *ADMC*, ca structuri distincte în cadrul Autorității Naționale de Securitate, denumită în continuare *ANS.*

(2) Structurile înființate potrivit alin. (1) au competențe specifice pe linia stocării/procesării informațiilor clasificate NATO în cadrul sistemelor de prelucrare automată a datelor, respectiv transmise prin rețele de comunicații ale datelor.

Art. 2. — (1) AAS, ASIC și ADMC sunt direct subordonate directorului executiv al ANS.

(2) Schimbul de informații clasificate NATO cu celelalte structuri ale ANS și armonizarea reglementărilor se fac prin intermediul Secretariatului tehnic al ANS.

Art. 3. — (1) AAS, ASIC și ADMC exercită atribuții de reglementare, autorizare și control potrivit legii și standardelor NATO privind protecția informațiilor clasificate NATO în format electronic.

(2) AAS, ASIC și ADMC își desfășoară activitatea pe baza regulamentelor proprii de organizare și funcționare, care se aprobă de către președintele ANS, cu avizul Consiliului de coordonare al ANS.

Art. 4. — AAS are următoarele atribuții principale:

a) elaborează strategia de acreditare de securitate din cadrul politicii generale de securitate a ANS;

b) răspunde de evaluarea și certificarea sistemelor informatice și de comunicații sau a unor elemente componente ale acestora;

c) acordă acreditarea de securitate pentru sistemele informatice și de comunicații care stochează, procesează sau transmit informații clasificate NATO.

Art. 5. — ASIC are următoarele atribuții principale:

a) elaborează metodologii și proceduri specifice privind protecția informațiilor clasificate NATO care sunt stocate, procesate sau transmise prin intermediul sistemelor informatice și de comunicații, coordonează și controlează implementarea acestora;

b) analizează cauzele provocatoare de incidente de securitate și vulnerabilitățile din sistemele informatice și de comunicații, necesare pentru managementul riscurilor, asupra securității sistemelor respective, întreprinde măsuri operative de prevenire sau înlăturare a vulnerabilităților în domeniu.

Art. 6. — ADMC are următoarele atribuții principale:

a) asigură managementul materialelor și echipamentelor criptografice;

b) distribuie materiale și echipamente criptografice.

Art. 7. — (1) AAS, ASIC și ADMC sunt conduse de câte un director, care are în subordine un director adjunct pentru problematica de apărare, numiți de către președintele ANS la propunerea directorului executiv al ANS și cu avizul Consiliului de coordonare al acesteia.

(2) Directorii AAS, ASIC și ADMC reprezintă ANS în domeniul lor de competență.

(3) În cadrul AAS, ASIC și ADMC își vor desfășura activitatea experți din Ministerul Afacerilor Externe, Ministerul Apărării Naționale, Serviciul Român de Informații, Serviciul de Informații Externe, Ministerul de Interne, Serviciul de Telecomunicații Speciale, Serviciul de Protecție și Pază și Ministerul Comunicațiilor și Tehnologiei Informației.

Art. 8. — Directorii, directorii adjuncți și experții care își desfășoară activitatea în cadrul AAS, ASIC și ADMC sunt salarizați de către instituțiile de la care provin.

Art. 9. — (1) AAS, ASIC și ADMC își desfășoară activitatea în spațiile asigurate de către ANS.

(2) ANS asigură echipamentul de birotică adecvat, precum și celelalte dotări necesare desfășurării eficiente a activității.

(3) Cheltuielile aferente activității desfășurate de AAS, ASIC și ADMC se suportă din bugetul Ministerului Afacerilor Externe.

Art. 10. — (1) Prezenta hotărâre completează în mod corespunzător prevederile Hotărârii Guvernului nr. 864/2000 privind înființarea, organizarea și funcționarea Autorității Naționale de Securitate, publicată în Monitorul Oficial al României, Partea I, nr. 495 din 10 octombrie 2000.

(2) În termen de 60 de zile de la data intrării în vigoare a prezentei hotărâri AAS, ASIC și ADMC vor elabora regulamentele proprii de organizare și funcționare.

PRIM-MINISTRU
ADRIAN NĂSTASE

Contrasemnează:
p. Ministrul afacerilor externe,
Mihnea Motoc,
secretar de stat
p. Ministrul apărării naționale,
George Maior
secretar de stat
Directorul Serviciului Român de Informații,
Radu-Alexandru Timofte
p. Directorul Serviciului de Informații Externe,
Alexandru Marcel

București, 15 aprilie 2002.
Nr. 354.

Regia Autonomă
Monitorul Oficial
în pas cu timpul

Centrul pentru relaţii cu publicul
Şos. Panduri nr. 1, bloc P33, parter, sector 5, Bucureşti
Tel.: 411.58.33 Fax: 410.77.36
E-mail: multimed@bx.logicnet.ro
Website: www.monitoruloficial.ro

PROMPT, COMOD, MODERN ŞI UŞOR DE UTILIZAT

Prompt, comod, modern - prin **procurarea electronică** a Monitorului Oficial al României atât în sistem abonament, cât şi selectiv, a anumitor numere ale Monitorului Oficial al României sau acte normative.
Cu ajutorul unui **„motor de căutare"** se poate regăsi cu uşurinţă un act normativ din perioada 22 decembrie 1989 până la zi, după orice criteriu sau orice combinaţie de criterii de căutare, răspunsul foarte rapid constând în prezentarea actelor găsite – funcţie de criteriile de căutare selectate – cu menţionarea titlului actului şi a numărului monitorului în care a fost publicat.

ACCESIBILITATE

Preţul unui abonament **pe anul 2002** la Monitorul Oficial al României, **Partea I şi Partea I numere bis** - Legi, decrete, hotărâri şi alte acte - este de **192 USD** pentru un echipament de tip server sau monopost. În condiţiile în care dispuneţi de **reţea**, pentru fiecare utilizator final contravaloarea prestaţiei este de **8 USD/lună**, acordându-se o **reducere de 20%** pentru o reţea cu mai mult de cinci staţii de lucru.

OPERATIVITATE

Transmiterea Monitorului Oficial al României se face prin **e-mail**, **zilnic**, pe măsura apariţiei acestuia, intrându-se în posesia lui în ziua tipăririi. Fiecare Monitor Oficial este cuprins într-un fişier de tip PDF şi se citeşte cu Acrobat Reader, ceea ce înseamnă că pentru a recepţiona şi a utiliza informaţia legislativă vă este suficient contul de e-mail şi Acrobat Reader, aplicaţie ce se poate lua **gratuit** de pe Internet (www.adobe.com).

DIVERSITATE

Abonament **pe anul 2002** la Monitorul Oficial al României, **Partea I, în limba maghiară - 120 USD**

Abonament **pe anul 2002** la Monitorul Oficial al României, **Partea a II-a** - Dezbateri parlamentare - **190 USD**.

Abonament **pe anul 2002** la Monitorul Oficial al României, **Partea a III-a** - Publicaţii şi anunţuri - **60 USD**.

Abonament **pe anul 2002** la Monitorul Oficial al României, **Partea a IV-a** - Publicaţii ale agenţilor economici - **228 USD**.

Abonament **pe anul 2002** la Monitorul Oficial al României, **Partea a VI-a** - Achiziţii publice - **180 USD**.

Prin aceleaşi mijloace multimedia (e-mail, CD, dischete):

- **colecţia electronică a Monitorului Oficial** din perioada **1989-2001** (**312 USD**)
- **selecţii** Monitorul Oficial, Partea I, Partea a II-a, Partea a III-a, Partea a IV-a, Partea a V-a, Partea a VI-a (**0,08 USD/pag.**)
- versiunea electronică a lucrării "**Actele publicate în Monitorul Oficial al României, Partea I - 22 decembrie 1989 - 31 ianuarie 2001**" - lucrare ce cuprinde titlurile actelor normative publicate în perioada menţionată cu indicarea actelor normative ce au adus modificări şi/sau completări (**15 USD**)

Preţurile includ T.V.A.
Plata se face în lei, la cursul de schimb (B.N.R.) din ziua efectuării plăţii.

COLECŢII TEMATICE pe suport electronic

Legislaţie privind jocurile de noroc	2,3 USD
Legislaţie în domeniul asistenţei medicale	7,8 USD
Legislaţie privind normele de medicina muncii	3,5 USD
Legislaţie privind dezvoltarea regională a României şi regimul zonelor defavorizate*	3,7 USD
Legislaţia viei şi vinului*	4,3 USD
Reglementări privind circulaţia pe drumurile publice	2,3 USD
Legislaţie în domeniul silviculturii şi protecţiei vânatului*	9,1 USD
Legislaţie privind investiţiile directe şi dezvoltarea activităţii economice*	0,7 USD
Reglementări privind concesionările în domeniul sanitar-veterinar	1,4 USD
Impozitul pe venit	6,1 USD
Reglementări privind locuinţa – ediţia a II-a	7,8 USD
Sistemul public de pensii şi alte drepturi de asigurări sociale	3 USD
Circulaţia rutieră	20 USD

COLECŢII TRILINGVE pe suport electronic

	Preţ în USD/versiune			
	română	franceză	engleză	germană	rusă
Vol.19 - Legea protecţiei mediului	1,7	3,8	3,6		
Vol.20 - Reglementări privind locuinţele trecute în proprietatea statului	3,1	6,4	6,6		
Vol.22 - Organizarea şi funcţionarea Consiliului Legislativ	1,8	3,8	3,8		
Vol.25 - Legea privind dreptul de autor şi drepturile conexe	2,1	4,4	4,2		
Vol.26 - Lege privind procedura reorganizării şi lichidării judiciare*	1, 4	3	3		
Vol.27 - Lege privind desfăşurarea în siguranţă a activităţilor nucleare	1,1	2,5	2,4		
Vol.28 - Legea apelor	2,4	5,4	5,1		
Vol.29 - Lege privind organizarea şi funcţionarea Consiliului Economic şi Social	0,3		0,6		
Vol.30 - Lege privind desfăşurarea în siguranţă a activităţilor nucleare	1,1		2,5	2,5	
Vol.31 - Amenajarea teritoriului naţional*	0,5	1	1		
Vol.32 - Societăţi comerciale. Registrul comerţului*	3,6	7,8	7,7		
Vol.33 - Legislaţie bancară	2,9	6,2	6,2		
Vol.34 - Avocatul Poporului	1,4	2,8	2,9		
Vol.35 - Dezvoltarea regională în România	0,3	0,8	0,7		
Vol.37 - Proprietatea publică şi concesiunile	1	2,1	2,1		
Vol.38 - Prevenirea şi sancţionarea spălării banilor	0,4	0,8	0,8		
Vol.40 - Dezvoltarea regională în România şi regimul zonelor defavorizate*	4	8,4	8,3		
Vol.41 - Investiţii directe şi dezvoltarea activităţii economice*	0,8	1,6	1,5		
Vol.42 - Ordinea publică, apărarea şi siguranţa naţională	2	4,4	4,3		
Vol.43 - Consiliul Legislativ. Curtea Supremă de Justiţie	3,2	6,9	6,9		
Vol.44 - Accesul la propriul dosar şi deconspirarea securităţii ca poliţie politică	0,6	1,3	1,2		
Vol.46 - Reglementări privind administraţia publică locală şi alegerile locale	3,2	7,1	7,8		
Vol.47 - Asigurări şi reasigurări în România	0,6	1,2	1,1		
Vol.48 - Fondul funciar	7,2	15,3	14,8		
Vol.49 - Reglementări privind locuinţa	3,3	7,1	6,8		
Vol.50 - Alegeri parlamentare şi prezidenţiale	3,8	8,2	8,2		
Vol.51 - Societatea Română de Radiodifuziune şi Societatea Română de Televiziune	1	2,2	2,2		
Vol.52 - Prevenirea, descoperirea şi sancţionarea faptelor de corupţie	0,5	1	1		
Vol.53 - Reglementări privind corupţia şi crima organizată	1,3	2,8	2,8		
Vol.54 - Legislaţie privind privatizarea societăţilor comerciale din turism	0,7	1,4	1,4	1,4	
Vol.55 - Statutul funcţionarilor publici	2,1	4,4	4,2		
Vol.56 – Administraţia publică locală	4,1	8,5	8,5		
Vol.57 – Protecţia copilului	5,6	11,8	11,6		
Vol.58 – Regimul juridic al unor imobile preluate în mod abuziv	1,4	2,8	2,7		

* Întrucât modificările intervenite în cuprinsul actelor normative au avut loc după data prelucrării informaţiei, actualizarea acestora se va face într-o ediţie viitoare.

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAŢILOR

Regia Autonomă „Monitorul Oficial", str. Izvor nr. 2–4, Palatul Parlamentului, sectorul 5, Bucureşti,
cont nr. 2511.1—12.1/ROL Banca Comercială Română — S.A. — Sucursala „Unirea" Bucureşti şi nr. 5069427282 Trezoreria sector 5, Bucureşti (alocat numai persoanelor juridice bugetare).
Adresa pentru publicitate: Centrul pentru relaţii cu publicul, Bucureşti, şos. Panduri nr. 1, bloc P33, parter, sectorul 5, tel. 411.58.33 şi 411.97.54, tel./fax 410.77.36.
Tiparul : Regia Autonomă „Monitorul Oficial", tel. 490.65.52, 335.01.11/2178 şi 402.21.78,
E-mail: ramomrk@bx.logicnet.ro, Internet: www.monitoruloficial.ro