Guvernul Romaniei

Anexa

din 13/06/2002
Versiune actualizata la data de 24/03/2005

cuprinzand Standardele nationale de protectie a informatiilor clasificate in Romania@

_____
@Text actualizat la data de 24.03.2005. Actul include modificarile din urmatoarele acte:
- H.G. nr. 2202/2004
- H.G. nr. 185/2005.

CAPITOLUL I
DISPOZITII GENERALE

Art. 1. - Standardele nationale de protectie a informatiilor clasificate in Romania cuprind normele de aplicare a Legii nr. 182/2002 privind protectia informatiilor clasificate referitoare la:
a) clasificarile informatiilor secrete de stat si normele privind masurile minime de protectie in cadrul fiecarei clase;
b) obligatiile si raspunderile autoritatilor si institutiilor publice, ale agentilor economici si ale altor persoane juridice de drept public sau privat privind protectia informatiilor secrete de stat;
c) normele privind accesul la informatiile clasificate, precum si procedura verificarilor de securitate;
d) regulile generale privind evidenta, intocmirea, pastrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea si distrugerea informatiilor secrete de stat;
e) regulile de identificare si marcare, inscriptionarile si mentiunile obligatorii pe documentele secrete de stat, in functie de nivelurile de secretizare, cerintele de evidenta a numerelor de exemplare si a destinatarilor, termenele si regimul de pastrare, interdictiile de reproducere si circulatie;
f) conditiile de fotografiere, filmare, cartografiere si executare a unor lucrari de arte plastice in obiective sau locuri care prezinta importanta deosebita pentru protectia informatiilor secrete de stat;
g) regulile privitoare la accesul strainilor la informatiile secrete de stat;
h) protectia informatiilor clasificate care fac obiectul contractelor industriale secrete - securitatea industriala;
i) protectia surselor generatoare de informatii - INFOSEC.
Art. 2. - **(1)** Prezentele standarde instituie sistemul national de protectie a informatiilor clasificate, in concordanta cu interesul national, cu criteriile si recomandarile NATO si sunt obligatorii pentru toate persoanele juridice sau fizice care gestioneaza astfel de informatii.
(2) Echivalenta informatiilor nationale clasificate, pe niveluri de secretizare, cu informatiile NATO clasificate este:

a) Strict secret de importanta deosebita	- NATO top secret
b) Strict secret	- NATO secret
c) Secret	- NATO confidential
d) Secret de serviciu	- NATO restricted

Art. 3. - Termenii folositi in prezentele standarde au urmatorul inteles:
- Autoritate Desemnata de Securitate - ADS - institutie abilitata prin lege sa stabileasca, pentru domeniul sau de activitate si responsabilitate, structuri si masuri proprii privind coordonarea si controlul activitatilor

referitoare la protectia informatiilor secrete de stat. Sunt autoritati desemnate de securitate, potrivit legii Ministerul Apararii Nationale, Ministerul de Interne, Ministerul Justitiei, Serviciul Roman de Informatii, Serviciul de Informatii Externe, Serviciul de Protectie si Paza, Serviciul de Telecomunicatii Speciale;

- autorizatie de acces la informatii clasificate - document eliberat cu avizul institutiilor abilitate, de conducatorul persoanei juridice detinatoare de astfel de informatii, prin care se confirma ca, in exercitarea atributiilor profesionale, posesorul acestuia poate avea acces la informatii secrete de stat de un anumit nivel de secretizare, potrivit principiului necesitatii de a cunoaste;

- autorizatie de securitate industriala - document eliberat de Oficiul Registrului National al Informatiilor Secrete de Stat - ORNISS - unui obiectiv industrial, prin care se atesta ca este abilitat sa participe la procedura de negociere a unui contract clasificat;

- autorizatie speciala - document eliberat de catre ORNISS prin care se atesta verificarea si acreditarea unei persoane de a desfasura activitati de fotografiere, filmare, cartografiere si lucrari de arte plastice pe teritoriul Romaniei, in obiective, zone sau locuri care prezinta importanta deosebita pentru protectia informatiilor secrete de stat;

- aviz de securitate industriala - document eliberat de catre ADS prin care se atesta ca obiectivul industrial contractant a implementat toate masurile de securitate necesare protectiei informatiilor clasificate vehiculate in derularea contractului incheiat;

- certificat de securitate - document eliberat persoanei cu atributii nemijlocite in domeniul protectiei informatiilor clasificate, respectiv functionarului de securitate sau salariatului din structura de securitate, care atesta verificarea si acreditarea de a detine, de a avea acces si de a lucra cu informatii clasificate de un anumit nivel de secretizare;

- certificat de securitate industriala - document eliberat de ORNISS unui obiectiv industrial, prin care se atesta ca este abilitat sa deruleze activitati industriale si/sau de cercetare ce presupun accesul la informatii clasificate;

- clasificarea informatiilor - incadrarea informatiilor intr-o clasa si nivel de secretizare;

- contract clasificat - orice contract incheiat intre parti, in conditiile legii, in cadrul caruia se cuprind si se vehiculeaza informatii clasificate, contractant unitate industriala, comerciala, de executie, de cercetare-proiectare sau prestatoare de servicii in cadrul unui contract clasificat;

- contractor - parte dintr-un contract clasificat, care are calitatea de beneficiar al lucrarilor sau serviciilor executate de contractant;

- controlul informatiilor clasificate - orice activitate de verificare a modului in care sunt gestionate documentele clasificate;

- declasificare - suprimarea mentiunilor de clasificare si scoaterea informatiei clasificate de sub incidenta reglementarilor proiective prevazute de lege;

- diseminarea informatiilor clasificate - activitatea de difuzare a informatiilor clasificate catre unitati sau persoane abilitate sa aiba acces la astfel de informatii;

- document clasificat - orice suport material care contine informatii clasificate, in original sau copie, precum:

a) hartie - documente olografe, dactilografiate sau tiparite, schite, harti, planse, fotografii, desene, indigo, listing;

b) benzi magnetice, casete audio-video, microfilme;

c) medii de stocare a sistemelor informatice - dischete, compact-discuri, hard-discuri, memorii PROM si EPROM, riboane;

d) dispozitive de procesare portabile - agende electronice, laptop-uri - la care hard-discul este folosit pentru stocarea informatiilor;

- functionar de securitate - persoana care indeplineste atributiile de proiectie a informatiilor clasificate in cadrul autoritatilor, institutiilor publice, agentilor economici cu capital integral sau partial de stat si altor persoane juridice de drept public sau privat;

- gestionarea informatiilor clasificate - orice activitate de elaborare, luare in evidenta, accesare, procesare, multiplicare, manipulare, transport, transmitere, inventariere, pastrare, arhivare sau distrugere a informatiilor clasificate;

- incident de securitate - orice actiune sau inactiune contrara reglementarilor de securitate a carei consecinta a determinat sau este de natura sa determine compromiterea informatiilor clasificate;

- indicator de interdictie - text sau simbol care semnaleaza interzicerea accesului sau derularii unor activitati in zone, obiective, sectoare sau locuri care prezinta importanta deosebita pentru protectia informatiilor clasificate;

- informatie clasificata compromisa - informatie clasificata care si-a pierdut integritatea, a fost ratacita, pierduta ori accesata, total sau partial, de persoane neautorizate;

- institutie cu atributii de coordonare a activitatii si de control al masurilor privitoare la protectia informatiilor clasificate sau institutie abilitata - Ministerul Apararii Nationale, Ministerul de Interne, Ministerul Justitiei, Serviciul Roman de Informatii, Serviciul de Informatii Externe, Serviciul de Protectie si Paza, Serviciul de Telecomunicatii Speciale, potrivit competentelor stabilite prin lege;

- marcare - activitatea de inscriptionare a nivelului de secretizare a informatiei si de semnalare a cerintelor speciale de protectie a acesteia;

- material clasificat - document sau produs prelucrat ori in curs de prelucrare, care necesita a fi protejat

impotriva cunoasterii neautorizate;
- necesitatea de a cunoaste - principiul conform caruia accesul la informatii clasificate se acorda in mod individual numai persoanelor care, pentru indeplinirea indatoririlor de serviciu, trebuie sa lucreze cu astfel de informatii sau sa aiba acces la acestea;
- negocieri - activitatile circumscrise adjudecarii unui contract sau subcontract, de la notificarea intentiei de organizare a licitatiei, pana la incheierea acesteia;
- obiectiv industrial - unitate de cercetare sau cu activitate de productie, care desfasoara activitati stiintifice, tehnologice sau economice ce au legatura cu siguranta sau cu apararea nationala, ori prezinta importanta deosebita pentru interesele economice si tehnico-stiintifice ale Romaniei;
- obiectiv, sector sau loc de importanta deosebita pentru protectia informatiilor secrete de stat - incinta sau perimetru anume desemnat, in care sunt gestionate informatii secrete de stat;
- parte contractanta - oricare dintre partile care convin sa negocieze, sa incheie sau sa deruleze un contract clasificat;
- protectia surselor generatoare de informatii - ansamblul masurilor destinate protectiei informatiilor elaborate, stocate sau transmise prin sisteme ori retele de prelucrare automata a datelor si/sau de comunicatii;
- securitate industriala - sistemul de norme si masuri care reglementeaza protectia informatiilor clasificate in domeniul activitatilor contractuale;
- sistem de protectie a informatiilor clasificate - ansamblul de masuri de natura juridica, procedurala, fizica, de protectie a personalului si a surselor generatoare de informatii, destinate securitatii materialelor si documentelor clasificate;
- structura de securitate - compartiment specializat in protectia informatiilor clasificate, organizat in cadrul autoritatilor, institutiilor publice, agentilor economici cu capital integral sau partial de stat si al altor persoane juridice de drept public sau privat;
- subcontractant - parte care isi asuma executarea unei parti a contractului clasificat sub coordonarea contractantului;
- trecerea la un alt nivel de clasificare sau de secretizare - schimbarea clasificarii, respectiv a nivelului de secretizare a informatiilor secrete de stat;
- unitate detinatoare de informatii clasificate sau unitate - autoritate sau institutie publica, agent economic cu capital integral sau partial de stat ori o alta persoana juridica de drept public sau privat care, potrivit legii, are dreptul de a detine informatii clasificate;
- verificare de securitate - totalitatea masurilor intreprinse de autoritatile desemnate de securitate, conform competentelor, pentru stabilirea onestitatii si profesionalismului persoanelor, in scopul avizarii eliberarii certificatului de securitate sau autorizatiei de acces la informatii clasificate;
- zona de securitate - perimetru delimitat si special amenajat unde sunt gestionate informatii clasificate.

CAPITOLUL II
CLASIFICAREA SI DECLASIFICAREA INFORMATIILOR. MASURI MINIME DE PROTECTIE SPECIFICE CLASELOR SI NIVELURILOR DE SECRETIZARE

SECȚIUNEA 1
Clasificarea informatiilor

Art. 4. - **(1)** Potrivit legii, informatiile sunt clasificate secrete de stat sau secrete de serviciu, in raport de importanta pe care o au pentru securitatea nationala si de consecintele ce s-ar produce ca urmare a dezvaluirii sau diseminarii lor neautorizate.
(2) Informatiile secrete de stat sunt informatiile a caror divulgare poate prejudicia siguranta nationala si apararea tarii si care, in functie de importanta valorilor protejate, se includ in urmatoarele niveluri de secretizare prevazute de lege:
a) strict secret de importanta deosebita;
b) strict secret;
c) secret.
(3) Informatiile a caror divulgare este de natura sa determine prejudicii unei persoane juridice de drept public sau privat se clasifica secrete de serviciu.
Art. 5. - **(1)** Autoritatile publice care elaboreaza ori lucreaza cu informatii secrete de stat au obligatia sa intocmeasca un ghid pe baza caruia se va realiza clasificarea corecta si uniforma a acestora.
(2) Ghidul prevazut la alin (1) se aproba personal si in scris de catre imputernicitii sau, dupa caz, functionarii superiori abilitati sa atribuie nivelurile de secretizare, conform legii.
Art. 6. - Autoritatile si institutiile publice intocmesc liste proprii cuprinzand categoriile de informatii secrete de stat in domeniile lor de activitate, care se aproba si se actualizeaza prin hotarare a Guvernului.
Art. 7. - Listele cu informatii secrete de serviciu se stabilesc de conducatorii unitatilor detinatoare de astfel de informatii.
Art. 8. - In listele cu informatii secrete de serviciu vor fi incluse informatiile care se refera la activitatea unitatii si care, fara a constitui, in intelesul legii, secrete de stat, nu trebuie cunoscute decat de persoanele carora le sunt necesare pentru indeplinirea atributiilor de serviciu, divulgarea lor putand prejudicia interesul

unitatii.

Art. 9. - Unitatile care gestioneaza informatii clasificate au obligatia sa analizeze ori de cate ori este necesar listele informatiilor secrete de stat si, dupa caz, sa prezinte Guvernului spre aprobare propuneri de actualizare si completare a acestora, conform legii.

Art. 10. - Atribuirea clasei si nivelului de secretizare a informatiilor se realizeaza prin consultarea ghidului de clasificare, a listelor cu informatii secrete de stat si a listelor cu informatii secrete de serviciu, elaborate potrivit legii.

Art. 11. - Seful ierarhic al emitentului are obligatia sa verifice daca informatiile au fost clasificate corect si sa ia masuri in consecinta, cand constata ca au fost atribuite niveluri de secretizare necorespunzatoare.

Art. 12. - **(1)** Termenele de clasificare a informatiilor secrete de stat vor fi stabilite de emitent, in functie de importanta acestora si de consecintele care s-ar produce ca urmare a dezvaluirii sau diseminarii lor neautorizate.

(2) Termenele de clasificare a informatiilor secrete de stat, pe niveluri de secretizare, cu exceptia cazului cand acestea necesita o protectie mai indelungata, sunt de pana la:

- 100 de ani pentru informatiile clasificate strict secret de importanta deosebita;

- 50 de ani pentru informatiile clasificate strict secret;

- 30 de ani pentru informatiile clasificate secret.

(3) Termenele prevazute la alin (2) pot fi prelungite prin hotarare a Guvernului, pe baza unei motivatii temeinice, la solicitarea conducatorilor unitatilor detinatoare de informatii clasificate sau, dupa caz, a imputernicitilor si functionarilor superiori abilitati sa atribuie nivelurile de secretizare.

Art. 13. - Fiecare imputernicit ori functionar superior abilitat sa atribuie niveluri de secretizare va dispune verificarea periodica a tuturor informatiilor secrete de stat carora le-au atribuit nivelurile de secretizare, prilej cu care, daca este necesar, vor fi reevaluate nivelurile si termenele de clasificare.

Art. 14. - **(1)** Documentul elaborat pe baza prelucrarii informatiilor cu niveluri de secretizare diferite va fi clasificat conform noului continut, care poate fi superior originalelor.

(2) Documentul rezultat din cumularea neprelucrata a unor extrase provenite din informatii clasificate va primi clasa sau nivelul de secretizare corespunzator continutului extrasului cu cel mai inalt nivel de secretizare.

(3) Rezumatele, traducerile si extrasele din documentele clasificate primesc clasa sau nivelul de secretizare corespunzator continutului.

Art. 15. - Marcarea informatiilor clasificate are drept scop atentionarea persoanelor care le gestioneaza sau le acceseaza ca sunt in posesia unor informatii in legatura cu care trebuie aplicate masuri specifice de acces si protectie, in conformitate cu legea.

Art. 16. - Cazurile considerate supraevaluari ori subevaluari ale clasei sau nivelului de secretizare vor fi supuse atentiei emitentului, iar daca acesta decide sa reclasifice informatiile va informa detinatorii.

Art. 17. - **(1)** Informatiile vor fi clasificate numai in cazul in care se impune protectia acestora, iar nivelurile de secretizare si termenele de clasificare subzista atat timp cat dezvaluirea sau diseminarea lor neautorizata ar putea prejudicia siguranta nationala, apararea tarii, ordinea publica sau interesele persoanelor juridice de drept public sau privat.

(2) Supraevaluarea sau subevaluarea nivelului de secretizare a informatiilor si a duratei pentru care au fost clasificate se pot contesta de catre orice persoana fizica sau juridica romana, in contencios administrativ.

Art. 18. - **(1)** in termen de 12 luni de la intrarea in vigoare a prezentei hotarari, detinatorii de informatii secrete de stat si secrete de serviciu, stabilite astfel potrivit H.C.M. nr. 19 din 14 ianuarie 1972, vor prezenta persoanelor sau autoritatilor publice imputernicite sa atribuie niveluri de secretizare propuneri privind incadrarea acestor informatii in noi clase si niveluri de secretizare, dupa caz.

(2) Pana la stabilirea noilor niveluri de secretizare, informatiile secrete de stat si secrete de serviciu mentionate la alin. (1) isi pastreaza nivelul si termenul de secretizare si vor fi protejate potrivit prezentelor standarde.

SECȚIUNEA a 2-a

Declasificarea si trecerea informatiilor clasificate
la un nivel inferior de secretizare

Art. 19. - Informatiile secrete de stat pot fi declasificate prin hotarare a Guvernului, la solicitarea motivata a emitentului.

Art. 20. - **(1)** Informatiile se declasifica daca:

a) termenul de clasificare a expirat;

b) dezvaluirea informatiilor nu mai poate prejudicia siguranta nationala, apararea tarii, ordinea publica, ori interesele persoanelor de drept public sau privat detinatoare;

c) a fost atribuit de o persoana neimputernicita prin lege.

(2) Declasificarea sau trecerea la un alt nivel de secretizare a informatiilor secrete de stat se realizeaza de imputernicitii si functionarii superiori abilitati prin lege sa atribuie niveluri de secretizare, cu avizul prealabil al institutiilor care coordoneaza activitatea si controlul masurilor privitoare la protectia informatiilor clasificate, potrivit competentelor materiale.

(3) Emitentii documentelor secrete de stat vor evalua periodic necesitatea mentinerii in nivelurile de secretizare acordate anterior si vor prezenta imputernicitilor si functionarilor superiori abilitati prin lege sa atribuie niveluri de secretizare, propuneri in consecinta.

Art. 21. - Ori de cate ori este posibil, emitentul unui document clasificat trebuie sa precizeze daca acesta poate fi declasificat ori trecut la un nivel inferior de secretizare, la o anumita data sau la producerea unui anumit eveniment.

Art. 22. - **(1)** La schimbarea clasei sau nivelului de secretizare atribuit initial unei informatii, emitentul este obligat sa incunostinteze structura/functionarul de securitate, care va face mentiunile necesare in registrele de evidenta.

(2) Data si noua clasa sau nivel de secretizare vor fi marcate pe document deasupra sau sub vechea inscriptie, care va fi anulata prin trasarea unei linii oblice.

(3) Emitentul informatiilor declasificate ori trecute in alt nivel de clasificare se va asigura ca gestionarii acestora sunt anuntati la timp, in scris, despre acest lucru.

Art. 23. - **(1)** Informatiile clasificate despre care s-a stabilit cu certitudine ca sunt compromise sau iremediabil pierdute vor fi declasificate.

(2) Declasificarea se face numai in baza cercetarii prin care s-a stabilit compromiterea sau pierderea informatiilor respective ori a suportului material al acestora, cu acordul scris al emitentului.

Art. 24. - Informatiile secrete de serviciu se declasifica de conducatorii unitatilor care le-au emis, prin scoaterea de pe listele prevazute la art. 8, care vor fi reanalizate ori de cate ori este necesar.

SECȚIUNEA a 3-a
Masuri minime de protectie a informatiilor clasificate

Art. 25. - Masurile de protectie a informatiilor clasificate vor fi stabilite in raport cu:

a) clasele si nivelurile de secretizare a informatiilor;

b) volumul si suportul informatiilor;

c) calitatea, functia si numarul persoanelor care au sau pot avea acces la informatii, potrivit certificatului de securitate si autorizatiei de acces si cu respectarea principiului necesitatii de a cunoaste;

d) amenintarile, riscurile si vulnerabilitatile ce pot avea consecinte asupra informatiilor clasificate.

Art. 26. - Transmiterea informatiilor clasificate catre alti utilizatori se va efectua numai daca acestia detin certificate de securitate sau autorizatii de acces corespunzator nivelului de secretizare.

Art. 27. - Certificatele de securitate apartinand persoanelor al caror comportament, atitudini sau manifestari pot crea premise de insecuritate pentru informatiile secrete de stat vor fi imediat retrase, cu incunostintarea institutiilor investite cu atributii de coordonare a activitatii si de control al masurilor privitoare la protectia informatiilor clasificate, potrivit competentelor.

Art. 28. - Conducatorii unitatilor si persoanele care gestioneaza informatii clasificate au obligatia de a aduce la cunostinta institutiilor cu atributii de coordonare si control in domeniu orice indicii din care pot rezulta premise de insecuritate pentru astfel de informatii.

SECȚIUNEA a 4-a
Structura/functionarul de securitate

Art. 29. - **(1)** Pentru implementarea masurilor de protectie a informatiilor clasificate, in unitatile detinatoare de astfel de informatii se infiinteaza, in conditiile legii, structuri de securitate cu atributii specifice.

(2) In situatia in care unitatea detine un volum redus de informatii clasificate, atributiile structurii de securitate vor fi indeplinite de functionarul de securitate.

(3) Structura de securitate se organizeaza si se incadreaza potrivit legii.

(4) Seful structurii de securitate, respectiv functionarul de securitate, este un adjunct al conducatorului persoanei juridice sau un membru al consiliului de administratie al unitatii.

Art. 30. - Seful structurii de securitate, respectiv functionarul de securitate, detine certificat de securitate corespunzator celui mai inalt nivel de clasificare a informatiilor secrete de stat gestionate de unitate.

Art. 31. - **(1)** Structura/functionarul de securitate are urmatoarele atributii generale:

a) elaboreaza si supune aprobarii conducerii unitatii normele interne privind protectia informatiilor clasificate, potrivit legii;

b) intocmeste programul de prevenire a scurgerii de informatii clasificate si il supune avizarii institutiilor abilitate, iar dupa aprobare, actioneaza pentru aplicarea acestuia;

c) coordoneaza activitatea de protectie a informatiilor clasificate, in toate componentele acesteia;

d) asigura relationarea cu institutia abilitata sa coordoneze activitatea si sa controleze masurile privitoare la protectia informatiilor clasificate, potrivit legii;

e) monitorizeaza activitatea de aplicare a normelor de protectie a informatiilor clasificate si modul de respectare a acestora;

f) consiliaza conducerea unitatii in legatura cu toate aspectele privind securitatea informatiilor clasificate;

g) informeaza conducerea unitatii despre vulnerabilitatile si riscurile existente in sistemul de protectie a informatiilor clasificate si propune masuri pentru inlaturarea acestora;

h) acorda sprijin reprezentantilor autorizati ai institutiilor abilitate, potrivit competentelor legale, pe linia

verificarii persoanelor pentru care se solicita accesul la informatii clasificate;

i) organizeaza activitati de pregatire specifica a persoanelor care au acces la informatii clasificate;

j) asigura pastrarea si organizeaza evidenta certificatelor de securitate si autorizatiilor de acces la informatii clasificate;

k) actualizeaza permanent evidenta certificatelor de securitate si a autorizatiilor de acces;

l) intocmeste si actualizeaza listele informatiilor clasificate elaborate sau pastrate de unitate, pe clase si niveluri de secretizare;

m) prezinta conducatorului unitatii propuneri privind stabilirea obiectivelor, sectoarelor si locurilor de importanta deosebita pentru protectia informatiilor clasificate din sfera de responsabilitate si, dupa caz, solicita sprijinul institutiilor abilitate;

n) efectueaza, cu aprobarea conducerii unitatii, controale privind modul de aplicare a masurilor legale de protectie a informatiilor clasificate;

o) exercita alte atributii in domeniul protectiei informatiilor clasificate, potrivit legii.

(2) Atributiile personalului din structura de securitate, respectiv ale functionarului de securitate, se stabilesc prin fisa postului, aprobata de conducatorul unitatii.

Art. 32. - Persoanele care lucreaza in structura de securitate sau, dupa caz, functionarul de securitate vor fi incluse in programe permanente de pregatire organizate de institutiile investite cu atributii de coordonare a activitatii si de control al masurilor privitoare la protectia informatiilor clasificate, potrivit legii.

SECȚIUNEA a 5-a
Accesul la informatiile clasificate

Art. 33. - Accesul la informatii clasificate este permis cu respectarea principiului necesitatii de a cunoaste numai persoanelor care detin certificat de securitate sau autorizatie de acces, valabile pentru nivelul de secretizare al informatiilor necesare indeplinirii atributiilor de serviciu.

Art. 34. - Persoanele care au acces la informatii strict secrete de importanta deosebita, in conditiile prevazute de prezentele standarde, vor fi inregistrate in fisa de consultare, prevazuta la anexa nr. 1, care va fi pastrata la detinatorul de drept al documentului.

Art. 35. - **(1)** Persoanele carora le-au fost eliberate certificate de securitate sau autorizatii de acces vor fi instruite, atat la acordarea acestora, cat si periodic, cu privire la continutul reglementarilor privind protectia informatiilor clasificate.

(2) Activitatile de instruire vor fi consemnate de structura/functionarul de securitate, sub semnatura, in fisa de pregatire individuala, prezentata la anexa nr. 2.

(3) Persoanele prevazute la alin. (1) vor semna angajamentul de confidentialitate prevazut la anexa nr. 3.

Art. 36. - **(1)** In cazuri exceptionale, determinate de situatii de criza, calamitati sau evenimente imprevizibile, conducatorul unitatii poate acorda acces temporar la informatii clasificate anumitor persoane care nu detin certificat de securitate sau autorizatie de acces, cu conditia asigurarii unui sistem corespunzator de evidenta.

(2) Persoanele care primesc dreptul de acces temporar la informatii secrete de stat vor semna angajamentul de confidentialitate si vor fi comunicate la ORNISS, in cel mai scurt timp posibil, pentru efectuarea verificarilor de securitate, potrivit procedurilor.

Art. 37. - In cazul informatiilor strict secrete de importanta deosebita, accesul temporar va fi acordat, pe cat posibil, persoanelor care detin deja certificate de securitate pentru acces la informatii strict secrete sau secrete.

Art. 38. - **(1)** Transmiterea informatiilor clasificate intre unitati se va efectua cu aprobarea emitentului si cu respectarea principiului necesitatii de a cunoaste.

(2) Predarea-primirea informatiilor clasificate intre unitatea detinatoare si unitatea primitoare se face cu respectarea masurilor de protectie prevazute in prezentele standarde.

Art. 39. - Structura/functionarul de securitate al unitatii detinatoare se va asigura ca reprezentantul unitatii primitoare detine certificatul de securitate sau autorizatia de acces corespunzatoare nivelului de secretizare a informatiilor clasificate ce fac obiectul predarii-primirii.

CAPITOLUL III
REGULI GENERALE PRIVIND EVIDENTA, INTOCMIREA, PASTRAREA, PROCESAREA, MULTIPLICAREA, MANIPULAREA, TRANSPORTUL, TRANSMITEREA SI DISTRUGEREA INFORMATIILOR CLASIFICATE

Art. 40. - **(1)** In unitatile detinatoare de informatii clasificate se organizeaza compartimente speciale pentru evidenta, intocmirea, pastrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea si distrugerea acestora in conditii de siguranta.

(2) Activitatea compartimentelor speciale prevazute la alin. (1) este coordonata de structura/functionarul de securitate.

Art. 41. - La redactarea documentelor ce contin informatii clasificate se vor respecta urmatoarele reguli:

a) mentionarea, in antet, a unitatii emitente, a numarului si datei inregistrarii, a clasei sau nivelului de secretizare, a numarului de exemplare si, dupa caz, a destinatarului;

b) numerele de inregistrare se inscriu pe toate exemplarele documentului si pe anexele acestora, fiind precedate de un zero (0) pentru documentele secrete, de doua zerouri (00) pentru cele strict secrete, de trei zerouri (000) pentru cele strict secrete de importanta deosebita si de litera "S" pentru secrete de serviciu;

c) la sfarsitul documentului se inscriu in clar, dupa caz, rangul, functia, numele si prenumele conducatorului unitatii emitente, precum si ale celui care il intocmeste, urmate de semnaturile acestora si stampila unitatii;

d) inscrierea, pe fiecare pagina a documentului, a clasei sau nivelului de secretizare atribuit acestuia;

e) pe fiecare pagina a documentelor ce contin informatii clasificate se inscriu numarul curent al paginii, urmat de numarul total al acestora.

Art. 42. - **(1)** in situatia in care documentul de baza este insotit de anexe, la sfarsitul textului se indica, pentru fiecare anexa, numarul de inregistrare, numarul de file al acesteia si clasa sau nivelul de secretizare.

(2) Anexele se clasifica in functie de continutul lor si nu de cel al documentelor pe care le insotesc.

(3) Adresa de insotire a documentului nu va cuprinde informatii detaliate referitoare la continutul documentelor anexate.

(4) Documentele anexate se semneaza, daca este cazul, de persoanele care au semnat documentul de baza.

(5) Aplicarea, pe documentele anexate, a stampilei unitatii emitente este obligatorie.

Art. 43. - **(1)** Cand documentele ce contin informatii clasificate se semneaza de o singura persoana, datele privind rangul, functia, numele si prenumele acesteia se inscriu sub text, in centrul paginii.

(2) Cand semneaza doua sau mai multe persoane, rangul, functia, numele si prenumele conducatorului unitatii se inscriu in partea stanga, iar ale celorlalti semnatari in partea dreapta, in ordinea rangurilor si functiilor.

Art. 44. - Cand documentele care contin informatii clasificate se emit in comun de doua sau mai multe unitati, denumirile acestora se inscriu separat in antet, iar la sfarsit se semneaza de catre conducatorii unitatilor respective, de la stanga la dreapta, aplicandu-se stampilele corespunzatoare.

Art. 45. - Informatiile clasificate vor fi marcate, inscriptionate si gestionate numai de catre persoane care au autorizatie sau certificat de securitate corespunzator nivelului de clasificare a acestora.

Art. 46. - **(1)** Toate documentele, indiferent de forma, care contin informatii clasificate au inscrise, pe fiecare pagina, nivelul de secretizare.

(2) Nivelul de secretizare se marcheaza prin stampilare, dactilografiere, tiparire sau olograf, astfel:

a) in partea dreapta sus si jos, pe exteriorul copertelor, pe pagina cu titlul si pe prima pagina a documentului;

b) in partea de jos si de sus, la mijlocul paginii, pe toate celelalte pagini ale documentului;

c) sub legenda, titlu sau scara de reprezentare si in exterior - pe verso - atunci cand acestea sunt pliate, pe toate schemele, diagramele, hartile, desenele si alte asemenea documente.

Art. 47. - Portiunile clar identificabile din documentele clasificate complexe, cum sunt sectiunile, anexele, paragrafele, titlurile, care au niveluri diferite de secretizare sau care nu sunt clasificate, trebuie marcate corespunzator nivelului de clasificare si secretizare.

Art. 48. - Marcajul de clasificare va fi aplicat separat de celelalte marcaje, cu caractere si/sau culori diferite.

Art. 49. - **(1)** Toate documentele clasificate aflate in lucru sau in stadiu de proiect vor avea inscrise mentiunile "Document in lucru" sau "Proiect" si vor fi marcate potrivit clasei sau nivelului de secretizare a informatiilor ce le contin.

(2) Gestionarea documentelor clasificate aflate in lucru sau in stadiu de proiect se face in aceleasi conditii ca si a celor in forma definitiva.

Art. 50. - Documentele sau materialele care contin informatii clasificate si sunt destinate unei persoane strict determinate vor fi inscriptionate, sub destinatar, cu mentiunea "Personal".

Art. 51. - **(1)** Fotografiile, filmele, microfilmele si negativele lor, rolele, bobinele sau containerele de pastrare a acestora se marcheaza vizibil cu o eticheta care indica numarul si data inregistrarii, precum si clasa sau nivelul de secretizare.

(2) Microfilmele trebuie sa aiba afisat la cele doua capete clasa sau nivelul de secretizare, iar la inceputul rolei, lista elementelor de continut.

Art. 52. - **(1)** Clasa sau nivelul de secretizare a informatiilor inregistrate pe benzi audio se imprima verbal, atat la inceputul inregistrarii, cat si la sfarsitul acesteia.

(2) Marcarea clasei sau a nivelului de secretizare pe benzi video trebuie sa asigure afisarea pe ecran a clasei sau a nivelului de secretizare. In cazul in care nu se poate stabili cu exactitate clasa sau nivelul de secretizare, inainte de inregistrarea benzilor, marcajul se aplica prin inserarea unui segment de banda la inceputul si la sfarsitul benzii video.

(3) Benzile audio si video care contin informatii clasificate pastreaza clasa sau nivelul de secretizare cel mai inalt atribuit pana in momentul:

a) distrugerii printr-un procedeu autorizat;

b) atribuirii unui nivel superior prin adaugarea unei inregistrari cu nivel superior de secretizare.

Art. 53. - Proiectiile de imagini trebuie sa afiseze, la inceputul si sfarsitul acestora, numarul si data inregistrarii, precum si clasa sau nivelul de secretizare.

Art. 54. - **(1)** Rolele, bobinele sau containerele de pastrare a benzilor magnetice, inclusiv cele video, pe

care au fost imprimate informatii secrete de stat, vor avea inscris, la loc vizibil, clasa sau nivelul de secretizare cel mai inalt atribuit acestora, care va ramane aplicat pana la distrugerea sau demagnetizarea lor.

(2) La efectuarea unei inregistrari pe banda magnetica, atat la inceputul, cat si la sfarsitul fiecarui pasaj, se va mentiona clasa sau nivelul de secretizare.

(3) In cazul detasarii de pe suportul fizic, fiecare capat al benzii va fi marcat, la loc vizibil, cu clasa sau nivelul de secretizare.

Art. 55. - In toate cazurile, ambalajele sau suportii in care se pastreaza documente sau materiale ce contin informatii clasificate vor avea inscriptionat clasa sau nivelul de secretizare, numarul si data inregistrarii in evidente si li se va atasa o lista cu denumirea acestora.

Art. 56. - **(1)** Atunci cand se utilizeaza documente clasificate ca surse pentru intocmirea unui alt document, marcajele documentelor sursa le vor determina pe cele ale documentului rezultat.

(2) Pe documentul rezultat se vor preciza documentele sursa care au stat la baza intocmirii lui.

Art. 57. - Numarul si data initiala a inregistrarii documentului clasificat trebuie pastrate, chiar daca i se aduc amendamente, pana cand documentul respectiv va face obiectul reevaluarii clasei sau a nivelului de secretizare.

Art. 58. - Conducatorii unitatilor vor asigura masurile necesare de evidenta si control al informatiilor clasificate, astfel incat sa se poata stabili, in orice moment, locul in care se afla aceste informatii.

Art. 59. - **(1)** Evidenta materialelor si documentelor care contin informatii clasificate se tine in registre speciale, intocmite potrivit modelelor prevazute in anexele nr. 4, 5 si 6.

(2) Fiecare document sau material va fi inscriptionat cu numarul de inregistrare si data cand este inscris in registrele de evidenta.

(3) Numerele de inregistrare sunt precedate de numarul de zerouri corespunzator nivelului de secretizare atribuit sau de litera "S" pentru secrete de serviciu.

(4) Toate registrele, condicile si borderourile se inregistreaza in registrul unic de evidenta a registrelor, condicilor, borderourilor si a caietelor pentru insemnari clasificate, conform modelului din anexa nr. 7.

(5) Fac exceptie actele de gestiune, imprimatele inseriate si alte documente sau materiale cuprinse in forme de evidenta specifice.

Art. 60. - **(1)** Documentele sau materialele care contin informatii clasificate inregistrate in registrele prevazute in art. 59 nu vor fi inregistrate in alte forme de evidenta.

(2) Emitentii si detinatorii de informatii clasificate sunt obligati sa inregistreze si sa tina evidenta tuturor documentelor si materialelor primite, expediate sau a celor intocmite de unitatea proprie, potrivit legii.

(3) In registrele pentru evidenta informatiilor clasificate vor fi mentionate numele si prenumele persoanei care a primit documentul, iar aceasta va semna de primire pe condica prevazuta in anexa nr. 8.

Art. 61. - **(1)** Atribuirea numerelor de inregistrare in registrele pentru evidenta se face consecutiv, pe parcursul unui an calendaristic.

(2) Numerele de inregistrare se inscriu obligatoriu pe toate exemplarele documentelor sau materialelor care contin informatii clasificate, precum si pe documentele anexate.

(3) Anual, documentele se claseaza in dosare, potrivit problematicii si termenelor de pastrare stabilite in nomenclatoare arhivistice, potrivit legii.

(4) Clasarea documentelor sau materialelor care contin informatii clasificate se face separat, in functie de suportul si formatul acestora, cu folosirea mijloacelor de pastrare si protejare adecvate.

Art. 62. - **(1)** Informatiile strict secrete de importanta deosebita vor fi compartimentate fizic si inregistrate separat de celelalte informatii.

(2) Evidenta documentelor strict secrete si secrete poate fi operata in acelasi registru.

Art. 63. - Hartile, planurile topografice, asamblajele de harti si alte asemenea documente se inregistreaza in registrele pentru evidenta informatiilor clasificate prevazute in anexele nr. 4, 5 si 6.

Art. 64. - Atribuirea aceluiasi numar de inregistrare unor documente cu continut diferit este interzisa.

Art. 65. - Registrele de evidenta vor fi completate de persoana desemnata care detine autorizatie sau certificat de securitate corespunzator.

Art. 66. - **(1)** Multiplicarea prin dactilografiere si procesare la calculator a documentelor clasificate poate fi realizata numai de catre persoane autorizate sa aiba acces la astfel de informatii.

(2) Multiplicarea documentelor clasificate poate fi realizata de persoane autorizate, numai in incaperi special destinate.

Art. 67. - **(1)** Documentelor care contin informatii clasificate rezultate in procesul de multiplicare li se atribuie numere din registrul de evidenta a informatiilor clasificate multiplicate, conform modelului din anexa nr. 9.

(2) Numerele se atribuie consecutiv, incepand cu cifra 1, pe parcursul unui an calendaristic si se inscriu obligatoriu pe toate exemplarele documentului.

Art. 68. - **(1)** Evidentierea operatiunii de multiplicare se face prin marcare atat pe original, cat si pe toate copiile rezultate.

(2) Pe documentul original marcarea se aplica in partea dreapta jos a ultimei pagini.

(3) Pe copiile rezultate, marcarea se aplica pe prima pagina, sub numarul de inregistrare al documentului.

(4) In cazul copierii succesive, la date diferite, a unui document clasificat, documentul original va fi marcat la fiecare operatiune, ce va fi, de asemenea, inscrisa in registru.

(5) Exemplarele rezultate in urma copierii documentului secret de stat se numeroteaza in ordine succesiva, chiar daca operatiunea se efectueaza de mai multe ori si la date diferite.

Art. 69. - **(1)** Multiplicarea documentelor clasificate se face in baza aprobarii conducatorului unitatii detinatoare, cu avizul structurii/functionarului de securitate, ambele inscrise pe cererea pentru copiere sau pe adresa de insotire in care se mentioneaza necesitatea multiplicarii.

(2) Parchetele, instantele si comisiile de cercetare pot multiplica documente care contin informatii clasificate numai in conditiile prezentelor standarde.

(3) Extrasul dintr-un document care contine informatii clasificate se face in baza cererii pentru copiere, cu aprobarea conducatorului unitatii, iar documentul rezultat va avea mentionat sub numarul de exemplar cuvantul "Extras" si numarul de inregistrare al documentului original.

(4) Clasa sau nivelul de secretizare atribuit unui document original se aplica, in mod identic, reproducerilor sau traducerilor.

Art. 70. - **(1)** Daca emitentul doreste sa aiba control exclusiv asupra reproducerii, documentul va contine o indicatie vizibila cu urmatorul continut: "Reproducerea acestui document, totala sau partiala, este interzisa".

(2) Informatiile clasificate inscrise pe documente cu regim restrictiv de reproducere care au mentiunea "Reproducerea interzisa" nu se multiplica.

Art. 71. - In cazul copierii unui document care contine informatii clasificate se procedeaza astfel:

a) se stabileste numarul de exemplare in care va fi multiplicat;

b) se completeaza si se aproba cererea pentru multiplicare, potrivit art. 69 alin. (1), dupa care aceasta se inregistreaza in registrul de evidenta - anexa nr. 4 sau anexa nr. 5, dupa caz;

c) documentul original se preda operatorului pe baza de semnatura;

d) dupa verificarea exemplarelor rezultate, beneficiarul semneaza in registrul de evidenta a informatiilor clasificate multiplicate, conform modelului din anexa nr. 9;

e) repartitia in vederea difuzarii exemplarelor copiate se consemneaza de catre structura/functionarul de securitate pe spatele cererii pentru copiere;

f) cererea pentru copiere impreuna cu exemplarele copiate se predau pe baza de semnatura structurii/functionarului de securitate in vederea difuzarii sau expedierii.

Art. 72. - **(1)** Cand se dactilografiaza, se proceseaza la calculator sau se copiaza documente care contin informatii clasificate, in mai mult de doua exemplare, pe spatele exemplarului original sau al cererii pentru copiere se inscriu destinatarii documentelor si numarul exemplarelor.

(2) Atunci cand numarul destinatarilor este mare se intocmeste un tabel de difuzare, care se inregistreaza ca document anexat la original.

(3) Numerotarea exemplarelor copiate se va face consecutiv pentru fiecare copie, indiferent de data executarii, avandu-se in vedere si numarul de exemplare rezultat in urma dactilografierii sau procesarii la calculator

Art. 73. - Documentele clasificate pot fi microfilmate sau stocate pe discuri optice ori pe suporti magnetici in urmatoarele conditii:

a) procesul de microfilmare sau stocare sa fie realizat cu aprobarea emitentului, de personal autorizat pentru clasa sau nivelul de secretizare a informatiilor respective;

b) microfilmelor, discurilor optice sau suportilor magnetici de stocare sa li se asigure aceeasi protectie ca a documentului original;

c) toate microfilmele, discurile optice sau suportii magnetici de stocare sa fie inregistrate intr-o evidenta specifica si supuse, ca si documentele originale, verificarii anuale.

Art. 74. - **(1)** Difuzarea informatiilor clasificate multiplicate se face obligatoriu cu avizul structurii/functionarului de securitate.

(2) Informatiile clasificate pot fi redifuzate de catre destinatarul initial la alti destinatari, cu respectarea normelor din prezentele standarde.

(3) Emitentul este obligat sa indice clar toate restrictiile care trebuie respectate pentru difuzarea unei informatii clasificate. Cand se impun astfel de restrictii, destinatarii pot proceda la o redifuzare numai cu aprobarea scrisa a emitentului.

Art. 75. - In cazul in care un document secret de stat este studiat de o persoana abilitata, pentru care s-a stabilit necesitatea de a accesa astfel de documente in vederea indeplinirii sarcinilor de serviciu, aceasta activitate trebuie consemnata in fisa de consultare, conform modelului din anexa nr. 1.

Art. 76. - **(1)** Informatiile clasificate iesite din termenul de clasificare se arhiveaza sau se distrug.

(2) Arhivarea sau distrugerea unui document clasificat se mentioneaza in registrul de evidenta principal, prin consemnarea cotei arhivistice de regasire sau, dupa caz, a numarului de inregistrare a procesului-verbal de distrugere.

(3) Distrugerea informatiilor clasificate inlocuite sau perimate se face numai cu avizul emitentului.

(4) Distrugerea documentelor clasificate sau a ciornelor care contin informatii cu acest caracter se face astfel incat sa nu mai poata fi reconstituite.

Art. 77. - **(1)** Documentele de lucru, ciornele sau materialele acumulate sau create in procesul de elaborare a unui document, care contin informatii clasificate, de regula, se distrug.

(2) In cazul in care se pastreaza, acestea vor fi datate, marcate cu clasa sau nivelul de secretizare cel mai inalt al informatiilor continute, arhivate si protejate corespunzator clasei sau nivelului de secretizare a

documentului final.

Art. 78. - **(1)** Informatiile strict secrete de importanta deosebita destinate distrugerii vor fi inapoiate unitatii emitente cu adresa de restituire.

(2) Fiecare asemenea informatie va fi trecuta pe un proces-verbal de distrugere, care va fi aprobat de conducerea unitatii si semnat de seful structurii/functionarul de securitate si de persoana care asista la distrugere, autorizata sa aiba acces la informatii strict secrete de importanta deosebita.

(3) In situatii de urgenta, protectia, inclusiv prin distrugere, a materialelor si documentelor strict secrete de importanta deosebita va avea intotdeauna prioritate fata de alte documente sau materiale.

(4) Procesele-verbale de distrugere si documentele de evidenta ale acestora vor fi arhivate si pastrate cel putin 10 ani.

Art. 79. - **(1)** Distrugerea informatiilor strict secrete, secrete si secrete de serviciu va fi evidentiata intr-un proces-verbal semnat de doua persoane asistente autorizate sa aiba acces la informatii de acest nivel, avizat de structura/functionarul de securitate si aprobat de conducatorul unitatii.

(2) Procesele-verbale de distrugere si documentele de evidenta a informatiilor strict secrete, secrete si secrete de serviciu vor fi pastrate de compartimentul care a executat distrugerea, o perioada de cel putin trei ani, dupa care vor fi arhivate si pastrate cel putin 10 ani.

Art. 80. - **(1)** Distrugerea ciornelor documentelor secrete de stat se realizeaza de catre persoanele care le-au elaborat.

(2) Procesul-verbal de distrugere a ciornelor se intocmeste in situatia in care acestea au fost inregistrate intr-o forma de evidenta.

Art. 81. - **(1)** Documentele si materialele ce contin informatii clasificate se transporta, pe teritoriul Romaniei, prin intermediul unitatii specializate a Serviciului Roman de Informatii, potrivit normelor stabilite prin hotarare a Guvernului.

(2) Documentele si materialele care contin informatii clasificate se transporta in strainatate prin valiza diplomatica, de catre curierii diplomatici selectionati si pregatiti de Serviciul de Informatii Externe.

(3) Este interzisa expedierea documentelor si materialelor ce contin informatii clasificate prin S.N. "Posta Romana" ori prin alte societati comerciale de transport.

Art. 82. - Conducatorii unitatilor detinatoare de informatii clasificate vor desemna, din structura de securitate proprie, in conditiile prezentelor standarde, cel putin un delegat imputernicit pentru transportul si executarea operatiunilor de predare-primire a corespondentei clasificate, intre aceasta si unitatea specializata a Serviciului Roman de Informatii.

CAPITOLUL IV
PROTECTIA INFORMATIILOR SECRETE DE STAT

SECȚIUNEA 1
Obligatiile si raspunderile ce revin autoritatilor si institutiilor publice, agentilor economici si altor persoane juridice pentru protectia informatiilor secrete de stat

Art. 83. - Protectia informatiilor secrete de stat reprezinta o obligatie ce revine tuturor persoanelor autorizate care le emit, le gestioneaza sau care intra in posesia lor.

Art. 84. - **(1)** Conducatorii unitatilor detinatoare de informatii secrete de stat sunt raspunzatori de aplicarea masurilor de protectie a informatiilor secrete de stat.

(2) Persoanele juridice de drept privat detinatoare de informatii secrete de stat au obligatia sa respecte si sa aplice reglementarile in vigoare stabilite pentru autoritatile si institutiile publice, in domeniul lor de activitate.

Art. 85. - Pana la infiintarea si organizarea structurii de securitate sau, dupa caz, pana la numirea functionarului de securitate, conducatorii unitatilor detinatoare de informatii secrete de stat vor desemna o persoana care sa indeplineasca temporar atributiile specifice protectiei informatiilor clasificate, prin cumul de functii.

Art. 86. - **(1)** Conducatorul unitatii care gestioneaza informatii secrete de stat este obligat:

a) sa asigure organizarea activitatii structurii de securitate, respectiv a functionarului de securitate si compartimentelor speciale pentru gestionarea informatiilor clasificate, in conditiile legii;

b) sa solicite institutiilor abilitate efectuarea de verificari pentru avizarea eliberarii certificatului de securitate si autorizatiei de acces la informatii clasificate pentru angajatii proprii;

c) sa notifice la ORNISS eliberarea certificatului de securitate sau autorizatiei de acces pentru fiecare angajat care lucreaza cu informatii clasificate;

d) sa aprobe listele cu personalul verificat si avizat pentru lucrul cu informatiile secrete de stat si evidenta detinatorilor de certificate de securitate si autorizatii de acces si sa le comunice la ORNISS si la institutiile abilitate sa coordoneze activitatea si controlul masurilor privitoare la protectia informatiilor clasificate, potrivit legii;

e) sa intocmeasca lista informatiilor secrete de stat si a termenelor de mentinere in nivelurile de secretizare si sa o supuna aprobarii Guvernului, potrivit legii;

f) sa stabileasca obiectivele, sectoarele si locurile din zona de competenta care prezinta importanta

deosebita pentru protectia informatiilor secrete de stat si sa le comunice Serviciului Roman de Informatii pentru a fi supuse spre aprobare Guvernului;

g) sa solicite asistenta de specialitate institutiilor abilitate sa coordoneze activitatea si sa controleze masurile privitoare la protectia informatiilor secrete de stat;

h) sa supuna avizarii institutiilor abilitate programul propriu de prevenire a scurgerii de informatii clasificate si sa asigure aplicarea acestuia;

i) sa elaboreze si sa aplice masurile procedurale de protectie fizica si de protectie a personalului care are acces la informatii clasificate;

j) sa intocmeasca ghidul pe baza caruia se va realiza incadrarea corecta si uniforma in nivelurile de secretizare a informatiilor secrete de stat, in stricta conformitate cu legea si sa il prezinte, spre aprobare, imputernicitilor si functionarilor superiori abilitati prin lege sa atribuie nivelurile de secretizare;

k) sa asigure aplicarea si respectarea regulilor generale privind evidenta, intocmirea, pastrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea si distrugerea informatiilor secrete de stat si a interdictiilor de reproducere si circulatie, in conformitate cu actele normative in vigoare;

l) sa comunice institutiilor abilitate, potrivit competentelor, lista functiilor din subordine care necesita acces la informatii secrete de stat;

m) la incheierea contractelor individuale de munca, a contractelor de colaborare sau conventiilor de orice natura sa precizeze obligatiile ce revin partilor pentru protectia informatiilor clasificate in interiorul si in afara unitatii, in timpul programului si dupa terminarea acestuia, precum si la incetarea activitatii in unitatea respectiva;

n) sa asigure includerea personalului structurii/functionarului de securitate in sistemul permanent de pregatire si perfectionare, conform prezentelor standarde;

o) sa aprobe normele interne de aplicare a masurilor privind protectia informatiilor clasificate, in toate componentele acesteia, si sa controleze modul de respectare in cadrul unitatii;

p) sa asigure fondurile necesare pentru implementarea masurilor privitoare la protectia informatiilor clasificate, conform legii;

q) sa analizeze, ori de cate ori este necesar, dar cel putin semestrial, modul in care structura/functionarul de securitate si personalul autorizat asigura protectia informatiilor clasificate;

r) sa asigure inventarierea anuala a documentelor clasificate si, pe baza acesteia, sa dispuna masuri in consecinta, conform legii;

s) sa sesizeze institutiile prevazute la art. 25 din Legea nr. 182/2002, conform competentelor, in legatura cu incidentele de securitate si riscurile la adresa informatiilor secrete de stat;

t) sa dispuna efectuarea de cercetari si, dupa caz, sa sesizeze organele de urmarire penala in situatia compromiterii informatiilor clasificate.

(2) De la prevederile alin. (1) lit. f) si h) se excepteaza institutiile prevazute la art. 25 din Legea nr. 182/2002.

SECȚIUNEA a 2-a
Protectia juridica

Art. 87. - Conducatorii unitatilor detinatoare de secrete de stat vor asigura conditiile necesare pentru ca toate persoanele care gestioneaza astfel de informatii sa cunoasca reglementarile in vigoare referitoare la protectia informatiilor clasificate.

Art. 88. - **(1)** Conducatorii unitatilor detinatoare de informatii secrete de stat au obligatia de a instiinta, in scris, institutiile prevazute la art. 25 din Legea nr. 182/2002, potrivit competentelor, prin cel mai operativ sistem de comunicare, despre compromiterea unor astfel de informatii.

(2) Instiintarea prevazuta la alin. (1) se face in scopul obtinerii sprijinului necesar pentru recuperarea informatiilor, evaluarea prejudiciilor, diminuarea si inlaturarea consecintelor.

(3) Instiintarea trebuie sa contina:

a) prezentarea informatiilor compromise, respectiv clasificarea, marcarea, continutul, data emiterii, numarul de inregistrare si de exemplare, emitentul si persoana sau compartimentul care le-a gestionat;

b) o scurta prezentare a imprejurarilor in care a avut loc compromiterea, inclusiv data constatarii, perioada in care informatiile au fost expuse compromiterii si persoanele neautorizate care au avut sau ar fi putut avea acces la acestea, daca sunt cunoscute;

c) precizari cu privire la eventuala informare a emitentului.

(4) La solicitarea institutiilor competente, instiintarile preliminare vor fi completate pe masura derularii cercetarilor.

(5) Documentele privind evaluarea prejudiciilor si activitatile ce urmeaza a fi intreprinse ca urmare a compromiterii vor fi prezentate institutiilor competente.

Art. 89. - Pentru prejudiciile cauzate detinatorului informatiei secrete de stat compromise, acesta are dreptul la despagubiri civile, potrivit dreptului comun.

Art. 90. - **(1)** Orice incalcare a reglementarilor de securitate va fi cercetata pentru a se stabili:

a) daca informatiile respective au fost compromise;

b) daca persoanele neautorizate care au avut sau ar fi putut avea acces la informatii secrete de stat prezinta suficienta incredere si loialitate, astfel incat rezultatul compromiterii sa nu creeze prejudicii;

c) masurile de remediere - corective, disciplinare sau juridice - care sunt recomandate.

(2) In situatia in care informatiile clasificate au fost accesate de persoane neautorizate, acestea vor fi instruite pentru a preveni producerea de eventuale prejudicii.

(3) In cazul savarsirii de infractiuni la protectia secretului de stat, unitatile detinatoare au obligatia de a sesiza organele de urmarire penala si de a pune la dispozitia acestora datele si materialele necesare probarii faptelor.

Art. 91. - **(1)** Structura/functionarul de securitate are obligatia de a tine evidenta cazurilor de incalcare a reglementarilor de securitate, a documentelor de cercetare si a masurilor de solutionare si sa le puna la dispozitia autoritatilor desemnate de securitate, conform competentelor ce le revin.

(2) Documentele mentionate la alin. (1) se pastreaza timp de cinci ani.

Art. 92. - Litigiile cu privire la calitatea de emitent ori detinator sau cele determinate de continutul informatiilor secrete de stat, inclusiv drepturile patrimoniale ce revin emitentului din contractele de cesiune si licenta, precum si litigiile referitoare la nerespectarea dispozitiilor legale privind dreptul de autor si drepturile conexe, inventiile si inovatiile, protectia modelelor industriale, combaterea concurentei neloiale si a celor stipulate in tratatele, acordurile si intelegerile la care Romania este parte, sunt de competenta instantelor judecatoresti.

SECȚIUNEA a 3-a
Protectia prin masuri procedurale

Art. 93. - Toate unitatile care detin informatii secrete de stat au obligatia sa stabileasca norme interne de lucru si de ordine interioara destinate protectiei acestor informatii, potrivit actelor normative in vigoare.

Art. 94. - **(1)** Masurile procedurale de protectie a informatiilor secrete de stat vor fi integrate in programul de prevenire a scurgerii de informatii clasificate, intocmit potrivit anexei nr. 10, care va fi prezentat, spre avizare, autoritatii abilitate sa coordoneze activitatea si sa controleze masurile privitoare la protectia informatiilor clasificate, potrivit legii.

(2) Sunt exceptate de obligativitatea prezentarii, spre avizare, a programului de prevenire a scurgem de informatii, mentionat la alin. (1), institutiile prevazute la art. 25 alin. (4) din Legea nr. 182/2002.

Art. 95. - Angajamentele de confidentialitate intocmite potrivit reglementarilor in vigoare vor garanta ca informatiile la care se acorda acces sunt protejate corespunzator.

SECȚIUNEA a 4-a
Protectia fizica

Art. 96. - Obiectivele, sectoarele si locurile in care sunt gestionate informatii secrete de stat trebuie protejate fizic impotriva accesului neautorizat.

Art. 97. - Masurile de protectie fizica - gratii la ferestre, incuietori la usi, paza la intrari, sisteme automate pentru supraveghere, control, acces, patrule de securitate, dispozitive de alarma, mijloace pentru detectarea observarii, ascultarii sau interceptarii - vor fi dimensionate in raport cu:

a) nivelul de secretizare a informatiilor, volumul si localizarea acestora;

b) tipul containerelor in care sunt depozitate informatiile;

c) caracteristicile cladirii si zonei de amplasare.

Art. 98. - Zonele in care sunt manipulate sau stocate informatii secrete de stat trebuie organizate si administrate in asa fel incat sa corespunda uneia din urmatoarele categorii:

a) zona de securitate clasa I, care presupune ca orice persoana aflata in interiorul acesteia are acces la informatii secrete de stat, de nivel strict secret de importanta deosebita si strict secret, si care necesita:

- perimetru clar determinat si protejat, in care toate intrarile si iesirile sunt supravegheate;

- controlul sistemului de intrare, care sa permita numai accesul persoanelor verificate corespunzator si autorizate in mod special;

- indicarea clasei si a nivelului de secretizare a informatiilor existente in zona;

b) zona de securitate clasa a II-a, care presupune ca gestionarea informatiilor de nivel secret se realizeaza prin aplicarea unor masuri specifice de protectie impotriva accesului persoanelor neautorizate si care necesita:

- perimetru clar delimitat si protejat, in care toate intrarile si iesirile sunt supravegheate;

- controlul sistemului de intrare care sa permita accesul neinsotit numai persoanelor verificate si autorizate sa patrunda in aceasta zona;

- reguli de insotire, supraveghere si prevenire a accesului persoanelor neautorizate la informatii clasificate.

Art. 99. - Incintele in care nu se lucreaza zilnic 24 de ore vor fi inspectate imediat dupa terminarea programului de lucru, pentru a verifica daca informatiile secrete de stat sunt asigurate in mod corespunzator.

Art. 100. - In jurul zonelor de securitate clasa I sau clasa a II-a poate fi stabilita o zona administrativa, cu perimetru vizibil delimitat, in interiorul careia sa existe posibilitatea de control al personalului si al vehiculelor.

Art. 101. - **(1)** Accesul in zonele de securitate clasa I si clasa a II-a va fi controlat prin verificarea

permisului de acces sau printr-un sistem de recunoastere individuala aplicat personalului.

(2) Unitatile detinatoare de informatii secrete de stat vor institui un sistem propriu de control al vizitatorilor, destinat interzicerii accesului neautorizat al acestora in zonele de securitate.

Art. 102. - Permisul de acces nu va specifica, in clar, identitatea unitatii emitente sau locul in care detinatorul are acces.

Art. 103. - Unitatile vor organiza, la intrarea sau la iesirea din zonele de securitate clasa I sau clasa a II-a, controale planificate si inopinate ale bagajelor, incluzand colete, genti si alte tipuri de suporti in care s-ar putea transporta materiale si informatii secrete de stat.

Art. 104. - Personalul inclus in sistemul de paza si aparare a obiectivelor, sectoarelor si locurilor in care sunt gestionate informatii secrete de stat trebuie sa detina autorizatie de acces corespunzator nivelului de secretizare a informatiilor necesare indeplinirii atributiilor ce ii revin.

Art. 105. - Este interzis accesul cu aparate de fotografiat, filmat, inregistrat audio-video, de copiat din baze de date informatice sau de comunicare la distanta, in locurile in care se afla informatii secrete de stat.

Art. 106. - Conducatorii unitatilor detinatoare de informatii secrete de stat vor stabili reguli cu privire la circulatia si ordinea interioara in zonele de securitate, astfel incat accesul sa fie permis exclusiv posesorilor de certificate de securitate si autorizatii de acces, cu respectarea principiului necesitatii de a cunoaste.

Art. 107. - Accesul pentru interventii tehnice, reparatii sau activitati de deservire in locuri in care se lucreaza cu informatii secrete de stat ori in care se pastreaza, se prelucreaza sau se multiplica astfel de informatii este permis numai angajatilor unitatii care detin autorizatii de acces, corespunzator celui mai inalt nivel de secretizare a informatiilor pe care le-ar putea cunoaste.

Art. 108. - **(1)** Pentru a distinge persoanele care au acces in diferite locuri sau sectoare in care sunt gestionate informatii secrete de stat, acestea vor purta insemne sau echipamente specifice.

(2) In locurile si sectoarele in care sunt gestionate informatii secrete de stat, insemnele si echipamentele distinctive se stabilesc prin regulamente de ordine interioara.

(3) Evidenta legitimatiilor, permiselor si a altor insemne si echipamente distinctive va fi tinuta de structura/functionarul de securitate al unitatii.

Art. 109. - **(1)** Persoanele care pierd permisele de acces in unitate, insemnele sau echipamentele specifice sunt obligate sa anunte de indata seful ierarhic.

(2) In situatiile mentionate la alin. (1), conducatorul institutiei va dispune cercetarea imprejurarilor in care s-au produs si va informa autoritatea desemnata de securitate competenta.

(3) Structura/functionarul de securitate va lua masurile ce se impun pentru a preveni folosirea permiselor de acces, insemnelor sau echipamentelor specifice de catre persoane neautorizate.

Art. 110. - Accesul fiecarui angajat al unitatii detinatoare de informatii secrete de stat in zone de securitate clasa I sau clasa a II-a se realizeaza prin intrari anume stabilite, pe baza permisului de acces, semnat de conducatorul acesteia.

Art. 111. - **(1)** Permisele de acces vor fi individuali/ale prin aplicarea unor semne distinctive.

(2) Permisele de acces se vizeaza semestrial.

(3) La incetarea angajarii permisele de acces vor fi retrase si anulate.

Art. 112. - Este interzis accesul altor persoane, in afara celor care dispun de permis de acces, in locurile in care sunt gestionate informatii secrete de stat.

Art. 113. - Accesul persoanelor din afara unitatii in zona administrativa sau in zonele de securitate este permis numai daca sunt insotite de persoane anume desemnate, cu bilet de intrare eliberat pe baza documentelor de legitimare de conducatorul unitatii.

Art. 114. - **(1)** Accesul angajatilor agentilor economici care efectueaza lucrari de constructii, reparatii si intretinere a cladirilor, instalatiilor sau utilitatilor in zonele administrative ori in zonele de securitate se realizeaza cu documente de acces temporar eliberate de conducatorii unitatilor beneficiare, pe baza actelor de identitate, la solicitarea reprezentantilor autorizati ai agentilor economici in cauza.

(2) Locurile in care se efectueaza lucrarile mentionate la alin. (1) se supravegheaza de catre persoane anume desemnate din unitatea beneficiara.

(3) Documentul de acces temporar are valabilitate pe durata executarii lucrarilor si se vizeaza trimestrial, iar la terminarea activitatilor se restituie emitentului.

(4) Pierderea documentului de acces temporar va fi luata in evidenta structurii/functionarului de securitate care va dispune masurile necesare de prevenire a folosirii lui de catre persoane neautorizate.

Art. 115. - Reprezentantii institutiilor care, potrivit competentelor legale, au atributii de coordonare si control pe linia protectiei informatiilor clasificate au acces la obiectivele, sectoarele si locurile in care sunt gestionate informatii clasificate, pe baza legitimatiei de serviciu si a delegatiei speciale, semnata de conducatorul autoritatii pe care o reprezinta.

Art. 116. - Persoanele aflate in practica de documentare, stagii de instruire sau schimb de experienta au acces numai in locurile stabilite de conducatorul unitatii, pe baza permiselor de acces eliberate in acest sens.

Art. 117. - Persoanele care solicita angajari, audiente, ori care prezinta reclamatii si sesizari vor fi primite in afara zonelor administrative sau in locuri special amenajate, cu aprobarea conducatorului unitatii.

Art. 118. - In afara orelor de program si in zilele nelucratoare, se vor organiza patrulari pe perimetrul unitatii, la intervale care vor fi stabilite prin instructiuni elaborate pe baza planului de paza si aparare al obiectivului.

Art. 119. - **(1)** Sistemele de paza, supraveghere si control-acces trebuie sa asigure prevenirea patrunderii neautorizate in obiectivele, sectoarele si locurile unde sunt gestionate informatii clasificate.

(2) Timpul de reactie a personalului de paza si aparare va fi testat periodic pentru a garanta interventia operativa in situatii de urgenta.

Art. 120. - **(1)** Unitatile care gestioneaza informatii secrete de stat vor intocmi planul de paza si aparare a obiectivelor, sectoarelor si locurilor care prezinta importanta deosebita pentru protectia informatiilor clasificate.

(2) Planul de paza si aparare mentionat la alin. (1) va fi inregistrat potrivit celui mai inalt nivel de secretizare a informatiilor protejate si va cuprinde totalitatea masurilor de securitate luate pentru prevenirea accesului neautorizat la acestea.

(3) Planul de paza si aparare va fi anexat programului de prevenire a scurgerii de informatii clasificate si va cuprinde:

a) date privind delimitarea si marcarea zonelor de securitate, dispunerea posturilor de paza si masurile de supraveghere a perimetrului protejat;

b) sistemul de control al accesului in zonele de securitate;

c) masurile de avertizare si alarmare pentru situatii de urgenta;

d) planul de evacuare a documentelor si modul de actiune in caz de urgenta;

e) procedura de raportare, cercetare si evidenta a incidentelor de securitate.

Art. 121. - Informatiile secrete de stat se pastreaza in containere speciale, astfel:

a) containere clasa A, autorizate la nivel national pentru pastrarea informatiilor strict secrete de importanta deosebita in zona de securitate clasa I;

b) containere clasa B, autorizate la nivel national pentru pastrarea informatiilor strict secrete si secrete in zone de securitate clasa I sau clasa a II-a.

Art. 122. - **(1)** Containerele din clasele A si B vor fi construite astfel incat sa asigure protectia impotriva patrunderii clandestine si deteriorarii sub orice forma a informatiilor.

(2) Standardele in care trebuie sa se incadreze containerele din clasele A si B se stabilesc de ORNISS.

Art. 123. - **(1)** Incaperile de securitate sunt incaperile special amenajate in zone de securitate clasa I sau clasa a II-a, in care informatiile secrete de stat pot fi pastrate pe rafturi deschise sau pot fi expuse pe harti, planse ori diagrame.

(2) Peretii, podelele, plafoanele, usile si incuietorile incaperilor de securitate vor asigura protectia echivalenta clasei containerului de securitate aprobat pentru pastrarea informatiilor clasificate potrivit nivelului de secretizare.

Art. 124. - **(1)** Ferestrele incaperilor de securitate dispuse la parter sau ultimul etaj vor fi protejate obligatoriu cu bare incastrate in beton sau asigurate antiefractie.

(2) In afara programului de lucru, usile incaperilor de securitate vor fi sigilate, iar sistemul de aerisire asigurat impotriva accesului neautorizat si introducerii materialelor incendiare.

Art. 125. - In situatii de urgenta, daca informatiile secrete de stat trebuie evacuate, se vor utiliza lazi metalice autorizate la nivel national din clasa corespunzatoare nivelului de secretizare a acestor informatii.

Art. 126. - Incuietorile folosite la containerele si incaperile de securitate in care sunt pastrate informatii secrete de stat se impart in trei grupe, astfel:

a) grupa A - incuietori autorizate pentru containerele din clasa A;

b) grupa B - incuietori autorizate pentru containerele din clasa B;

c) grupa C - incuietori pentru mobilierul de birou.

Art. 127. - Standardele mecanismelor de inchidere, a sistemelor cu cifru si incuietorilor, pe grupe de utilizare, se stabilesc de ORNISS.

Art. 128. - Cheile containerelor si incaperilor de securitate nu vor fi scoase din zonele de securitate.

Art. 129. - **(1)** In afara orelor de program, cheile de la incaperile si containerele de securitate vor fi pastrate in cutii sigilate, de catre personalul care asigura paza si apararea.

(2) Predarea si primirea cheilor de la incaperile si containerele de securitate se vor face, pe baza de semnatura, in condica special destinata - anexa nr. 11.

Art. 130. - **(1)** Pentru situatiile de urgenta, un rand de chei suplimentare sau, dupa caz, o evidenta scrisa a combinatiilor incuietorilor, vor fi pastrate in plicuri mate sigilate, in containere separate, intr-un compartiment stabilit de conducerea unitatii, sub control corespunzator.

(2) Evidenta fiecarei combinatii se va pastra in plic separat.

(3) Cheilor si plicurilor cu combinatii trebuie sa li se asigure acelasi nivel de protectie ca si informatiilor la care permit accesul.

Art. 131. - Combinatiile incuietorilor de la incaperile si containerele de securitate vor fi cunoscute de un numar restrans de persoane desemnate de conducerea unitatii.

Art. 132. - Cheile si combinatiile incuietorilor vor fi schimbate:

a) ori de cate ori are loc o schimbare de personal;

b) de fiecare data cand se constata ca au intervenit situatii de natura sa le faca vulnerabile;

c) la intervale regulate, de preferinta o data la sase luni, fara a se depasi 12 luni.

Art. 133. - **(1)** Sistemele electronice de alarmare sau de supraveghere destinate protectiei informatiilor secrete de stat vor fi prevazute cu surse de alimentare de rezerva.

(2) Orice defectiune sau interventie neautorizata asupra sistemelor de alarma sau de supraveghere

destinate protectiei informatiilor secrete de stat trebuie sa avertizeze personalul care le monitorizeaza.

(3) Dispozitivele de alarmare trebuie sa intre in functiune in cazul penetrarii peretilor, podelelor, tavanelor si deschizaturilor, sau la miscari in interiorul incaperilor de securitate.

Art. 134. - Copiatoarele si dispozitivele telefax se vor instala in incaperi special destinate si se vor folosi numai de catre persoanele autorizate, potrivit nivelului de secretizare a informatiilor la care au acces.

Art. 135. - Unitatile detinatoare de informatii secrete de stat au obligatia de a asigura protectia acestora impotriva ascultarilor neautorizate, pasive sau active.

Art. 136. - **(1)** Protectia impotriva ascultarii pasive a discutiilor confidentiale se realizeaza prin izolarea fonica a incaperilor.

(2) Protectia impotriva ascultarilor active, prin microfoane, radio-emitatori si alte dispozitive implantate, se realizeaza pe baza inspectiilor de securitate a incaperilor, accesoriilor, instalatiilor, sistemelor de comunicatii, echipamentelor si mobilierului de birou, realizate de unitatile specializate, potrivit competentelor legale.

Art. 137. - **(1)** Accesul in incaperile protejate impotriva ascultarilor se va controla in mod special.

(2) Periodic, personalul specializat in depistarea dispozitivelor de ascultare va efectua inspectii fizice si tehnice.

(3) Inspectiile fizice si tehnice vor fi organizate, in mod obligatoriu, in urma oricarei intrari neautorizate sau suspiciuni privind accesul persoanelor neautorizate si dupa executarea lucrarilor de reparatii, intretinere, zugravire sau redecorare.

(4) Nici un obiect nu va fi introdus in incaperile protejate impotriva ascultarii, fara a fi verificat in prealabil de catre personalul specializat in depistarea dispozitivelor de ascultare.

Art. 138. - **(1)** In zonele in care se poarta discutii confidentiale si care sunt asigurate din punct de vedere tehnic, nu se vor instala telefoane, iar daca instalarea acestora este absolut necesara, trebuie prevazute cu un dispozitiv de deconectare pasiv.

(2) Inspectiile de securitate tehnica in zonele prevazute in alin. (1) trebuie efectuate, in mod obligatoriu, inaintea inceperii convorbirilor, pentru identificarea fizica a dispozitivelor de ascultare si verificarea sistemelor telefonice, electrice sau de alta natura, care ar putea fi utilizate ca mediu de atac.

Art. 139. - **(1)** Echipamentele de comunicatii si dotarile din birouri, in principal cele electrice si electronice, trebuie verificate de specialisti ai autoritatilor desemnate de securitate competente, inainte de a fi folosite in zonele in care se lucreaza ori se discuta despre informatii strict secrete sau strict secrete de importanta deosebita, pentru a preveni transmiterea sau interceptarea, in afara cadrului legal, a unor informatii inteligibile.

(2) Pentru zonele mentionate la alin. (1) se va organiza o evidenta a tipului si numerelor de inventar ale echipamentului si mobilei mutate in/din interiorul incaperilor, care va fi gestionata ca material secret de stat.

SECȚIUNEA a 5-a
Protectia personalului

Art. 140. - **(1)** Unitatile detinatoare de informatii secrete de stat au obligatia de a asigura protectia personalului desemnat sa asigure securitatea acestora ori care are acces la astfel de informatii, potrivit prezentelor standarde.

(2) Masurile de protectie a personalului au drept scop:

a) sa previna accesul persoanelor neautorizate la informatii secrete de stat;

b) sa garanteze ca informatiile secrete de stat sunt distribuite detinatorilor de certificate de securitate/autorizatii de acces, cu respectarea principiului necesitatii de a cunoaste;

c) sa permita identificarea persoanelor care, prin actiunile sau inactiunile lor, pot pune in pericol securitatea informatiilor secrete de stat si sa previna accesul acestora la astfel de informatii.

(3) Protectia personalului se realizeaza prin: selectionarea, verificarea, avizarea si autorizarea accesului la informatiile secrete de stat, revalidarea, controlul si instruirea personalului, retragerea certificatului de securitate sau autorizatiei de acces.

Art. 141. - **(1)** Acordarea certificatului de securitate - anexa nr. 12 - si autorizatiei de acces la informatii clasificate - anexa nr. 13, potrivit nivelului de secretizare, este conditionata de avizul autoritatii desemnate de securitate.

(2) In vederea eliberarii certificatului de securitate/autorizatiei de acces conducatorul unitatii solicita in scris ORNISS, conform anexei nr. 14, efectuarea verificarilor de securitate asupra persoanei care urmeaza sa aiba acces la informatii secrete de stat.

(3) Solicitarea mentionata la alin. (2) va fi insotita de formularele tip, prevazute la anexele nr. 15, 16 si 17, potrivit nivelului de secretizare a informatiilor, completate de persoana in cauza, introduse in plic separat, sigilat.

(4) In functie de avizul comunicat de autoritatea desemnata, ORNISS va aproba eliberarea certificatului de securitate sau autorizatiei de acces si va incunostinta oficial conducatorul unitatii.

(5) Dupa obtinerea aprobarii mentionate la alin. (4), conducatorul unitatii va notifica la ORNISS si va elibera certificatul de securitate sau autorizatia de acces, conform art. 154.

Art. 142. - Certificatul de securitate sau autorizatia de acces se elibereaza numai in baza avizelor acordate de autoritatea desemnata de securitate in urma verificarilor efectuate asupra persoanei in cauza,

cu acordul scris al acesteia.

Art. 143. - In cadrul procedurilor de avizare trebuie acordata atentie speciala persoanelor care:

a) urmeaza sa aiba acces la informatii strict secrete si strict secrete de importanta deosebita;

b) ocupa functii ce presupun accesul permanent la un volum mare de informatii secrete de stat;

c) pot fi vulnerabile la actiuni ostile, ca urmare a importantei functiei in care vor fi numite, a mediului de relatii sau a locului de munca anterior.

Art. 144. - **(1)** Oportunitatea avizarii va fi evaluata pe baza verificarii si investigarii biografici celui in cauza.

(2) Cand persoanele urmeaza sa indeplineasca functii care le pot facilita accesul la informatii secrete de stat doar in anumite circumstante - paznici, curieri, personal de intretinere - se va acorda atentie primei verificari de securitate.

Art. 145. - Unitatile care gestioneaza informatii clasificate sunt obligate sa tina un registru de evidenta a certificatelor de securitate si autorizatiilor de acces la informatii clasificate - anexa nr. 18.

Art. 146. - **(1)** Ori de cate ori apar indicii ca detinatorul certificatului de securitate sau autorizatiei de acces nu mai indeplineste criteriile de compatibilitate privind accesul la informatiile secrete de stat, verificarile de securitate se reiau la solicitarea conducatorului unitatii adresata ORNISS.

(2) ORNISS poate solicita reluarea verificarilor, la sesizarea autoritatilor competente, in situatia in care sunt semnalate incompatibilitati privind accesul la informatii secrete de stat.

Art. 147. - Procedura de verificare in vederea acordarii accesului la informatii secrete de stat are drept scop identificarea riscurilor de securitate, aferente gestionarii informatiilor secrete de stat.

Art. 148. - **(1)** Structura/functionarul de securitate are obligatia sa puna la dispozitia persoanei selectionate formularele tip corespunzatoare nivelului de acces pentru care se solicita eliberarea certificatului de securitate/autorizatiei de acces si sa acorde asistenta in vederea completarii acestora.

(2) In functie de nivelul de secretizare a informatiilor pentru care se solicita avizul de securitate, termenele de prezentare a raspunsului de catre institutiile abilitate sa efectueze verificarile de securitate sunt:

a) pentru acces la informatii strict secrete de importanta deosebita - 90 de zile lucratoare;

b) pentru acces la informatii strict secrete - 60 de zile lucratoare;

c) pentru acces la informatii secrete - 30 de zile lucratoare.

Art. 149. - ORNISS are obligatia ca, in termen de 7 zile lucratoare de la primirea solicitarii, sa transmita ADS competente cererea tip de incepere a procedurii de verificare - anexa nr. 19, la care va anexa plicul sigilat cu formularele tip completate.

Art. 150. - **(1)** Dupa primirea formularelor, institutia abilitata va efectua verificarile in termenele prevazute la art. 148 si va comunica, in scris - anexa nr. 20, la ORNISS, avizul privind acordarea certificatului de securitate sau autorizatiei de acces la informatii clasificate.

(2) In cazul in care sunt identificate riscuri de securitate, ADS va evalua daca acestea constituie un impediment pentru acordarea avizului de securitate.

(3) In situatia in care sunt semnalate elemente relevante din punct de vedere al protectiei informatiilor secrete de stat, in luarea deciziei de acordare a avizului de securitate vor avea prioritate interesele de securitate.

Art. 151. - **(1)** In termen de 7 zile lucratoare de la primirea raspunsului de la autoritatea desemnata de securitate, ORNISS va decide asupra acordarii certificatului de securitate/autorizatiei de acces la informatii secrete de stat si va comunica unitatii solicitante - anexa nr. 21.

(2) Adresa de comunicare a deciziei ORNISS se realizeaza in trei exemplare, din care unul se transmite unitatii solicitante, iar al doilea institutiei care a efectuat verificarile.

(3) Daca avizul este pozitiv, conducatorul unitatii solicitante va elibera certificatul de securitate sau autorizatia de acces persoanei in cauza, dupa notificarea prealabila la ORNISS - anexa nr. 22.

Art. 152. - **(1)** Verificarea in vederea avizarii pentru accesul la informatii secrete de stat se efectueaza cu respectarea legislatiei in vigoare privind responsabilitatile in domeniul protectiei unor asemenea informatii, de catre urmatoarele institutii:

a) Serviciul Roman de Informatii, pentru:

- personalul propriu;

- personalul autoritatilor si institutiilor publice din zona de competenta, potrivit legii;

- personalul agentilor economici cu capital integral sau partial de stat si al persoanelor juridice de drept public sau privat, altele decat cele date in competenta institutiilor mentionate la lit. b), c) si d);

- personalul din cadrul Parchetului National Anticoruptie.@

b) Ministerul Apararii Nationale, pentru:

- personalul militar si civil propriu;

- personalul Oficiului Central de Stat pentru Probleme Speciale, Administratiei Nationale a Rezervelor de Stat si altor persoane juridice stabilite prin lege si personalul militar care isi desfasoara activitatea in strainatate;

c) Serviciul de Informatii Externe, pentru:

- personalul militar sau civil propriu;

- personalul roman al reprezentantelor diplomatice, misiunilor permanente, consulare, centrelor culturale, organismelor internationale si altor reprezentante ale statului roman in strainatate;

- cetatenii romani aflati in strainatate in cadrul unor contracte, stagii de perfectionare, programe de cercetare sau in calitate de angajati la firme;

d) Ministerul Administratiei si Internelor, Serviciul de Protectie si Paza si Serviciul de Telecomunicatii Speciale, pentru personalul propriu si al persoanelor juridice a caror activitate o coordoneaza;@

e) Ministerul Justitiei, pentru personalul propriu si al persoanelor juridice a caror activitate o coordoneaza, altul decat cel pentru care verificarea este de competenta Serviciului Roman de Informatii.@

(2) Institutiile mentionate la alin. (1) sunt abilitate sa solicite si sa primeasca informatii de la persoane juridice si fizice, in vederea acordarii avizului de acces la informatii clasificate.

_____

@Liniuta 4 de la lit. a) a alin. (1) a fost introdusa prin art. unic pct. 1 din H.G. nr. 2202/2004.

- Litera d) de la alin. (1) a fost modificata prin art. unic pct. 2 din H.G. nr. 2202/2004.

- Litera e) de la alin. (1) a fost introdusa prin art. unic pct. 3 din H.G. nr. 2202/2004.

Art. 153. - Institutiile competente in realizarea verificarilor de securitate coopereaza, pe baza de protocoale, in indeplinirea sarcinilor si obiectivelor propuse.

Art. 154. - Certificatul de securitate/autorizatia de acces se emite in doua exemplare originale, unul fiind pastrat de structura/functionarul de securitate, iar celalalt se trimite la ORNISS, care va informa institutia competenta care a efectuat verificarile.

Art. 155. - Valabilitatea certificatului de securitate/autorizatiei de acces eliberate unei persoane este de pana la patru ani, in aceasta perioada verificarile putand fi reluate oricand sunt indeplinite conditiile prevazute la art. 167.

Art. 156. - Pentru cadrele proprii, Ministerul Apararii Nationale, Ministerul de Interne, Ministerul Justitiei, Serviciul Roman de Informatii, Serviciul de Informatii Externe, Serviciul de Telecomunicatii Speciale si Serviciul de Protectie si Paza vor elabora instructiuni interne privind verificarea, avizarea, eliberarea si evidenta certificatelor de securitate/autorizatiilor de acces.

Art. 157. - Decizia privind avizarea eliberarii certificatului de securitate/autorizatiei de acces va fi luata pe baza tuturor informatiilor disponibile si va avea in vedere:

a) loialitatea indiscutabila a persoanei;

b) caracterul, obiceiurile, relatiile si discretia persoanei, care sa ofere garantii asupra:

- corectitudinii in gestionarea informatiilor secrete de stat;

- oportunitatii accesului neinsotit in compartimente, obiective, zone si locuri de securitate in care se afla informatii secrete de stat;

- respectarii reglementarilor privind protectia informatiilor secrete de stat din domeniul sau de activitate.

Art. 158. - **(1)** Principalele criterii de evaluare a compatibilitatii in acordarea avizului pentru eliberarea certificatului de securitate/autorizatiei de acces vizeaza atat trasaturile de caracter, cat si situatiile sau imprejurarile din care pot rezulta riscuri si vulnerabilitati de securitate.

(2) Sunt relevante si vor fi luate in considerare, la acordarea avizului de securitate, caracterul, conduita profesionala sau sociala, conceptiile si mediul de viata al sotului/sotiei sau concubinului/concubinei persoanei solicitante.

Art. 159. - Urmatoarele situatii imputabile atat solicitantului, cat si sotului/sotiei sau concubinului/concubinei acestuia reprezinta elemente de incompatibilitate pentru acces la informatii secrete de stat:

a) daca a comis sau a intentionat sa comita, a fost complice, a complotat sau a instigat la comiterea de acte de spionaj, terorism, tradare ori alte infractiuni contra sigurantei statului;

b) daca a incercat, a sustinut, a participat, a cooperat sau a sprijinit actiuni de spionaj, terorism ori persoane suspectate de a se incadra in aceasta categorie sau de a fi membre ale unor organizatii ori puteri straine inamice ordinii de drept din tara noastra;

c) daca este sau a fost membru al unei organizatii care a incercat, incearca sau sustine rasturnarea ordinii constitutionale prin mijloace violente, subversive sau alte forme ilegale;

d) daca este sau a fost un sustinator al vreunei organizatii prevazute la lit. c), este sau a fost in relatii apropiate cu membrii unor astfel de organizatii intr-o forma de natura sa ridice suspiciuni temeinice cu privire la increderea si loialitatea persoanei.

Art. 160. - Constituie elemente de incompatibilitate pentru accesul solicitantului la informatii secrete de stat oricare din urmatoarele situatii:

a) daca in mod deliberat a ascuns, a interpretat eronat sau a falsificat informatii cu relevanta in planul sigurantei nationale ori a mintit in completarea formularelor tip sau in cursul interviului de securitate;

b) are antecedente penale sau a fost sanctionat contraventional pentru fapte care indica tendinte infractionale;

c) are dificultati financiare serioase sau exista o discordanta semnificativa intre nivelul sau de trai si veniturile declarate;

d) consuma in mod excesiv bauturi alcoolice ori este dependent de alcool, droguri sau de alte substante interzise prin lege care produc dependenta;

e) are sau a avut comportamente imorale sau deviatii de comportament care pot genera riscul ca persoana sa fie vulnerabila la santaj sau presiuni;

f) a demonstrat lipsa de loialitate, necinste, incorectitudine sau indiscretie;

g) a incalcat reglementarile privind protectia informatiilor clasificate;

h) sufera sau a suferit de boli fizice sau psihice care ii pot cauza deficiente de discernamant confirmate

prin investigatie medicala efectuata cu acordul persoanei solicitante;

i) poate fi supus la presiuni din partea rudelor sau persoanelor apropiate care ar putea genera vulnerabilitati exploatabile de catre serviciile de informatii ale caror interese sunt ostile Romaniei si aliatilor sai.

Art. 161. - **(1)** Solicitarile pentru efectuarea verificarilor de securitate in vederea avizarii eliberarii certificatelor de securitate/autorizatiilor de acces la informatii secrete vor avea in vedere persoanele care:

a) in exercitarea atributiilor profesionale lucreaza cu date si informatii de nivel secret;

b) fac parte din personalul de executie sau administrativ si, in virtutea acestui fapt, pot intra in contact cu date si informatii de acest nivel;

c) este de presupus ca vor lucra cu date si informatii de nivel secret, datorita functiei pe care o detin;

d) se presupune ca nu pot avansa profesional in functie, daca nu au acces la astfel de informatii.

(2) Avizarea pentru acces la informatii secrete de stat, de nivel secret se va baza pe:

a) verificarea corectitudinii datelor mentionate in formularul de baza, anexa nr. 15;

b) referinte de la locurile de munca si din mediile frecventate, de la cel putin trei persoane.

(3) In situatia in care este necesara clarificarea anumitor aspecte sau la solicitarea persoanei verificate, reprezentantul institutiei abilitate sa efectueze verificarile de securitate poate avea o intrevedere cu aceasta.

Art. 162. - **(1)** Pentru eliberarea certificatelor de securitate/autorizatiilor de acces la informatii strict secrete se efectueaza verificari asupra persoanelor care:

a) in exercitarea atributiilor profesionale lucreaza cu date si informatii de nivel strict secret;

b) fac parte din personalul de executie sau administrativ si, in virtutea acestui fapt, pot intra in contact cu date si informatii de acest nivel;

c) este de presupus ca vor lucra cu date si informatii de nivel strict secret, datorita functiei pe care o detin;

d) se presupune ca nu pot avansa profesional in functie, daca nu au acces la astfel de informatii.

(2) Avizarea pentru acces la informatii strict secrete se va baza pe:

a) verificarea corectitudinii datelor personale mentionate in formularul de baza si in formularul suplimentar, anexele nr. 15 si 16;

b) referinte minime de la locurile de munca si din mediile frecventate de la cel putin trei persoane;

c) verificarea datelor prezentate in formular, despre membrii de familie;

d) investigatii la locul de munca si la domiciliu, care sa acopere o perioada de zece ani anteriori datei avizului sau incepand de la varsta de 18 ani;

e) un interviu cu persoana verificata, daca se considera ca ar putea clarifica aspecte rezultate din verificarile efectuate.

Art. 163. - **(1)** Pentru eliberarea certificatelor de securitate/autorizatiilor de acces la informatii strict secrete de importanta deosebita se efectueaza verificari asupra persoanelor care:

a) in exercitarea atributiilor profesionale lucreaza cu date si informatii de nivel strict secret de importanta deosebita;

b) fac parte din personalul de executie sau administrativ si, in virtutea acestui fapt, pot intra in contact cu informatii de acest nivel.

(2) Avizarea accesului la informatiile strict secrete de importanta deosebita se va baza pe:

a) verificarea corectitudinii datelor mentionate in formularul de baza, formularul suplimentar si formularul financiar, anexele nr. 15, 16 si 17;

b) investigatii de cunoastere a conduitei si antecedentelor la domiciliul actual si cele anterioare, la locul de munca actual si la cele anterioare, precum si la institutiile de invatamant urmate, incepand de la varsta de 18 ani, investigatii care nu se vor limita la audierea persoanelor indicate de solicitantul avizului;

c) verificari ale mediului relational pentru a identifica existenta unor riscuri de securitate in cadrul acestuia;

d) un interviu cu persoana solicitanta, pentru a detalia aspectele rezultate din verificarile efectuate;

e) in cazul in care, din verificarile intreprinse, rezulta incertitudini cu privire la sanatatea psihica sau comportamentul persoanei verificate, cu acordul acesteia poate fi supusa unui test psihologic.

Art. 164. - **(1)** Daca in cursul verificarilor, pentru orice nivel, apar informatii ce evidentiaza riscuri de securitate, se va realiza o verificare suplimentara, cu folosirea metodelor si mijloacelor specifice institutiilor cu atributii in domeniul sigurantei nationale.

(2) In cazul verificarii suplimentare mentionate la alin. (1) termenele de efectuare a verificarilor vor fi prelungite in mod corespunzator.

Art. 165. - In functie de nivelul de secretizare a informatiilor secrete de stat la care se acorda accesul, investigatia de cunoastere a antecedentelor va avea in vedere, gradual, urmatoarele:

a) consultarea registrelor de stare civila pentru verificarea datelor personale in vederea stabilirii, fara dubiu, a identitatii persoanei solicitante;

b) verificarea cazierului judiciar, in evidentele centrale si locale ale politiei, in baza de date a Registrului Comertului, precum si in alte evidente;

c) stabilirea nationalitatii persoanei si cetateniei prezente si anterioare;

d) confirmarea pregatirii in scolile, universitatile si alte institutii de invatamant urmate de titular, de la implinirea varstei de 18 ani;

e) cunoasterea conduitei la locul de munca actual si la cele anterioare, cu referinte obtinute din dosarele de angajare, aprecierile anuale asupra performantelor si eficientei activitatii, ori furnizate de sefii institutiilor, sefii de compartimente sau colegi;

f) organizarea de interviuri si discutii cu persoane care pot face aprecieri asupra trecutului, activitatii, comportamentului si corectitudinii persoanei verificate;

g) cunoasterea comportarii pe timpul serviciului militar si a modalitatii in care a fost trecut in rezerva;

h) existenta unor riscuri de securitate datorate unor eventuale presiuni exercitate din strainatate;

i) solvabilitatea si reputatia financiara a persoanei;

j) stabilirea indiciilor si obtinerea de probe conform carora persoana solicitanta este sau a fost membru ori afiliat al vreunei organizatii, asociatii, miscari, grupari straine sau autohtone, care au sprijinit sau au sustinut comiterea unor acte de violenta, in scopul afectarii drepturilor altor persoane, sau care incearca sa schimbe ordinea de stat prin mijloace neconstitutionale.

Art. 166. - **(1)** In cazul in care o persoana detine certificat de securitate/autorizatie de acces la informatii nationale clasificate, acesteia i se poate elibera si certificat de securitate pentru acces la informatii NATO clasificate valabil pentru acelasi nivel de secretizare sau pentru un nivel inferior.

(2) Daca informatiile NATO clasificate la care se solicita acces in conditiile alin. (1) sunt de nivel superior celui pentru care persoana in cauza detine certificat de securitate/autorizatie de acces se vor efectua verificarile necesare, potrivit standardelor in vigoare.

(3) Valabilitatea certificatului/autorizatiei eliberate in conditiile alin. (1) si (2) inceteaza la expirarea termenului de valabilitate al certificatului/autorizatiei initiale.

Art. 167. - **(1)** Revalidarea avizului privind accesul la informatii clasificate presupune reverificarea persoanei detinatoare a unui certificat de securitate/autorizatie de acces in vederea mentinerii sau retragerii acesteia.

(2) Revalidarea poate avea loc la solicitarea unitatii in care persoana isi desfasoara activitatea, sau a ORNISS, in oricare din urmatoarele situatii:

a) atunci cand pentru indeplinirea sarcinilor de serviciu ale persoanei detinatoare este necesar accesul la informatii de nivel superior;

b) la expirarea perioadei de valabilitate a certificatului de securitate/autorizatiei de acces detinute anterior;

c) in cazul in care apar modificari in datele de identificare ale persoanei;

d) la aparitia unor riscuri de securitate din punct de vedere al compatibilitatii accesului la informatii clasificate.

Art. 168. - La solicitarea revalidarii nu se elibereaza un nou certificat de securitate/autorizatie de acces, in urmatoarele situatii:

a) in cazul in care se constata neconcordante intre datele declarate in formularele tip si cele reale;

b) in cazul in care, pe parcursul perioadei de valabilitate a certificatului de securitate/autorizatiei de acces s-au evidentiat riscuri de securitate;

c) in cazul in care ORNISS solicita acest lucru, in mod expres.

Art. 169. - Pentru revalidarea accesului la informatii secrete de stat se deruleaza aceleasi activitati ca si la acordarea avizului initial, verificarile raportandu-se la perioada scursa de la eliberarea certificatului de securitate sau autorizatiei de acces anterioare.

Art. 170. - **(1)** Persoanele carora li se elibereaza certificate de securitate/autorizatii de acces vor fi instruite, obligatoriu, cu privire la protectia informatiilor clasificate, inaintea inceperii activitatii si ori de cate ori este nevoie.

(2) Activitatea de pregatire se efectueaza planificat, in scopul prevenirii, contracararii si eliminarii riscurilor si amenintarilor la adresa securitatii informatiilor clasificate.

(3) Pregatirea personalului se realizeaza diferentiat, potrivit nivelului de secretizare a informatiilor la care certificatul de securitate sau autorizatia de acces permite accesul si va fi inscrisa in fisa individuala de pregatire, care se pastreaza la structura/functionarul de securitate.

(4) Toate persoanele incadrate in functii care presupun accesul la informatii clasificate trebuie sa fie instruite temeinic, atat in perioada premergatoare numirii in functie, cat si la intervale prestabilite, asupra necesitatii si modalitatilor de asigurare a protectiei acestor informatii.

(5) Dupa fiecare instruire, persoana care detine certificat de securitate sau autorizatie de acces va semna ca a luat act de continutul reglementarilor privind protectia informatiilor secrete de stat.

Art. 171. - **(1)** Pregatirea personalului urmareste insusirea corecta a standardelor de securitate si a modului de implementare eficienta a masurilor de protectie a informatiilor clasificate

(2) Organizarea si coordonarea activitatii de pregatire a structurilor/functionarilor de securitate sunt asigurate de autoritatile desemnate de securitate.

Art. 172. - **(1)** Planificarea si organizarea activitatii de pregatire a personalului se realizeaza de catre structura/functionarul de securitate.

(2) Autoritatile desemnate de securitate vor controla, potrivit competentelor, modul de realizare a activitatii de pregatire a personalului care acceseaza informatii secrete de stat.

Art. 173. - **(1)** Pregatirea individuala a persoanelor care detin certificate de securitate/autorizatii de acces se realizeaza in raport cu atributiile profesionale.

(2) Toate persoanele care gestioneaza informatii clasificate au obligatia sa cunoasca reglementarile privind protectia informatiilor clasificate si procedurile interne de aplicare a masurilor de securitate specifice.

Art. 174. - **(1)** Pregatirea personalului se realizeaza sub forma de lectii, informari, prelegeri, simpozioane, schimb de experienta, seminarii, sedinte cu caracter aplicativ si se poate finaliza prin verificari sau certificari ale nivelului de cunostinte.

(2) Activitatile de pregatire vor fi organizate de structura/functionarul de securitate, conform tematicilor cuprinse in programele aprobate de conducerea unitatii.

Art. 175. - Certificatul de securitate sau autorizatia de acces isi inceteaza valabilitatea si se va retrage in urmatoarele cazuri:

a) la solicitarea ORNISS;

b) prin decizia conducatorului unitatii care a eliberat certificatul/autorizatia;

c) la solicitarea autoritatii desemnate de securitate competente;

d) la plecarea din unitate sau la schimbarea locului de munca al detinatorului in cadrul unitatii, daca noul loc de munca nu presupune lucrul cu astfel de informatii secrete de stat;

e) la schimbarea nivelului de acces.

Art. 176. - La retragerea certificatului de securitate sau autorizatiei de acces, in cazurile prevazute la art. 175 lit. a)-d), angajatului i se va interzice accesul la informatii secrete de stat, iar conducerea unitatii va notifica despre aceasta la ORNISS.

Art. 177. - Dupa luarea deciziei de retragere, unitatea va solicita ORNISS inapoierea exemplarului 2 al certificatului de securitate sau al autorizatiei de acces, dupa care va distruge ambele exemplare, pe baza de proces-verbal.

SECȚIUNEA a 6-a

Accesul cetatenilor straini, al cetatenilor romani care au si cetatenia altui stat, precum si al persoanelor apatride la informatiile secrete de stat si in locurile in care se desfasoara activitati, se expun obiecte sau se executa lucrari din aceasta categorie

Art. 178. - Cetatenii straini, cetatenii romani care au si cetatenia altui stal, precum si persoanele apatride pot avea acces la informatii secrete de stat, cu respectarea principiului necesitatii de a cunoaste si a conventiilor, protocoalelor, contractelor si altor intelegeri incheiate in conditiile legii.

Art. 179. - **(1)** Persoanele prevazute la art. 178 vor fi verificate si avizate conform prezentelor standarde, la solicitarea conducatorului unitatii in cadrul careia acestea urmeaza sa desfasoare activitati care presupun accesul la informatii secrete de stat.

(2) Conducatorul unitatii va elibera persoanelor respective o autorizatie de acces corespunzatoare nivelului de secretizare a informatiilor la care urmeaza sa aiba acces, valabila numai pentru perioada desfasurarii activitatilor comune, in baza acordului comunicat de ORNISS.

Art. 180. - **(1)** Persoanele prevazute la art. 178 care desfasoara activitati de asistenta tehnica, consultanta, colaborare stiintifica ori specializare vor purta ecusoane distincte fata de cele folosite de personalul propriu si vor fi insotite permanent de persoane anume desemnate de conducerea unitatii respective.

(2) Conducatorul unitatii este obligat sa delimiteze strict sectoarele si compartimentele in care persoanele mentionate la art. 178 pot avea acces si va stabili masuri pentru prevenirea prezentei acestora in alte locuri in care se gestioneaza informatii secrete de stat.

Art. 181. - **(1)** Structura/functionarul de securitate are obligatia de a instrui persoanele prevazute la art. 178 in legatura cu regulile pe care trebuie sa le respecte privind protectia informatiilor secrete de stat.

(2) Autorizatia de acces se va elibera numai dupa insusirea reglementarilor privind protectia informatiilor clasificate si semnarea angajamentului de confidentialitate.

Art. 182. - Nerespectarea de catre persoanele prevazute la art. 178 a regulilor privind protectia informatiilor clasificate va determina, obligatoriu, retragerea autorizatiei de acces.

CAPITOLUL V

CONDITIILE DE FOTOGRAFIERE, FILMARE, CARTOGRAFIERE SI EXECUTARE A UNOR LUCRARI DE ARTE PLASTICE IN OBIECTIVE SAU LOCURI CARE PREZINTA IMPORTANTA DEOSEBITA PENTRU PROTECTIA INFORMATIILOR SECRETE DE STAT

Art. 183. - **(1)** Este interzisa fotografierea, filmarea, cartografierea sau executarea de lucrari de arte plastice pe teritoriul Romaniei, in obiective, zone sau locuri de importanta deosebita pentru protectia informatiilor secrete de stat, fara autorizatie speciala eliberata de catre ORNISS, care va tine evidenta acestora, conform anexei nr. 23.

(2) Autorizatia speciala va fi eliberata de catre ORNISS in baza avizului dat de ADS, precum si de autoritatile sau institutiile care au obiective, zone si locuri de importanta pentru protectia informatiilor clasificate in arealul in care urmeaza sa se desfasoare activitati de aceasta natura.

(3) Obiectivele si mijloacele prevazute la art. 17 din Legea nr. 182/2002 pot fi filmate si fotografiate de catre personalul militar, pentru nevoile interne ale institutiilor militare, pe baza aprobarii scrise a ministrilor sau conducatorilor institutiilor respective, pentru obiectivele, zonele sau locurile din competenta lor.

Art. 184. - Trupele Ministerului Apararii Nationale, Ministerului de Interne si Serviciului Roman de Informatii, aflate la instructie, in aplicatii ori in interiorul obiectivelor prevazute la art. 17 din Legea nr. 182/2002, pot fi fotografiate sau filmate in scopuri educative si de pregatire militara, cu aprobarea conducatorilor acestor institutii sau a imputernicitilor desemnati.

Art. 185. - Fotografierea, filmarea, cartografierea sau executarea de lucrari de arte plastice in zonele de securitate si administrative ale unitatilor detinatoare de secrete de stat este permisa numai cu aprobarea scrisa a imputernicitilor abilitati sa atribuie niveluri de secretizare conform art. 19 din Legea 182/2002, potrivit competentelor materiale.

Art. 186. - **(1)** Cererea adresata ORNISS pentru eliberarea autorizatiei speciale de filmare, fotografiere, cartografiere sau de executare a lucrarilor de arte plastice va cuprinde, obligatoriu, mentionarea obiectului si locului activitatii, aparatura folosita, perioada de timp in care urmeaza a se realiza, datele de identitate ale persoanei care le va efectua, precum si aprobarea prevazuta la art. 185.

(2) Termenul de raspuns este de 60 de zile lucratoare de la data primirii cererii. Pentru zborurile aerofotogrammetrice efectuate la scari de zbor mai mari de 1:20.000 in scopul realizarii pe planuri topografice si cadastrale, termenul este de 30 de zile lucratoare.@

(3) Titularii autorizatiei speciale sunt obligati sa se prezinte, inaintea inceperii lucrarilor, la conducatorii institutiilor unde acestea vor fi executate, pentru a se pune de acord cu privire la modalitatea de actiune si verificarea aparaturii ce va fi folosita.

_____

@Alineatul (2) a fost modificat prin art. unic pct. 1 din H.G. nr. 185/2005.

Art. 187. - Daca solicitantul poseda autorizatie de nivel corespunzator obiectivului vizat, autorizatia speciala va fi eliberata in termen de 15 zile lucratoare de la data primirii solicitarii, cu respectarea principiului nevoii de a cunoaste.

Art. 188. - Obiectivele, zonele si locurile in care fotografierea, filmarea, cartografierea sau executarea de lucrari de arte plastice se efectueaza numai cu autorizare vor fi marcate cu indicatoare de interdictie in acest sens, care vor fi instalate prin grija institutiilor carora le apartin, cu avizul de specialitate al organelor administratiei publice locale.

Art. 189. - **(1)** Emiterea, detinerea sau folosirea de date si documente geodezice, topo-fotogrammetrice si cartografice, ce constituie secrete de stat, urmeaza, in privinta clasificarii, marcarii, inscriptionarii, procesarii, manipularii, evidentei, intocmirii, multiplicarii, transmiterii, pastrarii, transportului si distrugerii acestora, regimul prevazut de reglementarile in vigoare privitoare la protectia informatiilor clasificate in Romania.

(2) Ministerele si celelalte organe ale administratiei publice centrale si locale, care intocmesc documente geodezice, topo-fotogrammetrice si cartografice cu caracter secret de stat, le vor nominaliza in listele proprii de informatii clasificate, potrivit dispozitiilor legale in vigoare.

Art. 190. - **(1)** Activitatea de aerofotografiere cu camere fotogrammetrice digitale sau analogice a teritoriului Romaniei, la o scara de zbor mai mare de 1:20.000, se efectueaza pe baza autorizatiei speciale eliberate de ORNISS si in prezenta reprezentantului Ministerului Apararii Nationale.

(2) In vederea eliberarii autorizatiei mentionate la alin. (1), cererea adresata ORNISS trebuie sa contina, pe langa datele prevazute la art. 186 alin. (1), si scara de zbor la care vor fi efectuate activitatile de aerofotografiere.

(3) Activitatile de developare a materialului fotografic si scanarea negativelor, dupa caz, se pot realiza, in prezenta reprezentantului Ministerului Apararii Nationale, de catre persoane juridice care indeplinesc conditiile legale privind protectia informatiilor clasificate.

(4) Materialele obtinute din activitatile de aerofotografiere prevazute la alin. (1) se predau persoanelor juridice autorizate, pe baza de documente justificative, in prezenta reprezentantului Ministerului Apararii Nationale.

(5) ORNISS tine evidenta autorizatiilor speciale si dispune retragerea acestora, la propunerea motivata a organelor de control abilitate.

(6) Developarea materialului fotografic si scanarea negativelor de catre persoanele juridice autorizate se realizeaza exclusiv pe teritoriul national.

(7) Materialele rezultate in urma procesului de developare si scanare, precum si cele rezultate in urma activitatilor de aerofotografiere cu camere fotogrammetrice digitale sunt declasificate, cu avizul Autoritatilor Desemnate de Securitate (ADS), de catre Ministerul Apararii Nationale, in termen de 30 de zile lucratoare de la primirea acestora.

(8) In termenul prevazut la alin. (7) produsele finale rezultate in urma declasificarii se vor preda la ORNISS, prin grija reprezentantului Ministerului Apararii Nationale, pentru a fi puse la dispozitie beneficiarului.

(9) Se excepteaza de la obligatia indeplinirii procedurii prevazute la alin. (1)-(8) activitatile de aerofotografiere, efectuate pe teritoriul Romaniei, la o scara de zbor mai mica sau egala cu 1:20.000.@

_____

@Articolul a fost modificat prin art. unic pct. 2 din H.G. nr. 185/2005.

CAPITOLUL VI
EXERCITAREA CONTROLULUI ASUPRA MASURILOR PRIVITOARE LA PROTECTIA INFORMATIILOR CLASIFICATE

Art. 191. - **(1)** Serviciul Roman de Informatii, prin unitatea sa specializata, are competenta generala de exercitare a controlului asupra modului de aplicare a masurilor de protectie de catre institutiile publice si

unitatile detinatoare de informatii clasificate.

(2) Activitatea de control in cadrul Ministerului Apararii Nationale, Ministerului de Interne, Ministerului de Justitie, Serviciului Roman de Informatii, Serviciului de Informatii Externe, Serviciului de Protectie si Paza si Serviciului de Telecomunicatii Speciale se reglementeaza prin ordine ale conducatorilor acestor institutii, potrivit legii.

(3) Controlul privind masurile de protectie a informatiilor clasificate in cadrul Parlamentului, Administratiei Prezidentiale, Guvernului si Consiliului Suprem de Aparare a Tarii se organizeaza conform legii.

(4) Activitatea de control in cadrul reprezentantelor Romaniei in strainatate se reglementeaza si se realizeaza de catre Serviciul de Informatii Externe.

Art. 192. - Controlul are ca scop:

a) evaluarea eficientei masurilor concrete de protectie adoptate la nivelul detinatorilor de informatii clasificate, in conformitate cu legea, cu prevederile prezentelor standarde si altor norme in materie, precum si cu programele de prevenire a scurgerii de informatii clasificate;

b) identificarea vulnerabilitatilor existente in sistemul de protectie a informatiilor clasificate, care ar putea conduce la compromiterea acestor informatii, in vederea luarii masurilor de prevenire necesare;

c) luarea masurilor de remediere a deficientelor si de perfectionare a cadrului organizatoric si functional la nivelul structurii controlate;

d) constatarea cazurilor de nerespectare a normelor de protectie a informatiilor clasificate si aplicarea sanctiunilor contraventionale sau, dupa caz, sesizarea organelor de urmarire penala, in situatia in care fapta constituie infractiune;

e) informarea Consiliului Suprem de Aparare a Tarii si Parlamentului cu privire la modul in care unitatile detinatoare de informatii clasificate aplica reglementarile in materie.

Art. 193. - **(1)** Fiecare actiune de control se incheie printr-un document de constatare, intocmit de echipa/persoana care l-a efectuat.

(2) In cazul in care controlul releva fapte si disfunctionalitati de natura sa reprezinte riscuri majore de securitate pentru protectia informatiilor clasificate va fi informat, de indata, Consiliul Suprem de Aparare a Tarii, iar institutia controlata va dispune masuri imediate de remediere a deficientelor constatate, va initia cercetarea administrativa si, dupa caz, va aplica masurile sanctionatorii si va sesiza organele de urmarire penala, in situatia in care rezulta indicii ca s-ar fi produs infractiuni.

Art. 194. - In functie de obiectivele urmarite, controalele pot fi:

a) controale de fond, care urmaresc verificarea intregului sistem organizatoric, structural si functional de protectie a informatiilor clasificate;

b) controale tematice, care vizeaza anumite domenii ale activitatii de protectie a informatiilor clasificate;

c) controale in situatii de urgenta, care au ca scop verificarea unor aspecte punctuale, stabilite ca urmare a identificarii unui risc de securitate.

Art. 195. - In functie de modul in care sunt stabilite si organizate, controalele pot fi:

a) planificate;

b) inopinate;

c) determinate de situatii de urgenta.

Art. 196. - Conducatorii unitatilor care fac obiectul controlului au obligatia sa puna la dispozitia echipelor de control toate informatiile solicitate privind modul de aplicare a masurilor prevazute de lege pentru protectia informatiilor clasificate.

Art. 197. - Conducatorii unitatilor detinatoare de informatii clasificate au obligatia sa organizeze anual si ori de cate ori este nevoie controale interne

CAPITOLUL VII
SECURITATEA INDUSTRIALA

SECȚIUNEA 1
Dispozitii generale

Art. 198. - Prevederile prezentului capitol se vor aplica tuturor persoanelor juridice de drept public sau privat care desfasoara ori solicita sa desfasoare activitati contractuale ce presupun accesul la informatii clasificate.

SECȚIUNEA a 2-a
Atributiile Oficiului Registrului National al Informatiilor Secrete de Stat si ale autoritatilor desemnate de securitate in domeniul protectiei informatiilor clasificate care fac obiectul activitatilor contractuale

Art. 199. - In domeniul protectiei informatiilor clasificate care fac obiectul activitatilor contractuale, ORNISS are urmatoarele atributii:

a) stabileste strategia de implementare unitara la nivel national a masurilor de protectie a informatiilor clasificate care fac obiectul activitatilor contractuale;

b) elibereaza autorizatia si certificatul de securitate industriala, la cererea persoanelor juridice interesate;

c) gestioneaza, la nivel national, evidentele privind: persoanele juridice detinatoare de autorizatii de securitate industriala; persoanele juridice detinatoare de certificate de securitate industriala; persoanele fizice care detin certificate de securitate sau autorizatii de acces eliberate in scopul negocierii sau executarii unui contract clasificat.

Art. 200. - In sfera lor de competenta legala, autoritatile desemnate de securitate au urmatoarele atributii:

a) efectueaza verificarile de securitate necesare acordarii avizului de securitate industriala, pe care il transmite la ORNISS in vederea eliberarii autorizatiei sau, dupa caz, a certificatului de securitate industriala;

b) asigura asistenta de specialitate obiectivelor industriale in vederea implementarii standardelor de securitate in domeniul protectiei informatiilor clasificate vehiculate in cadrul activitatilor industriale;

c) desfasoara activitati de pregatire a personalului cu atributii pe linia protectiei informatiilor clasificate, vehiculate in cadrul activitatilor industriale;

d) efectueaza verificari in situatiile in care s-au semnalat incalcari ale reglementarilor de protectie, distrugeri, disparitii, dezvaluiri neautorizate de informatii clasificate, furnizate sau produse in cadrul unui contract clasificat;

e) se asigura ca fiecare obiectiv industrial, in cadrul caruia urmeaza sa fie gestionate informatii clasificate, a desemnat o structura/functionar de securitate in vederea exercitarii efective a atributiilor pe linia protectiei acestora, in cadrul contractelor clasificate;

f) monitorizeaza, in conditiile legii, modul de asigurare a protectiei informatiilor clasificate in procesul de negociere si derulare a contractelor, iar in cazul in care constata factori de risc si vulnerabilitati, informeaza imediat ORNISS si propune masurile necesare,

g) avizeaza programele de prevenire a scurgerii informatiilor clasificate din obiectivele industriale, anexele de securitate ale contractelor clasificate si monitorizeaza respectarea prevederilor acestora;

h) efectueaza controale de securitate si informeaza ORNISS asupra concluziilor rezultate;

i) verifica si prezinta ORNISS propuneri de solutionare a sesizarilor, reclamatiilor si observatiilor referitoare la modul de aplicare si respectare a standardelor de protectie in cadrul contractelor clasificate.

SECȚIUNEA a 3-a

Protectia informatiilor clasificate care fac obiectul activitatilor contractuale

Art. 201. - **(1)** Clauzele si procedurile de protectie vor fi stipulate in anexa de securitate a fiecarui contract clasificat, care presupune acces la informatii clasificate.

(2) Anexa de securitate prevazuta la alin. (1) va fi intocmita de partea contractanta detinatoare de informatii clasificate ce vor fi utilizate in derularea contractului clasificat.

(3) Clauzele si procedurile de protectie vor fi supuse, periodic, inspectiilor si verificarilor de catre autoritatea desemnata de securitate competenta.

Art. 202. - Partea contractanta detinatoare de informatii clasificate ce vor fi utilizate in derularea unui contract este responsabila pentru clasificarea si definirea tuturor componentelor acestuia, in conformitate cu normele in vigoare, sens in care poate solicita sprijin de la ADS, conform competentelor materiale stabilite prin lege.

Art. 203. - La clasificarea contractelor se vor aplica urmatoarele reguli generale:

a) in toate stadiile de planificare si executie, contractul se clasifica pe niveluri corespunzatoare, in functie de continutul informatiilor;

b) clasificarile se aplica numai acelor parti ale contractului care trebuie protejate;

c) cand in derularea unui contract se folosesc informatii din mai multe surse, cu niveluri de clasificare diferite, contractul va fi clasificat in functie de nivelul cel mai inalt al informatiilor, iar masurile de protectie vor fi stabilite in mod corespunzator;

d) declasificarea sau trecerea la o alta clasa sau nivel de secretizare a unei informatii din cadrul contractului se aproba de conducatorul persoanei juridice care a autorizat clasificarea initiala.

Art. 204. - In cazul in care apare necesitatea protejarii informatiilor dintr-un contract care, anterior, nu a fost necesar a fi clasificat, contractorul are obligatia declansarii procedurilor de clasificare si protejare conform reglementarilor in vigoare.

Art. 205. - In cazul in care contractantul cedeaza unui subcontractant realizarea unei parti din contractul clasificat, se va asigura ca acesta detine autorizatie sau certificat de securitate industriala si este obligat sa instiinteze contractorul, iar la incheierea subcontractului sa prevada clauze si proceduri de protectie in conformitate cu prevederile prezentelor standarde.

Art. 206. - **(1)** In procesul de negociere a unui contract clasificat pot participa doar reprezentanti autorizati ai obiectivelor industriale care detin autorizatie de securitate industriala eliberata de catre ORNISS, care va tine evidenta acestora.

(2) Autorizatiile de securitate industriala se elibereaza pentru fiecare contract clasificat in parte.

(3) In cazul in care obiectivul industrial nu detine autorizatii de securitate industriala pentru participarea la negocierea acelui contract, este obligatorie initierea procedurii de autorizare.

Art. 207. - **(1)** Invitatiile la licitatii sau prezentari de oferte, in cazul contractelor clasificate, trebuie sa contina o clauza prin care potentialul ofertant este obligat sa inapoieze documentele clasificate care i-au

fost puse la dispozitie, in cazul in care nu depune oferta pana la data stabilita sau nu castiga competitia intr-un termen precizat de organizator, care sa nu depaseasca 15 zile de la comunicarea rezultatului.

(2) In situatiile mentionate la alin (1), ofertantul care a pierdut licitatia are obligatia sa pastreze confidentialitatea informatiilor la care a avut acces.

Art. 208. - Contractorul pastreaza evidenta tuturor participantilor la intalnirile de negociere, datele de identificare ale acestora si angajamentele de confidentialitate, organizatiile pe care le reprezinta, tipul si scopul intalnirilor, precum si informatiile la care acestia au avut acces

Art. 209. - Contractantii care intentioneaza sa deruleze activitati industriale cu subcontractanti sunt obligati ia respecte procedurile prevazute in acest capitol sa respecte procedurile prevazute in acest capitol.

Art. 210. - Contractantul si subcontractantii sunt obligati sa implementeze si sa respecte toate masurile de protectie a informatiilor clasificate puse la dispozitie sau care au fost generate pe timpul derularii contractelor.

Art. 211. - Autoritatile desemnate de securitate vor verifica, potrivit competentelor, daca obiectivul industrial indeplineste urmatoarele cerinte:

a) poseda structura/functionar de securitate responsabila cu protectia informatiilor clasificate care fac obiectul activitatilor contractuale;

b) asigura sprijinul necesar pentru efectuarea inspectiilor de securitate periodice, pe intreaga durata a contractului clasificat;

c) nu permite diseminarea, fara autorizatie scrisa din partea emitentului, a nici unei informatii clasificate ce i-a fost incredintata in cadrul derularii unui contract clasificat;

d) aproba accesul la informatiile vehiculate in cadrul contractului clasificat numai persoanelor care detin certificat de securitate sau autorizatie de acces, in conformitate cu principiul necesitatii de a cunoaste;

e) dispune de posibilitatile necesare pentru a informa asupra oricarei compromiteri, divulgari, distrugeri, sustrageri, sabotaje sau activitati subversive ori altor riscuri la adresa securitatii informatiilor clasificate vehiculate sau a persoanelor angajate in derularea contractului respectiv si orice schimbari privind proprietatea, controlul sau managementul obiectivului industrial cu implicatii asupra statutului de securitate al acestuia;

f) impune subcontractantilor obligatii de securitate similare cu cele aplicate contractantului;

g) nu utilizeaza in alte scopuri decat cele specifice contractului informatiile clasificate la care are acces, fara permisiunea scrisa a emitentului;

h) inapoiaza toate informatiile clasificate ce i-au fost incredintate, precum si pe cele generate pe timpul derularii contractului, cu exceptia cazului in care asemenea informatii au fost distruse autorizat sau pastrarea lor a fost autorizata de catre contractor pentru o perioada de timp strict determinata;

i) respecta procedura stabilita pentru protectia informatiilor clasificate legate de contract.

Art. 212. - Dupa adjudecarea contractului clasificat, contractantul are obligatia de a informa ORNISS, in vederea initierii procedurii de obtinere a certificatului de securitate industriala.

Art. 213. - Contractul clasificat va putea fi pus in executare numai in conditiile in care:

a) ORNISS a emis certificatul de securitate industriala;

b) au fost eliberate certificate de securitate sau autorizatii de acces pentru persoanele care, in indeplinirea sarcinilor ce le revin, necesita acces la informatii secrete de stat;

c) personalul autorizat al contractantului a fost instruit asupra reglementarilor de securitate industriala de catre structura/functionarul de securitate si a semnat fisa individuala de pregatire.

SECȚIUNEA a 4-a

Procedura de verificare, avizare si certificare a obiectivelor industriale care negociaza si deruleaza contracte clasificate

Art. 214. - Verificarea, avizarea si eliberarea autorizatiei si certificatului de securitate industriala reprezinta ansamblul procedural de securitate ce se aplica numai obiectivelor industriale care au sau vor avea acces la informatii clasificate in cadrul contractelor sau subcontractelor secrete de stat, incheiate cu detinatorii unor astfel de informatii.

Art. 215. - **(1)** Pentru participarea la negocieri in vederea incheierii unui contract clasificat, conducatorul obiectivului industrial adreseaza ORNISS o cerere pentru eliberarea autorizatiei de securitate industriala - anexa nr. 24, la care anexeaza chestionarul de securitate industriala - anexa nr. 25.

(2) Dupa obtinerea avizului de la autoritatea desemnata de securitate competenta, ORNISS elibereaza autorizatia de securitate industriala - anexa nr. 28.

(3) Evidenta autorizatiilor de securitate industriala eliberate potrivit alin. (2) se realizeaza conform anexei nr. 31.

Art. 216. - **(1)** Pentru derularea contractelor clasificate, ORNISS elibereaza obiectivelor industriale, certificate de securitate industriala - anexa nr. 29.

(2) Procedura de avizare a eliberarii certificatului de securitate industriala se realizeaza pe baza cererii pentru eliberarea certificatului de securitate industriala - anexa nr. 30, chestionarului de securitate - anexele nr. 26 si 27 si a copiei anexei de securitate mentionata la art. 201.

(3) ORNISS va tine evidenta certificatelor de securitate industriala potrivit anexei nr. 32.

Art. 217. - Activitatea de verificare in vederea eliberarii autorizatiei si a certificatelor de securitate trebuie

sa asigure indeplinirea urmatoarelor obiective principale:
a) prevenirea accesului persoanelor neautorizate la informatii clasificate;
b) garantarea ca informatiile clasificate sunt distribuite pe baza existentei certificatului de securitate industriala si a principiului necesitatii de a cunoaste;
c) identificarea persoanelor care, prin actiunile lor, pot pune in pericol protectia informatiilor clasificate si interzicerea accesului acestora la astfel de informatii;
d) garantarea faptului ca obiectivele industriale au capacitatea de a proteja informatiile clasificate in procesul de negociere, respectiv de derulare a contractului.
Art. 218. - **(1)** Pentru a i se elibera autorizatia si certificatul de securitate, obiectivul industrial trebuie sa indeplineasca urmatoarele cerinte:
a) sa posede program de prevenire a scurgerii de informatii clasificate, avizat conform reglementarilor in vigoare;
b) sa fie stabil din punct de vedere economic;
c) sa nu fi inregistrat o greseala de management cu implicatii grave asupra starii de securitate a informatiilor clasificate pe care le gestioneaza;
d) sa fi respectat obligatiile de securitate din cadrul contractelor clasificate derulate anterior;
e) personalul implicat in derularea contractului sa detina certificat de securitate de nivel egal celui al informatiilor vehiculate in cadrul contractului clasificat.
(2) Neindeplinirea cerintelor mentionate la alin (1), precum si furnizarea intentionata a unor informatii inexacte in completarea chestionarului sau in documentele prezentate in vederea certificarii constituie elemente de incompatibilitate in procesul de eliberare a autorizatiei sau certificatului de securitate industriala.
Art. 219. - Obiectivul industrial nu este considerat stabil din punct de vedere economic daca:
a) este in proces de lichidare;
b) este in stare de faliment ori se afla in procedura reorganizarii judiciare sau a falimentului;
c) este implicat intr-un litigiu care ii afecteaza stabilitatea economica;
d) nu isi indeplineste obligatiile financiare catre stat;
e) nu si-a indeplinit la timp, in mod sistematic, obligatiile financiare catre persoane fizice sau juridice.
Art. 220. - **(1)** Un obiectiv industrial nu corespunde din punct de vedere al protectiei informatiilor clasificate daca se constata ca prezinta riscuri de securitate.
(2) Sunt considerate riscuri de securitate:
a) derularea unor activitati ce contravin intereselor de siguranta nationala sau angajamentelor pe care Romania si le-a asumat in cadrul acordurilor bilaterale sau multinationale;
b) relatiile cu persoane fizice sau juridice straine ce ar putea aduce prejudicii intereselor statului roman;
c) asociatiile, persoane fizice si juridice, care pot reprezenta factori de risc pentru interesele de stat ale Romaniei.
Art. 221. - **(1)** Pentru eliberarea autorizatiei sau certificatului de securitate industriala, solicitantul va transmite la ORNISS urmatoarele documente:
a) cererea de eliberare a autorizatiei, respectiv a certificatului de securitate industriala;
b) chestionarul de securitate completat, introdus intr-un plic separat, sigilat.
(2) Pentru eliberarea certificatului de securitate industriala, solicitantul va atasa si o copie a anexei de securitate.
Art. 222. - In termen de 7 zile lucratoare de la primirea cererii, ORNISS va solicita autoritatii desemnate de securitate competente sa efectueze verificarile de securitate.
Art. 223. - Avizul de securitate eliberat de autoritatea desemnata de securitate competenta trebuie sa garanteze ca:
a) agentul economic nu prezinta riscuri de securitate;
b) sunt aplicate in mod corespunzator masurile de securitate fizica, prevazute de reglementarile in vigoare, precum si normele privind accesul persoanelor la informatii clasificate;
c) obiectivul industrial este solvabil din punct de vedere financiar;
d) obiectivul industrial nu a fost si nu este implicat sub nici o forma in activitatea unor organizatii, asociatii, miscari, grupari de persoane straine sau autohtone care au adoptat sau adopta o politica de sprijinire sau aprobare a comiterii de acte de sabotaj, subversive sau teroriste.
Art. 224. - Verificarile de securitate se realizeaza astfel:
a) verificarea de securitate de nivel I - pentru eliberarea avizului necesar autorizatiei de securitate industriala;
b) verificarea de securitate de nivel II - pentru eliberarea avizului necesar certificatului de securitate industriala de nivel secret;
c) verificarea de securitate de nivel III - pentru eliberarea avizului necesar certificatului de securitate industriala de nivel strict secret;
d) verificarea de securitate de nivel IV - pentru eliberarea avizului necesar certificatului de securitate industriala de nivel strict secret de importanta deosebita.
Art. 225. - In cadrul certificarii de securitate se desfasoara urmatoarele activitati:
(1) Pentru verificarile de securitate de nivel I:
a) verificarea corectitudinii datelor consemnate in chestionarul de securitate industriala, conform anexei

nr. 25;

b) verificarea modului de aplicare a prevederilor programului de prevenire a scurgerii de informatii clasificate;

c) evaluarea statutului de securitate a fiecarei persoane cu putere de decizie - asociati/actionari, administratori, persoanele din comitetul director si structura de securitate - ori executiva implicata in negocierea contractului clasificat;

d) verificarea datelor minime referitoare la bonitatea si stabilitatea economica a obiectivului industrial - domeniu si obiect de activitate, statut juridic, actionari, garantii bancare.

(2) Pentru verificarile de securitate de nivel II:

a) verificarea corectitudinii datelor consemnate in chestionarul de securitate industriala - anexa nr. 26;

b) evaluarea statutului de securitate a fiecarei persoane cu putere de decizie - asociati/actionari, administratori, persoanele din comitetul director si structura de securitate - ori executiva implicata in derularea contractului clasificat;

c) verificarea unor date minime referitoare la bonitatea si stabilitatea economica a obiectivului industrial - domeniu si obiect de activitate, statut juridic, actionari, garantii bancare;

d) verificarea modului de implementare si de aplicare a normelor si masurilor de securitate fizica, de securitate a personalului si a documentelor, prevazute pentru nivelul secret.

(3) Pentru verificarea de securitate de nivel III:

a) verificarea corectitudinii datelor consemnate in chestionarul de securitate industriala - anexa nr. 27;

b) evaluarea statutului de securitate a fiecarei persoane cu putere de decizie - asociati/actionari, administratori, persoanele din comitetul director si structura de securitate - ori executiva implicata in derularea contractului clasificat, precum si a celor desemnate sa participe la activitatile de negociere a acestuia;

c) verificarea datelor referitoare la bonitatea si stabilitatea economica a agentului economic - domeniu si obiect de activitate, statut juridic, actionari, garantii bancare - incluzand si aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;

d) verificarea existentei autorizarii sistemului informatic si de comunicatii propriu, pentru nivelul strict secret;

e) verificarea modului de implementare si de aplicare a normelor si masurilor de securitate fizica, de securitate a personalului si a documentelor, prevazute pentru nivelul strict secret;

f) discutii cu proprietarii, membrii consiliului director, functionarii de securitate, angajatii, in vederea clarificarii datelor rezultate din chestionar, dupa caz.

(4) Pentru verificarea de securitate de nivel IV:

a) verificarea corectitudinii datelor consemnate in chestionarul de securitate industriala - anexa nr. 27;

b) evaluarea statutului de securitate a fiecarei persoane cu putere de decizie - asociati/actionari, administratori, persoanele din comitetul director si structura de securitate - ori executiva implicata in derularea contractului clasificat;

c) verificarea informatiilor detaliate referitoare la bonitatea si stabilitatea economica a agentului economic - domeniu si obiect de activitate, statut juridic, actionari, garantii bancare - incluzand si aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;

d) verificarea existentei autorizarii sistemului informatic si de comunicatii propriu, pentru nivel strict secret de importanta deosebita;

e) verificarea modului de implementare si de aplicare a normelor si masurilor de securitate fizica, de securitate a personalului si a documentelor, prevazute pentru nivelul strict secret de importanta deosebita;

f) discutii cu proprietarii, membrii consiliului director, functionarii de securitate, angajatii, in vederea clarificarii datelor rezultate din chestionar, dupa caz.

Art. 226. - In cazul unui obiectiv industrial la al carui management/actionariat participa cetateni straini, cetateni romani care au si cetatenia altui stat sau/si persoane apatride, ORNISS, impreuna cu ADS competenta, va evalua masura in care interesul strain ar putea reprezenta o amenintare la adresa protectiei informatiilor secrete de stat, care vor fi incredintate acelui obiectiv industrial.

Art. 227. - In indeplinirea sarcinilor si obiectivelor ce le revin, pe linia protectiei informatiilor clasificate, ADS competente coopereaza pe baza protocoalelor ce vor fi incheiate intre ele cu avizul ORNISS.

Art. 228. - In vederea desfasurarii procedurilor de avizare, obiectivul industrial are obligatia de a permite accesul reprezentantilor ADS in sediile, la echipamentele, operatiunile si la alte activitati, respectiv de a prezenta documentele necesare si de a furniza, la cerere, alte date si informatii.

Art. 229. - **(1)** Daca in urma verificarii de securitate se constata ca sunt indeplinite cerintele de securitate necesare asigurarii protectiei la nivelul de clasificare corespunzator informatiilor vehiculate in cadrul contractului clasificat, ORNISS elibereaza si transmite obiectivului industrial autorizatia sau certificatul de securitate industriala.

(2) Daca se constata ca obiectivul industrial nu indeplineste conditiile de securitate necesare, ORNISS nu elibereaza autorizatia sau certificatul de securitate industriala si informeaza obiectivul industrial in acest sens. ORNISS nu este obligat sa prezinte motivele refuzului. Refuzul eliberarii autorizatiei sau certificatului de securitate industriala va fi comunicat si la ADS care a efectuat verificarile de securitate.

(3) Cand sunt semnalate elemente care nu constituie riscuri, dar sunt relevante din punct de vedere al securitatii, in luarea deciziei de eliberare a autorizatiei sau certificatului de securitate industriala vor avea

prioritate interesele de securitate.

Art. 230. - In termen de 7 zile lucratoare de la primirea avizului de securitate din partea autoritatilor desemnate de securitate, ORNISS va elibera autorizatia sau certificatul de securitate industriala ori, dupa caz, va comunica obiectivului industrial refuzul eliberarii acestora.

Art. 231. - Obiectivul industrial are obligatia de a comunica ORNISS toate modificarile survenite privind datele de securitate incluse in chestionarul completat, pe intreaga durata de valabilitate a autorizatiei sau certificatului de securitate industriala.

Art. 232. - Termenele pentru eliberarea autorizatiei sau certificatului de securitate industriala sunt:

a) pentru autorizatia de securitate industriala - 60 de zile lucratoare;

b) pentru certificat de securitate industriala de nivel secret - 90 de zile lucratoare;

c) pentru certificat de securitate industriala de nivel strict secret - 120 de zile lucratoare;

d) pentru certificat de securitate industriala de nivel strict secret de importanta deosebita - 180 de zile lucratoare.

Art. 233. - **(1)** Autorizatia de securitate are valabilitate pana la incheierea contractului sau pana la retragerea de la negocieri.

(2) Daca in perioada mentionata la alin. (1) contractul clasificat care a facut obiectul negocierilor este adjudecat, contractantul este obligat sa solicite la ORNISS eliberarea certificatului de securitate industriala.

(3) Termenul de valabilitate al certificatului de securitate industriala este determinat de perioada derularii contractului clasificat, dar nu mai mult de 3 ani, dupa care contractantul este obligat sa solicite revalidarea acestuia.

Art. 234. - In situatia in care ORNISS decide retragerea autorizatiei sau certificatului de securitate industriala va instiinta contractantul, contractorul si autoritatea desemnata de securitate competenta.

Art. 235. - Autorizatia sau certificatul de securitate industriala se retrage de ORNISS in urmatoarele cazuri:

a) la solicitarea obiectivului industrial;

b) la propunerea motivata a autoritatii desemnate de securitate competente;

c) la expirarea termenului de valabilitate;

d) la incetarea contractului;

e) la schimbarea nivelului de certificare acordat initial;

CAPITOLUL VIII
PROTECTIA SURSELOR GENERATOARE DE INFORMATII - INFOSEC

SECȚIUNEA 1
Dispozitii generale

Art. 236. - Modalitatile si masurile de protectie a informatiilor clasificate care se prezinta in format electronic sunt similare celor pe suport de hartie.

Art. 237. - Termenii specifici, folositi in prezentul capitol, cu aplicabilitate in domeniul INFOSEC, se definesc dupa cum urmeaza:

- INFOSEC - ansamblul masurilor si structurilor de protectie a informatiilor clasificate care sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatice de comunicatii si al altor sisteme electronice, impotriva amenintarilor si a oricaror actiuni care pot aduce atingere confidentialitatii, integritatii, disponibilitatii autenticitatii si nerepudierii informatiilor clasificate precum si afectarea functionarii sistemelor informatice, indiferent daca acestea apar accidental sau intentionat. Masurile INFOSEC acopera securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografica, precum si depistarea si prevenirea amenintarilor la care sunt expuse informatiile si sistemele;

- informatiile in format electronic - texte, date, imagini, sunete, inregistrate pe dispozitive de stocare sau pe suporturi magnetice, optice, electrice ori transmise sub forma de curenti, tensiuni sau camp electromagnetic, in eter sau in retele de comunicatii;

- sistemul de prelucrare automata a datelor - SPAD - ansamblul de elemente interdependente in care se includ echipamentele de calcul, produsele software de baza si aplicative, metodele, procedeele si, daca este cazul, personalul, organizate astfel incat sa asigure indeplinirea functiilor de stocare, prelucrare automata si transmitere a informatiilor in format electronic, si care se afla sub coordonarea si controlul unei singure autoritati. Un SPAD poate sa cuprinda subsisteme, iar unele dintre acestea pot fi ele insele SPAD;

- componentele specifice de securitate ale unui SPAD, necesare asigurarii unui nivel corespunzator de protectie pentru informatiile clasificate care urmeaza a fi stocate sau procesate intr-un SPAD, sunt:

• functii si caracteristici hardware/firmware/software;
• proceduri de operare si moduri de operare;
• proceduri de evidenta;
• controlul accesului;
• definirea zonei de operare a SPAD;
• definirea zonei de operare a posturilor de lucru/a terminalelor la distanta;
• restrictii impuse de politica de management;
• structuri fizice si dispozitive;

• mijloace de control pentru personal si comunicatii;

- retele de transmisii de date - RTD - ansamblul de elemente interdependente in care se includ echipamente, programe si dispozitive de comunicatie, tehnica de calcul hardware si software, metode si proceduri pentru transmisie si receptie de date si controlul retelei, precum si, daca este cazul, personalul aferent. Toate acestea sunt organizate astfel incat sa asigure indeplinirea functiilor de transmisie a informatiilor in format electronic intre doua sau mai multe SPAD sau sa permita interconectarea cu alte RTD-uri. O RTD poate utiliza serviciile unuia sau mai multor sisteme de comunicatii, mai multe RTD pot utiliza serviciile unuia si aceluiasi sistem de comunicatii.

Caracteristicile de securitate ale unei RTD cuprind caracteristicile de securitate ale sistemelor SPAD individuale conectate, impreuna cu toate componentele si facilitatile asociate retelei - facilitati de comunicatii ale retelei, mecanisme si proceduri de identificare si etichetare, controlul accesului, programe si proceduri de control si revizie - necesare pentru a asigura un nivel corespunzator de protectie pentru informatiile clasificate, care sunt transmise prin intermediul RTD;

- RTD locala - retea de transmisii de date care interconecteaza mai multe computere sau echipamente de retea, situate in acelasi perimetru;

- sistemul informatic si de comunicatii - SIC ansamblu informatic prin intermediul caruia se stocheaza, se proceseaza si se transmit informatii in format electronic, alcatuit din cel putin un SPAD, izolat sau conectat la o RTD. Poate avea o configuratie complexa, formata din mai multe SPAD-uri si/sau RTD-uri interconectate;

- securitatea SPAD, RTD si SIC - aplicarea masurilor de securitate la SPAD si RTD - SIC cu scopul de a preveni sau impiedica extragerea sau modificarea informatiilor clasificate stocate, procesate, transmise prin intermediul acestora - prin interceptare, alterare, distrugere, accesare neautorizata cu mijloace electronice, precum si invalidarea de servicii sau functii, prin mijloace specifice;

- confidentialitatea - asigurarea accesului la informatii clasificate numai pe baza certificatului de securitate al persoanei, in acord cu nivelul de secretizare a informatiei accesate si a permisiunii rezultate din aplicarea principiului nevoii de a cunoaste;

- integritatea - interdictia modificarii - prin stergere sau adaugare - ori a distrugerii in mod neautorizat a informatiilor clasificate;

- disponibilitatea - asigurarea conditiilor necesare regasirii si folosirii cu usurinta, ori de cate ori este nevoie, cu respectarea stricta a conditiilor de confidentialitate si integritate a informatiilor clasificate;

- autenticitatea - asigurarea posibilitatii de verificare a identitatii pe care un utilizator de SPAD sau RTD pretinde ca o are;

- nerepudierea - masura prin care se asigura faptul ca, dupa emiterea/receptionarea unei informatii intr-un sistem de comunicatii securizat, expeditorul/destinatarul nu poate nega, in mod fals, ca a expediat/primit informatii;

- risc de securitate - probabilitatea ca o amenintare sau o vulnerabilitate ale SPAD sau RTD - SIC sa se materializeze in mod efectiv;

- managementul de risc - are ca scop identificarea, controlul si minimizarea riscurilor de securitate si este o activitate continua de stabilire si mentinere a unui nivel de securitate in domeniul tehnologiei informatiei si comunicatiilor - TIC - intr-o unitate, in sensul ca, pornind de la analiza de risc, identifica si evalueaza amenintarile si vulnerabilitatile si propune aplicarea masurilor adecvate de contracarare, proiectate la un pret de cost corelat cu consecintele care ar decurge din divulgarea, modificarea sau stergerea informatiilor care trebuie protejate;

- regula celor doi - obligativitatea colaborarii a doua persoane pentru indeplinirea unei activitati specifice;

- produs informatic de securitate - componenta de securitate care se incorporeaza intr-un SPAD sau RTD - SIC si care serveste la sporirea sau asigurarea confidentialitatii, integritatii, disponibilitatii, autenticitatii si nerepudierii informatiilor stocate, procesate sau transmise;

- securitatea calculatoarelor - COMPUSEC - aplicarea la nivelul fiecarui calculator a facilitatilor de securitate hardware, software si firmware, pentru a preveni divulgarea, manevrarea, modificarea sau stergerea neautorizata a informatiilor clasificate ori invalidarea neautorizata a unor functii;

- securitatea comunicatiilor - COMSEC - aplicarea masurilor de securitate in telecomunicatii, cu scopul de a proteja mesajele dintr-un sistem de telecomunicatii, care ar putea fi interceptate, studiate, analizate si, prin reconstituire, pot conduce la dezvaluiri de informatii clasificate.

COMSEC reprezinta ansamblul de proceduri, incluzand:

a) masuri de securitate a transmisiilor;

b) masuri de securitate impotriva radiatiilor - TEMPEST;

c) masuri de acoperire criptologica;

d) masuri de securitate fizica, procedurala, de personal si a documentelor;

e) masuri COMPUSEC;

- TEMPEST - ansamblul masurilor de testare si de realizare a securitatii impotriva scurgerii de informatii, prin intermediul emisiilor electromagnetice parazite;

- evaluarea - examinarea detaliata, din punct de vedere tehnic si functional, a aspectelor de securitate ale SPAD si RTD - SIC sau a produselor de securitate, de catre o autoritate abilitata in acest sens.

Prin procesul de evaluare se verifica:

a) prezenta facilitatilor/functiilor de securitate cerute;

b) absenta efectelor secundare compromitatoare care ar putea decurge din implementarea facilitatilor de securitate;

c) functionalitatea globala a sistemului de securitate;

d) satisfacerea cerintelor de securitate specifice pentru un SPAD si RTD - SIC;

e) stabilirea nivelului de incredere al SPAD sau RTD - SIC ori al produselor informatice de securitate implementate;

f) existenta performantelor de securitate ale produselor informatice de securitate instalate in SPAD sau RTD - SIC;

- certificarea - emiterea unui document de constatare, la care se ataseaza unul de analiza, in care sunt prezentate modul in care a decurs evaluarea si rezultatele acesteia in documentul de constatare se mentioneaza masurile in care SPAD si RTD - SIC satisfac cerintele de securitate, precum si masura in care produsele informatice de securitate raspund exigentelor referitoare la protectia informatiilor clasificate in format electronic;

- acreditarea - etapa de acordare a autorizarii si aprobarii unui SPAD sau RTD - SIC de a prelucra informatii clasificate, in spatiul/mediul operational propriu.

Etapa de acreditare trebuie sa se desfasoare dupa ce s-au implementat toate procedurile de securitate si dupa ce s-a atins un nivel suficient de protectie a resurselor de sistem. Acreditarea se face, in principal, pe baza CSS si include urmatoarele:

a) nota justificativa despre obiectivul acreditarii sistemului, nivelul/nivelurile de clasificare a informatiilor care urmeaza sa fie procesate si vehiculate, modul/modurile de operare protejata propuse;

b) nota justificativa despre managementul riscurilor - modul de tratare, gestionare si rezolvare a riscurilor - in care se specifica pericolele si punctele vulnerabile, precum si masurile adecvate de contracarare a acestora;

c) o descriere detaliata a facilitatilor de securitate si a procedurilor propuse, destinate SPAD sau RTD - SIC. Aceasta descriere va reprezenta elementul esential pentru finalizarea procesului de acreditare;

d) planul de implementare si intretinere a caracteristicilor de securitate;

e) planul de desfasurare a etapelor de testare, evaluare si certificare a securitatii SPAD sau RTD - SIC;

f) certificatul si, acolo unde este necesar, elemente de acreditare suplimentare;

- zona SPAD - reprezinta o zona de lucru in care se gasesc si opereaza unul sau mai multe calculatoare, unitati periferice locale si de stocare, mijloace de control si echipament specific de retea si de comunicatii. Zona SPAD nu include zona in care sunt amplasate terminale, echipamente periferice sau statii de lucru la distanta, chiar daca aceste echipamente sunt conectate la echipamentul central de calcul din zona SPAD;

- zona terminal/statie de lucru la distanta - reprezinta o zona, separata de zona SPAD, in care se gasesc:

a) elemente de tehnica de calcul;

b) echipamentele periferice locale, terminale sau statii de lucru la distanta, conectate la echipamentele din zona SPAD;

c) echipamente de comunicatii;

- amenintarea - posibilitatea de compromitere accidentala sau deliberata a securitatii SPAD sau RTD - SIC, prin pierderea confidentialitatii, a integritatii sau disponibilitatii informatiilor in format electronic sau prin afectarea functiilor care asigura autenticitatea si nerepudierea informatiilor;

- vulnerabilitatea - slabiciune sau lipsa de control care ar putea permite sau facilita o manevra tehnica, procedurala sau operationala, prin care se ameninta o valoare sau tinta specifica.

Art. 238. - Abrevierile utilizate in prezentul capitol semnifica:

a) CSTIC - componenta de securitate pentru tehnologia informatiei si comunicatiilor instituita in unitatile detinatoare de informatii clasificate;

b) TIC - tehnologia informatiei si comunicatiilor;

c) CSS - cerintele de securitate specifice.

Art. 239. - **(1)** Informatiile care se prezinta in format electronic pot fi:

a) stocate si procesate in cadrul SPAD sau transmise prin intermediul RTD;

b) stocate si transportate prin intermediul suporturilor de memorie, dispozitivelor electronice - cipuri de memorie, hartie perforata sau alte suporturi specifice.

(2) Incarcarea informatiilor pe mediile prevazute in alin. (1) lit. b, precum si interpretarea lor pentru a deveni inteligibile, se face cu ajutorul echipamentelor electronice specializate.

Art. 240. - **(1)** Sistemele SPAD si RTD - SIC au dreptul sa stocheze, sa proceseze sau sa transmita informatii clasificate, numai daca sunt autorizate potrivit prezentei hotarari.

(2) In vederea autorizarii SPAD si RTD - SIC unitatile vor intocmi, cu aprobarea organelor lor de conducere, strategia proprie de securitate, in baza careia vor implementa sisteme proprii de securitate, care vor include utilizarea de produse specifice tehnologiei informatiei si comunicatiilor, personal instruit si masuri de protectie a informatiei, incluzand controlul accesului la sistemele si serviciile informatice si de comunicatii, pe baza principiului necesitatii de a cunoaste si al nivelului de secretizare atribuit.

(3) SPAD si RTD - SIC vor fi supuse procesului de acreditare, urmat de evaluari periodice, in vederea mentinerii acreditarii.

Art. 241. - **(1)** Aplicarea reglementarilor in vigoare referitoare la protectia informatiilor clasificate in format electronic functioneaza unitar la nivel national. Sistemul de emitere si implementare a masurilor de securitate adresate protectiei informatiilor clasificate care sunt stocate, procesate sau transmise de SPAD

sau RTD - SIC, precum si controlul modului de implementare a masurilor de securitate se realizeaza de catre o structura functionala cu atributii de reglementare, control si autorizare, care include:

a) o agentie pentru acordarea acreditarii de functionare in regim de securitate;

b) o agentie care elaboreaza si implementeaza metode, mijloace si masuri de securitate;

c) o agentie responsabila cu protectia criptografica.

(2) Agentiile mentionate la alin. (1) sunt subordonate institutiei desemnate la nivel national, pentru protectia informatiilor clasificate, ORNISS.

(3) Masurile de protectie a informatiilor clasificate in format electronic trebuie reactualizate permanent, prin depistare, documentare si gestionare a amenintarilor si vulnerabilitatilor la adresa informatiilor clasificate si sistemelor care le prelucreaza, stocheaza si transmit.

Art. 242. - Masurile de securitate INFOSEC vor fi structurate dupa nivelul de clasificare al informatiilor pe care le protejeaza si in conformitate cu continutul acestora.

Art. 243. - Conducatorul unitatii detinatoare de informatii clasificate raspunde de securitatea propriilor informatii care sunt stocate, procesate sau transmise in SPAD sau RTD - SIC.

Art. 244. - **(1)** in fiecare unitate care administreaza SPAD si RTD - SIC in care se stocheaza, se proceseaza sau se transmit informatii clasificate, se va institui o componenta de securitate pentru tehnologia informatiei si a comunicatiilor - CSTIC, in subordinea structurii/functionarului de securitate.

(2) In functie de volumul de activitate si daca cerintele de securitate permit, atributiile CSTIC pot fi indeplinite numai de catre functionarul de securitate TIC sau pot fi preluate, in totalitate, de catre structura/functionarul de securitate din unitate.

(3) CSTIC indeplineste atributii privind:

a) implementarea metodelor, mijloacelor si masurilor necesare protectiei informatiilor in format electronic;

b) exploatarea operationala a SPAD si RTD - SIC in conditii de securitate;

c) coordonarea cooperarii dintre unitatea detinatoare a SPAD sau RTD - SIC si autoritatea care asigura acreditarea;

d) implementarea masurilor de securitate si protectia criptografica ale SPAD sau RTD - SIC.

(4) CSTIC reprezinta punctul de contact al agentiilor competente cu unitatile care detin in administrare SPAD sau RTD - SIC si, dupa caz, poate fi investita, temporar, de catre aceste agentii, cu unele dintre atributiile lor.

(5) Propunerile pe linie de securitate avansate de catre CSTIC devin operationale numai dupa ce au fost aprobate de catre conducerea unitatii care detine in administrare respectivul SPAD sau RTD - SIC.

Art. 245. - CSTIC se instituie la nivelul fiecarei SPAD si RTD - SIC si reprezinta persoana sau compartimentul cu responsabilitatea delegata de catre agentia de securitate pentru informatica si comunicatii de a implementa metodele, mijloacele si masurile de securitate si de a exploata SPAD si RTD - SIC in conditii de securitate.

Art. 246. - CSTIC este condusa de catre functionarul de securitate TIC si are in compunere administratorii de securitate si, dupa caz, si alti specialisti din SPAD sau RTD - SIC. Toata structura CSTIC face parte din personalul unitatii care administreaza SPAD sau RTD - SIC.

Art. 247. - Exercitarea atributiilor CSTIC trebuie sa cuprinda intregul ciclu de viata al SPAD sau RTD - SIC, incepand cu proiectarea, continuand cu elaborarea specificatiilor, testarea instalarii, acreditarea, testarea periodica in vederea reacreditarii, exploatarea operationala, modificarea si incheind cu scoaterea din uz. In anumite situatii, rolul CSTIC poate fi preluat de catre alte componente ale unitatii, in decursul ciclului de viata.

Art. 248. - CSTIC mijloceste cooperarea dintre conducerea unitatii careia ii apartine SPAD sau RTD - SIC si agentia pentru acreditare de securitate, atunci cand unitatea:

a) planifica dezvoltarea sau achizitia de SPAD sau RTD;

b) propune schimbari ale unei configuratii de sistem existente;

c) propune conectarea unui SPAD sau a unei RTD - SIC cu un alt SPAD sau RTD - SIC;

d) propune schimbari ale modului de operare de securitate ale SPAD sau RTD - SIC;

e) propune schimbari in programele existente sau utilizarea de noi programe, pentru optimizarea securitatii SPAD sau RTD - SIC;

f) initiaza proceduri de modificare a nivelului de clasificare a SPAD si RTD - SIC care au fost deja acreditate;

g) planifica sau propune intreprinderea oricarei alte activitati referitoare la imbunatatirea securitatii SPAD sau RTD - SIC deja acreditate.

Art. 249. - CSTIC, cu aprobarea autoritatii de acreditare de securitate, stabileste standardele si procedurile de securitate care trebuie respectate de catre furnizorii de echipamente, pe parcursul dezvoltarii, instalarii si testarii SPAD si RTD - SIC si raspunde pentru justificarea, selectia, implementarea si controlul componentelor de securitate, care constituie parte a SPAD si RTD - SIC.

Art. 250. - CSTIC stabileste, pentru structurile de securitate si management ale SPAD si RTD - SIC, inca de la infiintare, responsabilitatile pe care le vor exercita pe tot ciclul de viata al SPAD si RTD - SIC respective.

Art. 251. - Activitatea INFOSEC din SPAD si RTD - SIC, desfasurata de catre CSTIC, trebuie condusa si coordonata de persoane care detin certificat de securitate corespunzator, cu pregatire de specialitate in domeniul sistemelor TIC precum si al securitatii acestora, obtinuta in institutii de invatamant acreditate

INFOSEC, sau care au lucrat in domeniu cel putin 5 ani.

Art. 252. - Protectia SPAD si RTD - SIC din compunerea sistemelor de armament si de detectie va fi definita in contextul general al sistemelor din care acestea fac parte si va fi realizata prin aplicarea prevederilor prezentelor standarde.

SECȚIUNEA a 2-a

Structuri organizatorice cu atributii specifice in domeniul INFOSEC

A. Agentia de acreditare de securitate

Art. 253. - Agentia de acreditare de securitate este subordonata institutiei desemnate la nivel national pentru protectia informatiilor clasificate, are reprezentanti delegati din cadrul ADS implicate, in functie de SPAD si RTD -SIC care trebuie acreditate, si indeplineste urmatoarele atributii principale:

a) asigura, la nivel national, acreditarea de securitate si reacreditarea SPAD si RTD - SIC care stocheaza, proceseaza sau transmit informatii clasificate, in functie de nivelul de clasificare a acestora;

b) asigura evaluarea si certificarea sistemelor SPAD si RTD - SIC sau a unor elemente componente ale acestora;

c) stabileste criteriile de acreditare de securitate pentru SPAD si RTD - SIC.

Art. 254. - Agentia de acreditare de securitate isi exercita atributiile in domeniul INFOSEC in numele institutiei desemnate la nivel national pentru protectia informatiilor clasificate si are responsabilitatea de a impune standarde de securitate in acest domeniu.

B. Agentia de securitate pentru informatica si comunicatii

Art. 255. - Agentia de securitate pentru informatica si comunicatii este structura subordonata institutiei desemnate la nivel national pentru protectia informatiilor electronice clasificate, avand reprezentanti delegati din cadrul ADS implicate care actioneaza la nivel national.

Art. 256. - Agentia este responsabila de conceperea si implementarea mijloacelor, metodelor si masurilor de protectie a informatiilor clasificate care sunt stocate, procesate sau transmise prin intermediul SPAD si RTD - SIC si are, in principal, urmatoarele atributii:

a) coordoneaza activitatile de protectie a informatiilor clasificate care sunt stocate, procesate sau transmise prin intermediul SPAD si RTD - SIC;

b) elaboreaza si promoveaza reglementari si standarde specifice;

c) analizeaza cauzele incidentelor de securitate si gestioneaza baza de date privind amenintarile si vulnerabilitatile din sistemele de comunicatie si informatice, necesare pentru elaborarea managementul de risc;

d) semnaleaza agentiei de acreditare de securitate incidentele de securitate in domeniu;

e) integreaza masurile privind protectia fizica, de personal, a documentelor administrative, COMPUSEC, COMSEC, TEMPEST si criptografica;

f) executa inspectii periodice asupra SPAD si RTD - SIC in vederea reacreditarii;

g) supune certificarii si autorizarii sistemele de securitate specifice SPAD si RTD - SIC.

Art. 257. - Pentru indeplinirea atributiilor sale, agentia de securitate pentru informatica si comunicatii coopereaza cu agentia de acreditare de securitate, cu agentia de protectie criptografica si cu alte structuri cu atributii in domeniu.

C. Agentia de protectie criptografica

Art. 258. - Agentia de protectie criptografica se organizeaza la nivel national, este subordonata institutiei desemnate la nivel national pentru protectia informatiilor clasificate si are urmatoarele atributii principale:

a) asigura managementul materialelor si echipamentelor criptografice;

b) realizeaza distribuirea materialelor si echipamentelor criptografice;

c) raporteaza institutiei desemnate la nivel national pentru protectia informatiilor clasificate incidentele de securitate cu care s-a confruntat;

d) coopereaza cu agentia de acreditare de securitate, cu agentia de concepere si implementare a metodelor, mijloacelor si masurilor de securitate si cu alte structuri cu atributii in domeniu.

SECȚIUNEA a 3-a

Masuri, cerinte si moduri de operare

A. Masuri si cerinte specifice INFOSEC

Art. 259. - **(1)** Masurile de protectie a informatiilor clasificate in format electronic se aplica sistemelor SPAD si RTD - SIC care stocheaza, proceseaza sau transmit asemenea informatii.

(2) Unitatile detinatoare de informatii clasificate au obligatia de a stabili si implementa un ansamblu de masuri de securitate a sistemelor SPAD si RTD - SIC - fizice, de personal, administrative, de tip TEMPEST si criptografic.

Art. 260. - Masurile de securitate destinate protectiei SPAD si RTD - SIC trebuie sa asigure controlul accesului pentru prevenirea sau detectarea divulgarii neautorizate a informatiilor. Procesul de certificare si acreditare va stabili daca aceste masuri sunt corespunzatoare.

B. Cerinte de securitate specifice SPAD si RTD - SIC

Art. 261. - **(1)** Cerintele de securitate specifice - CSS se constituie intr-un document incheiat intre agentia de acreditare de securitate si CSTIC, ce va cuprinde principii si masuri de securitate care trebuie sa stea la baza procesului de certificare si acreditare a SPAD sau RTD - SIC.

(2) CSS se elaboreaza pentru fiecare SPAD si RTD - SIC care stocheaza, proceseaza sau transmite informatii clasificate, sunt stabilite de catre CSTIC si aprobate de catre agentia de acreditare de securitate.

Art. 262. - CSS vor fi formulate inca din faza de proiectare a SPAD sau RTD - SIC si vor fi dezvoltate pe tot ciclul de viata al sistemului.

Art. 263. - CSS au la baza standardele nationale de protectie, parametrii esentiali ai mediului operational, nivelul minim de autorizare a personalului, nivelul de clasificare a informatiilor gestionate si modul de operare a sistemului care urmeaza sa fie acreditat.

C. Moduri de operare

Art. 264. - SPAD si RTD - SIC care stocheaza, proceseaza sau transmit informatii clasificate vor fi certificate si acreditate sa opereze, pe anumite perioade de timp, in unul din urmatoarele moduri de operare:

a) dedicat;

b) de nivel inalt;

c) multi-nivel.

Art. 265. - **(1)** In modul de operare dedicat, toate persoanele cu drept de acces la SPAD sau la RTD trebuie sa aiba certificat de securitate pentru cel mai inalt nivel de clasificare a informatiilor stocate, procesate sau transmise prin aceste sisteme. Necesitatea de a cunoaste pentru aceste persoane se stabileste cu privire la toate informatiile stocate, procesate sau transmise in cadrul SPAD sau RTD - SIC.

(2) In acest mod de operare, principiul necesitatii de a cunoaste nu impune o separare a informatiilor in cadrul SPAD sau RTD, ca mijloc de securitate a SIC. Celelalte masuri de protectie prevazute vor asigura indeplinirea cerintelor impuse de cel mai inalt nivel de clasificare a informatiilor gestionate si de toate categoriile de informatii cu destinatie speciala stocate, procesate sau transmise in cadrul SPAD sau RTD.

Art. 266. - **(1)** In modul de operare de nivel inalt, toate persoanele cu drept de acces la SPAD sau la RTD - SIC trebuie sa aiba certificat de securitate pentru cel mai inalt nivel de clasificare a informatiilor stocate, procesate sau transmise in cadrul SPAD sau RTD - SIC, iar accesul la informatii se va face diferentiat, conform principiului necesitatii de a cunoaste.

(2) Pentru a asigura accesul diferentiat la informatii, conform principiului necesitatii de a cunoaste, se instituie facilitati de securitate care sa asigure un acces selectiv la informatii in cadrul SPAD sau RTD - SIC.

(3) Celelalte masuri de protectie vor satisface cerintele pentru cel mai inalt nivel de clasificare si pentru toate categoriile de informatii cu destinatie speciala stocate, procesate, transmise in cadrul SPAD sau RTD - SIC.

(4) Toate informatiile stocate, procesate sau vehiculate in cadrul unui SPAD sau RTD - SIC in acest mod de operare vor fi protejate ca informatii cu destinatie speciala, avand cel mai inalt nivel de clasificare care a fost constatat in multimea informatiilor stocate, procesate sau vehiculate prin sistem.

Art. 267. - **(1)** In modul de operare multi-nivel, accesul la informatiile clasificate se face diferentiat, potrivit principiului necesitatii de a cunoaste, conform urmatoarelor reguli:

a) nu toate persoanele cu drept de acces la SPAD sau RTD - SIC au certificat de securitate pentru acces la informatii de cel mai inalt nivel de clasificare care sunt stocate, procesate sau transmise prin aceste sisteme;

b) nu toate persoanele cu acces la SPAD sau RTD - SIC au acces la toate informatiile stocate, procesate sau transmise prin aceste sisteme.

(2) Aplicarea regulilor prevazute la alin. (1) impune instituirea, in compensatie, a unor facilitati de securitate care sa asigure un mod selectiv, individual, de acces la informatiile clasificate din cadrul SPAD sau RTD - SIC.

D. Administratorii de securitate

Art. 268. - **(1)** Securitatea SPAD a retelei si a obiectivului SIC se asigura prin functiile de administrator de securitate.

(2) Administratorii de securitate sunt:

a) administratorul de securitate al SPAD;

b) administratorul de securitate al retelei;

c) administratorul de securitate al obiectivului SIC.

(3) Functiile de administratori de securitate trebuie sa asigure indeplinirea atributiilor CSTIC. Daca este cazul, aceste functii pot fi cumulate de catre un singur specialist.

Art. 269. - **(1)** CSTIC desemneaza un administrator de securitate al SPAD responsabil cu supervizarea dezvoltarii, implementarii si administrarii masurilor de securitate dintr-un SPAD, inclusiv participarea la elaborarea procedurilor operationale de securitate.

(2) La recomandarea autoritatii de acreditare de securitate, CSTIC poate desemna structuri de administrare ale SPAD care indeplinesc aceleasi atributii.

Art. 270. - Administratorul de securitate al retelei este desemnat de CSTIC pentru un SIC de mari dimensiuni sau in cazul interconectarii mai multor SPAD si indeplineste atributii privind managementul securitatii comunicatiilor.

Art. 271. - **(1)** Administratorul de securitate al obiectivului SIC este desemnat de CSTIC sau de autoritatea de securitate competenta si raspunde de asigurarea implementarii si mentinerea masurilor de securitate aplicabile obiectivului SIC respectiv.

(2) Responsabilitatile unui administrator de securitate al obiectivului SIC pot fi indeplinite de catre structura/functionarul de securitate al unitatii, ca parte a indatoririlor sale profesionale.

(3) Obiectivul SIC reprezinta un amplasament specific sau un grup de amplasamente in care functioneaza un SPAD si/sau RTD. Responsabilitatile si masurile de securitate pentru fiecare zona de amplasare a unui terminal/statie de lucru care functioneaza la distanta trebuie explicit determinate.

E. Utilizatorii si vizitatorii

Art. 272. - **(1)** Toti utilizatorii de SPAD sau RTD - SIC poarta responsabilitatea in ce priveste securitatea acestor sisteme - raportate, in principal, la drepturile acordate si sunt indrumati de catre administratorii de securitate

(2) Utilizatorii vor fi autorizati pentru clasa si nivelul de secretizare a informatiilor clasificate stocate, procesate sau transmise in SPAD sau RTD - SIC. La acordarea accesului la informatii, individual, se va urmari respectarea principiului necesitatii de a cunoaste.

(3) Informarea si constientizarea utilizatorilor asupra indatoririlor lor de securitate trebuie sa asigure o eficacitate sporita a sistemului de securitate.

Art. 273. - Vizitatorii trebuie sa aiba autorizare de securitate de nivel corespunzator si sa indeplineasca principiul necesitatii de a cunoaste, in situatia in care accesul unui vizitator fara autorizare de securitate este considerat necesar, vor fi luate masuri de securitate suplimentare pentru ca acesta sa nu poata avea acces la informatiile clasificate.

SECȚIUNEA a 4-a
Componentele EVFOSEC

A. Securitatea personalului

Art. 274. - **(1)** Utilizatorii SPAD si RTD - SIC sunt autorizati si li se permite accesul la informatii clasificate pe baza principiului necesitatii de a cunoaste si in functie de nivelul de clasificare a informatiilor stocate, procesate sau transmise prin aceste sisteme.

(2) Unitatile detinatoare de informatii clasificate in format electronic au obligatia de a institui masuri speciale pentru instruirea si supravegherea personalului, inclusiv a personalului de proiectare de sistem care are acces la SPAD si RTD, in vederea prevenirii si inlaturarii vulnerabilitatilor fata de accesarea neautorizata.

Art. 275. - In proiectarea SPAD si RTD - SIC trebuie sa se aiba in vedere ca atribuirea sarcinilor si raspunderilor personalului sa se faca in asa fel incat sa nu existe o persoana care sa aiba cunostinta sau acces la toate programele si cheile de securitate - parole, mijloace de identificare personala.

Art. 276. - Procedurile de lucru ale personalului din SPAD si RTD - SIC trebuie sa asigure separarea intre operatiunile de programare si cele de exploatare a sistemului sau retelei. Este interzis, cu exceptia unor situatii speciale, ca personalul sa faca atat programarea, cat si operarea sistemelor sau retelelor si trebuie instituite proceduri speciale pentru depistarea acestor situatii.

Art. 277. - Pentru orice fel de modificare aplicata unui sistem SPAD sau RTD - SIC este obligatorie colaborarea a cel putin doua persoane - regula celor doi. Procedurile de securitate vor mentiona explicit situatiile in care regula celor doi trebuie aplicata.

Art. 278. - Pentru a asigura implementarea corecta a masurilor de securitate, personalul SPAD si RTD - SIC si personalul care raspunde de securitatea acestora trebuie sa fie instruit si informat astfel incat sa isi cunoasca reciproc atributiile

B. Securitatea fizica

Art. 279. - Zonele in care sunt amplasate SPAD si/sau RTD - SIC si cele cu terminale la distanta, in care sunt prezentate, stocate, procesate sau transmise informatii clasificate ori in care este posibil accesul potential la astfel de informatii, se declara zone de securitate clasa I sau clasa II ale obiectivului si se supun masurilor de protectie fizica stabilite prin prezentele standarde.

Art. 280. - In zonele in care sunt amplasate sisteme SPAD si terminale la distanta - statii de lucru, unde se proceseaza si/sau pot fi accesate informatii clasificate, se aplica urmatoarele masuri generale de securitate:

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

b) zonele si locurile in care securitatea SPAD sau RTD - SIC sau a terminalelor la distanta poate fi modificata nu trebuie sa fie niciodata ocupate de un singur angajat autorizat;

c) persoanelor care solicita acces temporar sau cu intermitente in aceste zone trebuie sa li se autorizeze accesul, ca vizitatori, de catre responsabilul pe probleme de securitate al zonei, desemnat de catre

administratorul de securitate al obiectivului SIC. Vizitatorii vor fi insotiti permanent, pentru a avea garantia ca nu pot avea acces la informatii clasificate si nici la echipamentele utilizate.

Art. 281. - In functie de riscul de securitate si de nivelul de secretizare al informatiilor stocate, procesate si transmise, se impune cerinta de aplicare a regulii de lucru cu doua persoane si in alte zone, ce vor fi stabilite in stadiul initial al proiectului si prezentate in cadrul CSS.

Art. 282. - Cand un SPAD este exploatat in mod autonom, deconectat in mod permanent de alte SPAD, tinand cont de conditiile specifice, de alte masuri de securitate, tehnice sau procedurale si de rolul pe care il are respectivul SPAD in functionarea de ansamblu a sistemului, agentia de acreditare de securitate trebuie sa stabileasca masuri specifice de protectie, adaptate la structura acestui SPAD, conform nivelului de clasificare a informatiilor gestionate.

C. Controlul accesului la SPAD si/sau la RTD - SIC

Art. 283. - Toate informatiile si materialele care privesc accesul la un SPAD sau RTD - SIC sunt controlate si protejate prin reglementari corespunzatoare nivelului de clasificare cel mai inalt si specificului informatiilor la care respectivul SPAD sau RTD - SIC permite accesul.

Art. 284. - Cand nu mai sunt utilizate, informatiile si materialele de control specificate la articolul precedent trebuie sa fie distruse conform prevederilor prezentelor standarde.

D. Securitatea informatiilor clasificate in format electronic

Art. 285. - Informatiile clasificate in format electronic trebuie sa fie controlate conform regulilor INFOSEC, inainte de a fi transmise din zonele SPAD si RTD - SIC sau din cele cu terminale la distanta.

Art. 286. - Modul in care este prezentata informatia in clar, chiar daca se utilizeaza codul prescurtat de transmisie sau reprezentarea binara ori alte forme de transmitere la distanta, nu trebuie sa influenteze nivelul de clasificare acordat informatiilor respective.

Art. 287. - Cand informatiile sunt transferate intre diverse SPAD sau RTD - SIC, ele trebuie sa fie protejate atat in timpul transferului, cat si la nivelul sistemelor informatice ale beneficiarului, corespunzator cu nivelul de clasificare al informatiilor transmise.

Art. 288. - Toate mediile de stocare a informatiilor se pastreaza intr-o modalitate care sa corespunda celui mai inalt nivel de clasificare a informatiilor stocate sau suportilor, fiind protejate permanent.

Art. 289. - Copierea informatiilor clasificate situate pe medii de stocare specifice TIC se executa in conformitate cu prevederile din procedurile operationale de securitate.

Art. 290. - Mediile refolosibile de stocare a informatiilor utilizate pentru inregistrarea informatiilor clasificate isi mentin cea mai inalta clasificare pentru care au fost utilizate anterior, pana cand respectivelor informatii li se reduce nivelul de clasificare sau sunt declasificate, moment in care mediile susmentionate se reclasifica in mod corespunzator sau sunt distruse in conformitate cu prevederile procedurilor operationale de securitate.

E. Controlul si evidenta informatiilor in format electronic

Art. 291. - **(1)** Evidenta automata a accesului la informatiile clasificate in format electronic se tine in registrele de acces si trebuie realizata neconditionat prin software.

(2) Registrele de acces se pastreaza pe o perioada stabilita de comun acord intre agentia de acreditare de securitate si CSTIC.

(3) Perioada minima de pastrare a registrelor de acces la informatiile strict secrete de importanta deosebita este de 10 ani, iar a registrelor de acces la informatiile strict secrete si secrete, de cel putin 3 ani.

Art. 292. - **(1)** Mediile de stocare care contin informatii clasificate utilizate in interiorul unei zone SPAD pot fi manipulate ca unic material clasificat, cu conditia ca materialul sa fie identificat, marcat cu nivelul sau de clasificare si controlat in interiorul zonei SPAD, pana in momentul in care este distrus, redus la o copie de arhiva sau pus intr-un dosar permanent.

(2) Evidentele acestora vor fi mentinute in cadrul zonei SPAD pana cand sunt supuse controlului sau distruse, conform prezentelor standarde.

Art. 293. - In cazul in care un mediu de stocare este generat intr-un SPAD sau RTD - SIC, iar apoi este transmis intr-o zona cu terminal/statie de lucru la distanta, se stabilesc proceduri adecvate de securitate, aprobate de catre agentia de acreditare de securitate. Procedurile trebuie sa cuprinda si instructiuni specifice privind evidenta informatiilor in format electronic.

F. Manipularea si controlul mediilor de stocare a informatiilor clasificate in format electronic

Art. 294. - **(1)** Toate mediile de stocare secrete de stat se identifica si se controleaza in mod corespunzator nivelului de secretizare.

(2) Pentru informatiile neclasificate sau secrete de serviciu se aplica regulamente de securitate interne.

(3) Identificarea si controalele trebuie sa asigure urmatoarele cerinte:

a) Pentru nivelul secret:

- un mijloc de identificare - numar de serie si marcajul nivelului de clasificare - pentru fiecare astfel de mediu, in mod separat;

- proceduri bine definite pentru emiterea, primirea, retragerea, distrugerea sau pastrarea mediilor de stocare;

- evidentele manuale sau tiparite la imprimanta, indicand continutul si nivelul de secretizare a informatiilor inregistrate pe mediile de stocare.

b) Pentru nivelul strict secret si strict secret de importanta deosebita, informatiile detaliate asupra mediului de stocare, incluzand continutul si nivelul de clasificare, se tin intr-un registru adecvat.

Art. 295. - Controlul punctual si de ansamblu al mediilor de stocare, pentru a asigura compatibilitatea cu procedurile de identificare si control in vigoare, trebuie sa asigure indeplinirea urmatoarelor cerinte:

a) pentru nivelul secret - controalele punctuale ale prezentei fizice si continutului mediilor de stocare se efectueaza periodic, verificandu-se daca acele medii de stocare nu contin informatii cu un nivel de clasificare superior;

b) pentru nivelul strict secret - toate mediile de stocare se inventariaza periodic, controland punctual prezenta lor fizica si continutul, pentru a verifica daca pe acele medii nu sunt stocate informatii cu un nivel de clasificare superior;

c) pentru nivelul strict secret de importanta deosebita, toate mediile se verifica periodic, cel putin anual si se controleaza punctual, in legatura cu prezenta fizica si continutul lor.

G. Declasificarea si distrugerea mediilor de stocare a informatiilor in format electronic

Art. 296. - Informatiile clasificate inregistrate pe medii de stocare refolosibile se sterg doar in conformitate cu procedurile operationale de securitate.

Art. 297. - **(1)** Cand un mediu de stocare urmeaza sa iasa din uz, trebuie sa fie declasificat suprimandu-se orice marcaje de clasificare, ulterior putand fi utilizat ca mediu de stocare nesecret. Daca acesta nu poate fi declasificat, trebuie distrus printr-o procedura aprobata.

(2) Sunt interzise declasificarea si refolosirea mediilor de stocare care contin informatii strict secrete de importanta deosebita, acestea putand fi numai distruse, in conformitate cu procedurile operationale de securitate.

Art. 298. - Informatiile clasificate in format electronic stocate pe un mediu de unica folosinta - cartele, benzi perforate - trebuie distruse conform prevederilor procedurilor operationale de securitate.

SECȚIUNEA a 5-a
Reguli generale de securitate TIC

A. Securitatea comunicatiilor

Art. 299. - Toate mijloacele folosite pentru transmiterea electromagnetica a informatiilor clasificate se supun instructiunilor de securitate a comunicatiilor emise de catre institutia desemnata la nivel national pentru protectia informatiilor clasificate.

Art. 300. - Intr-un SPAD - SIC trebuie sa se dispuna mijloace de interzicere a accesului la informatiile clasificate de la toate terminalele/statiile de lucru la distanta, atunci cand se solicita acest lucru, prin deconectare fizica sau prin proceduri software speciale, aprobate de catre autoritatea de acreditare de securitate.

B. Securitatea la instalare si fata de emisiile electromagnetice

Art. 301. - Instalarea initiala a SPAD sau RTD - SIC sau orice modificare majora adusa acestora vor fi executate de persoane autorizate, in conditiile prezentelor standarde. Lucrarile vor fi permanent supravegheate de personal tehnic calificat, care are acces la informatii de cel mai inalt nivel de clasificare pe care respectivul SPAD sau RTD - SIC le va stoca, procesa sau transmite.

Art. 302. - Toate echipamentele SPAD si RTD - SIC vor fi instalate in conformitate cu reglementarile specifice in vigoare, emise de catre institutia desemnata la nivel national pentru protectia informatiilor clasificate, cu directivele si standardele tehnice corespunzatoare.

Art. 303. - Sistemele SPAD si RTD - SIC care stocheaza, proceseaza sau transmit informatii secrete de stat vor fi protejate corespunzator fata de vulnerabilitatile de securitate cauzate de radiatiile compromitatoare - TEMPEST.

C. Securitatea in timpul procesarii informatiilor clasificate

Art. 304. - Procesarea informatiilor se realizeaza in conformitate cu procedurile operationale de securitate, prevazute in prezentele standarde.

Art. 305. - Transmiterea informatiilor secrete de stat catre instalatii automate - a caror functionare nu necesita prezenta unui operator uman - este interzisa, cu exceptia cazului cand se aplica reglementari speciale aprobate de catre autoritatea de acreditare de securitate, iar acestea au fost specificate in procedurile operationale de securitate.

Art. 306. - In SPAD sau RTD - SIC care au utilizatori - existenti sau potentiali - fara certificate de securitate emise conform prezentelor standarde nu se pot stoca, procesa sau transmite informatii strict secrete de importanta deosebita.

D. Procedurile operationale de securitate

Art. 307. - Procedurile operationale de securitate reprezinta descrierea implementarii strategiei de securitate ce urmeaza sa fie adoptata, a procedurilor operationale de urmat si a responsabilitatilor

personalului.

Art. 308 - Procedurile operationale de securitate sunt elaborate de catre agentia de concepere si implementare a metodelor, mijloacelor si masurilor de securitate, in colaborare cu CSTIC, precum si cu agentia de acreditare de securitate, care are atributii de coordonare, si alte autoritati cu atributii in domeniu. Agentia de acreditare de securitate va aproba procedurile de operare inainte de a autoriza stocarea, procesarea sau transmiterea informatiilor secrete de stat prin SPAD - RTD - SIC.

E. Protectia produselor software si managementul configuratiei

Art. 309. - CSTIC are obligatia sa efectueze controale periodice, prin care sa stabileasca daca toate produsele software originale - sisteme de operare generale, subsisteme si pachete soft - aflate in folosinta, sunt protejate in conditii conforme cu nivelul de clasificare al informatiilor pe care acestea trebuie sa le proceseze. Protectia programelor - software de aplicatie se stabileste pe baza evaluarii nivelului de secretizare a acestora, tinand cont de nivelul de clasificare a informatiilor pe care urmeaza sa le proceseze.

Art. 310. - **(1)** Este interzisa utilizarea de software neautorizat de catre agentia de acreditare de securitate.

(2) Conservarea exemplarelor originale, a copiilor - backup sau off-site, precum si salvarile periodice ale datelor obtinute din procesare vor fi executate in conformitate cu prevederile procedurilor operationale de securitate.

Art. 311. - **(1)** Versiunile software care sunt in uz trebuie sa fie verificate la intervale regulate, pentru a garanta integritatea si functionarea lor corecta.

(2) Versiunile noi sau modificate ale software-ului nu vor fi folosite pentru procesarea informatiilor secrete de stat, pana cand procedurile de securitate ale acestora nu sunt testate si aprobate conform CSS.

(3) Un software care imbunatateste posibilitatile sistemului si care nu are nici o procedura de securitate nu poate fi folosit inainte de a fi verificat de catre CSTIC.

F. Verificari pentru depistarea virusilor de calculator si a software-ului nociv

Art. 312. - Verificarea prezentei virusilor si software-ului nociv se face in conformitate cu cerintele impuse de catre agentia de acreditare de securitate.

Art. 313. - **(1)** Versiunile de software noi sau modificate - sisteme de operare, subsisteme, pachete de software si software de aplicatie - stocate pe diferite medii care se introduc intr-o unitate, trebuie verificate obligatoriu pe sisteme de calcul izolate, in vederea depistarii software-ului nociv sau a virusilor de calculator, inainte de a fi folosite in SPAD sau RTD - SIC. Periodic se va proceda la verificarea software-ului instalat.

(2) Verificarile trebuie facute mai frecvent daca SPAD sau RTD - SIC sunt conectate la alt SPAD sau RTD - SIC sau la o retea publica de comunicatii.

G. Intretinerea tehnica a SPAD sau RTD - SIC

Art. 314. - **(1)** In contractele de intretinere a SPAD si RTD - SIC care stocheaza, proceseaza sau transmit informatii secrete de stat, se vor specifica cerintele care trebuie indeplinite pentru ca personalul de intretinere si aparatura specifica a acestuia sa poata fi introduse in zona de operare a sistemelor respective.

(2) Personalul de intretinere trebuie sa detina certificate de securitate de nivel corespunzator nivelului de secretizare a informatiilor la care au acces.

Art. 315. - Scoaterea echipamentelor sau a componentelor hardware din zona SPAD sau RTD - SIC se executa in conformitate cu prevederile procedurilor operationale de securitate.

Art. 316. - Cerintele mentionate la art. 314 trebuie stipulate in CSS, iar procedurile de desfasurare a activitatii respective trebuie stabilite in procedurile operationale de securitate. Nu se accepta tipurile de intretinere care constau in aplicarea unor proceduri de diagnosticare ce implica accesul de la distanta la sistem, decat daca activitatea respectiva se desfasoara sub control strict si numai cu aprobarea agentiei de acreditare de securitate.

H. Achizitii

Art. 317. - Sistemele SPAD sau RTD - SIC, precum si componentele lor hardware si software sunt achizitionate de la furnizori interni sau externi selectati dintre cei agreati de catre agentia de acreditare de securitate.

Art. 318. - Componentele sistemelor de securitate implementate in SPAD sau RTD - SIC trebuie acreditate pe baza unei documentatii tehnice amanuntite privind proiectarea, realizarea si modul de distribuire al acestora.

Art. 319. - SPAD sau RTD - SIC care stocheaza, proceseaza sau transmit informatii secrete de stat sau componentele lor de baza - sisteme de operare de scop general, produse de limitare a functionarii pentru realizarea securitatii si produse pentru comunicare in retea - se pot achizitiona numai daca au fost evaluate si certificate de catre agentia de acreditare de securitate.

Art. 320. - Pentru SPAD si RTD - SIC care stocheaza, proceseaza sau transmit informatii secrete de serviciu, sistemele si componentele lor de baza vor respecta, pe cat posibil, criteriile prevazute de prezentele standarde.

Art. 321. - La inchirierea unor componente hardware sau software, in special a unor medii de stocare, se

va tine cont ca astfel de echipamente, odata utilizate in SPAD sau RTD - SIC ce proceseaza, stocheaza sau transmit informatii clasificate, vor fi supuse masurilor de protectie reglementate prin prezentele standarde. O data clasificate, componentele respective nu vor putea fi scoase din zonele SPAD sau RTD - SIC decat dupa declasificare.

I. Acreditarea SPAD si RTD - SIC

Art. 322. - **(1)** Toate SPAD si RTD - SIC, inainte de a fi utilizate pentru stocarea, procesarea sau transmiterea informatiilor clasificate, trebuie acreditate de catre agentia de acreditare de securitate, pe baza datelor furnizate de catre CSS, procedurilor operationale de securitate si altor documentatii relevante.

(2) Subsistemele SPAD si RTD - SIC si statiile de lucru cu acces la distanta sau terminalele vor fi acreditate ca parte integranta a sistemelor SPAD si RTD - SIC la care sunt conectate, in cazul in care un sistem SPAD sau RTD - SIC deserveste atat NATO, cat si organizatiile/structurile interne ale tarii, acreditarea se va face de catre autoritatea nationala de securitate, cu consultarea ADS si a agentiilor INFOSEC, potrivit competentelor.

J. Evaluarea si certificarea

Art. 323. - In situatiile ce privesc modul de operare de securitate multi-nivel, inainte de acreditarea propriu-zisa a SPAD sau RTD - SIC, hardware-ul, firmware-ul si software-ul vor fi evaluate si certificate de catre agentia de acreditare de securitate, in acest sens, institutia desemnata la nivel national pentru protectia informatiilor clasificate va stabili criterii diferentiate pentru fiecare nivel de secretizare a informatiilor vehiculate de SPAD sau RTD - SIC.

Art. 324. - Cerintele de evaluare si certificare se includ in planificarea sistemului SPAD si RTD - SIC si sunt stipulate explicit in CSS, imediat dupa ce modul de operare de securitate a fost stabilit.

Art. 325. - Urmatoarele situatii impun evaluarea si certificarea de securitate in modul de operare de securitate multi-nivel:

a) pentru SPAD sau RTD - SIC care stocheaza, proceseaza sau transmite informatii clasificate strict secret de importanta deosebita;

b) pentru SPAD sau RTD - SIC care stocheaza, proceseaza sau transmite informatii clasificate strict secret, in cazurile in care:

- SPAD sau RTD - SIC este interconectat cu un alt SPAD sau RTD - SIC - de exemplu, apartinand altui CSTIC;

- SPAD sau RTD - SIC are un numar de utilizatori posibili care nu poate fi definit exact.

Art. 326. - Procesele de evaluare si certificare trebuie sa se desfasoare, conform principiilor si instructiunilor aprobate, de catre echipe de expertizare cu pregatire tehnica adecvata si autorizate corespunzator. Aceste echipe vor fi compuse din experti selectionati de catre agentia de acreditare de securitate.

Art. 327. - **(1)** In procesele de evaluare si certificare se va stabili in ce masura un SPAD sau RTD - SIC indeplineste conditiile de securitate specificate prin CSS, avandu-se in vedere ca, dupa incheierea procesului de evaluare si certificare, anumite sectiuni - paragrafe sau capitole - din CSS trebuie sa fie modificate sau actualizate.

(2) Procesele de evaluare si certificare trebuie sa inceapa din stadiul de definire a SPAD sau RTD - SIC si continua pe parcursul fazelor de dezvoltare.

K. Verificari de rutina pentru mentinerea acreditarii

Art. 328. - Pentru toate SPAD si RTD - SIC care stocheaza, proceseaza sau transmit informatii secrete de stat, CSTIC stabileste proceduri de control prin care sa se poata stabili daca schimbarile intervenite in SIC sunt de natura a le compromite securitatea.

Art. 329. - **(1)** Modificarile care implica reacreditarea sau pentru care se solicita aprobarea anterioara a agentiei de acreditare de securitate trebuie sa fie identificate cu claritate si expuse in CSS.

(2) Dupa orice modificare, reparare sau eroare care ar fi putut afecta dispozitivele de securitate ale SPAD sau RTD - SIC, CSTIC trebuie sa efectueze o verificare privind functionarea corecta a dispozitivelor de securitate.

(3) Mentinerea acreditarii SPAD sau RTD - SIC trebuie sa depinda de satisfacerea criteriilor de verificare.

Art. 330. - **(1)** Toate SPAD si RTD - SIC care stocheaza, proceseaza sau transmit informatii secrete de stat sunt inspectate si reexaminate periodic de catre agentia de acreditare de securitate.

(2) Pentru SPAD sau RTD - SIC care stocheaza, proceseaza sau transmit informatii strict secrete de importanta deosebita, inspectia se va face cel putin o data pe an.

L. Securitatea microcalculatoarelor sau a calculatoarelor personale

Art. 331. - **(1)** Microcalculatoarele sau calculatoarele personale care au discuri fixe sau alte medii nevolatile de stocare a informatiei, ce opereaza autonom sau ca parte a unei retele, precum si calculatoarele portabile cu discuri fixe sunt considerate medii de stocare a informatiilor, in acelasi sens ca si celelalte medii amovibile de stocare a informatiilor.

(2) In masura in care acestea stocheaza informatii clasificate trebuie supuse prezentelor standarde.

Art. 332. - Echipamentelor prevazute la art. 331 trebuie sa li se acorde nivelul de protectie pentru acces,

manipulare, stocare si transport, corespunzator cu cel mai inalt nivel de clasificare a informatiilor care au fost vreodata stocate sau procesate pe ele, pana la trecerea la un alt nivel de clasificare sau declasificarea lor, in conformitate cu procedurile legale.

M. Utilizarea echipamentelor de calcul proprietate privata

Art. 333. - **(1)** Este interzisa utilizarea mediilor de stocare amovibile, a software-ului si a hardware-ului, aflate in proprietate privata, pentru stocarea, procesarea si transmiterea informatiilor secrete de stat.

(2) Pentru informatiile secrete de serviciu sau neclasificate, se aplica reglementarile interne ale unitatii.

Art. 334. - Este interzisa introducerea mediilor de stocare amovibile, a software-ului si hardware-ului, aflate in proprietate privata, in zonele in care se stocheaza, se proceseaza sau se transmit informatii clasificate, fara aprobarea conducatorului unitatii.

N. Utilizarea echipamentelor contractorilor sau a celor puse la dispozitie de alte institutii

Art. 335. - Utilizarea intr-un obiectiv a echipamentelor si a software-ului contractantilor, pentru stocarea, procesarea sau transmiterea informatiilor clasificate este permisa numai cu avizul CSTIC si aprobarea sefului unitatii.

Art. 336. - Utilizarea intr-un obiectiv a echipamentelor si software-ului puse la dispozitie de catre alte institutii poate fi permisa, in acest caz echipamentele sunt evidentiate in inventarul unitatii, in ambele situatii, trebuie obtinut avizul CSTIC.

O. Marcarea informatiilor cu destinatie speciala

Art. 337. - Marcarea informatiilor cu destinatie speciala se aplica, in mod obisnuit, informatiilor clasificate care necesita o distributie limitata si manipulare speciala, suplimentar fata de caracterul atribuit prin clasificarea de securitate.

CAPITOLUL IX
CONTRAVENTII SI SANCTIUNI LA NORMELE PRIVIND PROTECTIA INFORMATIILOR CLASIFICATE

Art. 338. - **(1)** Constituie contraventii la normele privind protectia informatiilor clasificate urmatoarele fapte:

a) detinerea fara drept, sustragerea, divulgarea, alterarea sau distrugerea neautorizata a informatiilor secrete de stat;

b) neindeplinirea masurilor prevazute in art. 18, 25-28, 29, 96-139 si 140-181;

c) neindeplinirea obligatiilor prevazute la art. 31, 41-43, 213, 214;

d) nerespectarea normelor prevazute in art. 140-142, 145, 159, 160, 162, 163, 179-181, 183 alin. (1) si 185-190;

e) neindeplinirea sau indeplinirea defectuoasa a obligatiilor prevazute in art. 240 alin. (2) si (3), art. 243 si art. 248, precum si nerespectarea regulilor prevazute in art. 274-336.

(2) Contraventiile prevazute la alin. (1) se sanctioneaza astfel:

a) contraventiile prevazute la alin. (1) lit. a) se sanctioneaza cu amenda de la 500.000 lei la 50.000.000 lei in cazul faptelor de detinere fara drept sau de alterare a informatiilor clasificate si cu amenda de la 10.000.000 lei la 100.000.000 lei, in cazul faptelor de sustragere, divulgare sau distrugere neautorizata a informatiilor clasificate;

b) faptele prevazute in alin. (1) lit. b) si c) se sanctioneaza cu avertisment sau cu amenda de la 500.000 lei la 25.000.000 lei;

c) faptele prevazute in alin. (1) lit. d) se sanctioneaza cu avertisment sau cu amenda de la 1.000.000 lei la 50.000.000 lei;

d) faptele prevazute in alin 1 lit. e) se sanctioneaza cu amenda de la 5.000.000 lei la 50.000.000 lei.

(3) Persoanele sau autoritatile care constata contraventiile pot aplica, dupa caz, si sanctiunea complementara, constand in confiscarea, in conditiile legii, a bunurilor destinate, folosite sau rezultate din contraventii.

(4) Dispozitiile reglementarilor generale referitoare la regimul juridic al contraventiilor se aplica in mod corespunzator.

Art. 339. - **(1)** Contraventiile si sanctiunile prevazute la art. 338 se constata si se aplica, in limitele competentelor ce le revin, de catre persoane anume desemnate din Serviciul Roman de Informatii, Ministerul Apararii Nationale, Ministerul de Interne, Ministerul Justitiei, Serviciul de Informatii Externe, Serviciul de Protectie si Paza si Serviciul de Telecomunicatii Speciale.

(2) Pot sa constate contraventiile si sa aplice sanctiunile prevazute la art. 338, in limitele competentelor stabilite:

a) persoane anume desemnate din ORNISS;

b) conducatorii autoritatilor sau institutiilor publice, agentilor economici cu capital partial sau integral de stat si ai altor persoane juridice de drept public;

c) autoritatile sau persoanele prevazute de reglementarile generale referitoare la regimul juridic al contraventiilor.

(3) Plangerile impotriva proceselor-verbale de constatare a contraventiilor si de aplicare a sanctiunilor se solutioneaza potrivit reglementarilor generale privind regimul juridic al contraventiilor.

CAPITOLUL X
DISPOZITII FINALE

Art. 340. - Nomenclatura functiilor, conditiile de studii si vechime, precum si salarizarea personalului cu atributii privind evidenta, intocmirea, pastrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea si distrugerea informatiilor clasificate se stabilesc potrivit actelor normative in vigoare.

Art. 341. - Conducatorii unitatilor care gestioneaza informatii clasificate vor lua masuri ca dispozitiile prezentelor standarde sa fie aduse la cunostinta tuturor salariatilor si vor intreprinde masuri pentru:

a) crearea structurilor interne specializate cu atributii in aplicarea prezentelor standarde;

b) nominalizarea personalului cu atributii si functii privind gestionarea informatiilor clasificate;

c) initierea demersurilor prevazute de lege si de prezentele standarde, pentru obtinerea abilitarilor privind accesul la informatii clasificate.

Art. 342. - La solicitarea persoanelor juridice din sfera de competenta a Serviciului Roman de Informatii, R.A. Rasirom va evalua conformitatea si va prezenta ORNISS propuneri de eliberare a certificatelor de acreditare a calitatii pentru sistemele si echipamentele de protectie fizica a informatiilor clasificate.

Art. 343. - **(1)** Prezentele standarde se interpreteaza si se aplica in concordanta cu Normele privind protectia informatiilor clasificate ale Organizatiei Tratatului Atlanticului de Nord in Romania, aprobate prin Hotararea Guvernului nr. 353 din 15 aprilie 2002.

(2) In eventualitatea unor neconcordante intre cele doua reglementari mentionate la alin (1), au prioritate Normele privind protectia informatiilor clasificate ale Organizatiei Tratatului Atlanticului de Nord in Romania, aprobate prin Hotararea Guvernului nr. 353 din 15 aprilie 2002.

Art. 344. - Dispozitiile prezentelor standarde referitoare la contraventiile si sanctiunile la normele privind protectia informatiilor clasificate se aplica dupa 60 de zile de la publicarea prezentei hotarari.

Art. 345. - Anexele nr. 1-32 fac parte integranta din prezentele standarde nationale de protectie a informatiilor clasificate. privind gestionarea acestora.

ANEXA Nr. 1

FISA DE CONSULTARE
a documentului "Strict secret de importanta deosebita" nr. _____ din _____
privind _____

Nr. crt.	Numele, prenumele si functia celor care au luat cunostinta de continutul documentului	Numarul si seria certificatului de securitate	Data si ora primirii documentului	Semnatura celui care a primit documentul	Cine a aprobat consultarea documentului (numele, prenumele, functia)	Data si ora restituirii documentului	Numele, prenumele si semnatura celui care a primit documentul (in urma restituirii)	Obs.

ANEXA Nr. 2

ROMANIA
UNITATEA_____
Compartimentul _____
Nr. _____ din _____

FISA DE PREGATIRE INDIVIDUALA

NUME:
PRENUME:
FUNCTIA:
COMPARTIMENTUL:

Nr. crt.	Tema pregatirii	Forma de pregatire	Locul	Perioada	Semnatura titularului de fisa	Observatii

+---------+----------+---------+--------------+----------+----------+----------+
+---------+----------+---------+--------------+----------+----------+----------+

ANEXA Nr. 3

ANGAJAMENT DE CONFIDENTIALITATE*)

_____

*) Pentru persoanele care au acces la informatii secrete de stat si de serviciu.

Subsemnatul _____ nascut in localitatea _____ la data de _____, fiul (fiica) lui _____ si a _____ angajat al _____ in functia de _____, cu domiciliul in localitatea _____, strada _____, nr. ____, bl. ____, sc. ____, et. ____, ap. ____, judetul/sectorul _____, posesor al certificatului/autorizatiei seria _____, nr. _____, declar ca am luat cunostinta de dispozitiile legale cu privire la protectia informatiilor clasificate si ma angajez sa pastrez cu strictete secretul de stat si de serviciu, sa respect intocmai normele legale cu privire la evidenta, manipularea si pastrarea informatiilor, datelor si documentelor secrete de stat si de serviciu ce mi-au fost incredintate, inclusiv dupa incetarea activitatilor care presupun accesul la aceste informatii.

Sunt constient ca in cazul in care voi incalca prevederile normative privind protectia informatiilor clasificate voi raspunde, potrivit legii, administrativ, disciplinar, material, civil ori penal, in raport cu gravitatea faptei.

Data .....

Semnatura

.....

DAT IN PREZENTA

_____,

(numele si prenumele functionarului de securitate)

Semnatura

ANEXA Nr. 4

ROMANIA
(UNITATEA)

_____

Compartimentul _____

REGISTRUL DE EVIDENTA
al informatiilor strict secrete de importanta deosebita

INTRARE

Nr. de inregistrare	Data inregistrarii: anul	luna	ziua	Nr. si data documentului la expeditor	De la cine provine	Continutul pe scurt al documentului	Nr. ex.	Nr. file/ ex.	Nr. anexe	Nr. file anexe	Cui i s-a repartizat documentul

IESIRE

Data expedierii: anul	luna	ziua	Destinatar	Nr. ex.	Nr. file	Nr. anexe	Nr. file anexe	Nr. borderoului de expediere	Nr. dosarului si fila unde a fost clasat documentul sau nr. procesului-verbal de distrugere	Observatii

ANEXA Nr. 5

ROMANIA
(UNITATEA)

_____

Compartimentul _____

REGISTRUL DE EVIDENTA

al informatiilor strict secrete si secrete

INTRARE

Nr. de inregistrare	Data inregistrarii			Nr. si data documentului	De la cine provine	Nr. file/ ex.	Nivelul de secretizare	Continutul pe scurt al documentului	Nr. anexe	Nr. file anexe	Cui i s-a repartizat documentul
	anul	luna	ziua	la expeditor							

IESIRE

Data expedierii			Nivelul de secretizare	Destinatar	Nr. ex.	Nr. file anexe	Nr. file anexe	Nr. borderoului de expediere	Nr. dosarului si fila unde a fost clasat documentul (nr. procesului-verbal de distrugere)	Observatii
anul	luna	ziua								

ANEXA Nr. 6

ROMANIA
(UNITATEA)

Compartimentul _____

REGISTRUL DE EVIDENTA
al informatiilor secrete de serviciu

INTRARE

Nr. de inregistrare	Data inregistrarii			Nr. si data documentului la expeditor	De la cine provine	Continutul pe scurt al documentului	Nr. ex.	Nr. file/ ex.	Nr. anexe	Nr. file anexe	Cui i s-a repartizat documentul
	anul	luna	ziua								

IESIRE

Data expedierii			Destinatar	Nr. ex.	Nr. file anexe	Nr. anexe	Nr. file anexe	Nr. borderoului de expediere	Nr. dosarului si fila unde a fost clasat documentul (nr. procesului-verbal de distrugere)	Observatii
anul	luna	ziua								

ANEXA Nr. 7

REGISTRU UNIC
de evidenta a registrelor, condicilor, borderourilor si a
caietelor pentru insemnari clasificate

Nr. crt./ seria	Nr. file	Denumirea materialelor distribuite	Numele, prenumele celui care a primit materialul	Seria si numarul certificatului de securitate	Data distribuirii			Semnatura celui care a primit materialul	Nr. dosarului unde a fost clasat sau nr. procesului-verbal de distrugere	Obs.
					Ziua	Luna	Anul			

ANEXA Nr. 8

ROMANIA
(UNITATEA)

Compartimentul _____

CONDICA DE PREDARE - PRIMIRE
a documentelor clasificate

Nr. crt.	Compunerea documentului					Numele, prenumele, seria si nr. certificatului de securitate ale persoanei careia i-a fost predat documentul	Data	Semnatura de primire	Semnatura de restituire	Obs.
	Nr. de inregistrare	Denumire document	Clasa (nivelul de secretizare)	Ex. nr.	Nr. de dosare, mape sau file					

ANEXA Nr. 9

ROMANIA
(UNITATEA)
_____
Compartimentul _____

REGISTRUL
de evidenta a informatiilor clasificate multiplicate

INTRARE

Nr. de inregistrare	Compartimentul care a solicitat copierea	Numele si prenumele celui care a predat documentul	Numarul de inregistrare al documentului original si al cererii de copiere	Data si semnatura de primire a documentului pentru copiat	Nivelul de secretizare al documentului copiat	Nr. file	Nr. anexe

IESIRE

Documentul copiat		Forma de copiere	Data, numele si prenumele persoanei care a primit originalul si copiile	Observatii
Nr. exemplare	Total file copiate			

ANEXA Nr. 10

ANTET
(institutia/agentul economic)

Nr. _____ din _____

CLASIFICAREA
(dupa completare, in functie de nivelul maxim de clasificare a informatiilor pe care le cuprinde)
APROB
(functia, numele si prenumele conducatorului institutiei/agentului economic, semnatura si stampila)

PROGRAMUL DE PREVENIRE A SCURGERII DE INFORMATII CLASIFICATE DETINUTE DE
_____
(unitatea care il intocmeste)

CAPITOLUL I

BAZA LEGALA

Se va mentiona cadrul normativ care a stat la baza intocmirii programului.

CAPITOLUL II

1. GENERALITATI

Se va face o scurta prezentare a institutiei/agentului economic, sucursalelor si filialelor. Vor fi prezentate elementele de concretizare a identitatii, statutului juridic, obiectul de activitate.

2. OBIECTIVE

Vor fi prezentate obiectivele urmarite prin masurile prezentate in program. Vor fi vizate urmatoarele obiective minimale: - apararea informatiilor clasificate impotriva actiunilor de compromitere, sabotaj, sustragere, distrugere neautorizata sau alterare; - prevenirea accesului neautorizat la astfel de informatii, a cunoasterii si diseminarii lor ilegale; - inlaturarea riscurilor si vulnerabilitatilor ce pot pune in pericol protectia informatiilor clasificate; - asigurarea cadrului procedural necesar protectiei informatiilor clasificate.

3. PRINCIPII

Se precizeaza principiile care stau la baza masurilor de prevenire a scurgerii de informatii. Masurile de prevenire a scurgerii de informatii se bazeaza pe: - autorizarea accesului la informatiile clasificate absolut necesare indeplinirii atributiilor de serviciu (principiul "nevoii de a cunoaste"); - asigurarea aplicarii masurilor de protectie, in mod diferentiat, pe zone de securitate si in functie de nivelurile de acces la informatii clasificate; - accesul la informatii clasificate este permis numai in baza verificarilor si abilitarilor legale; - aplicarea, in mod obligatoriu si unitar, a masurilor de protectie atat in locurile in care se depoziteaza informatiile clasificate si in cazul sistemelor informatice care stocheaza, prelucreaza sau transmit informatii de acest fel, cat si al persoanelor care au acces la acestea si utilizatorilor retelelor respective; - raspunderea personala privind aplicarea masurilor de protectie stipulate prin programul de prevenire a scurgerii de informatii clasificate.

CAPITOLUL III

1. ELEMENTE GENERALE PRIVIND INFORMATIILE CLASIFICATE DETINUTE DE INSTITUTIA/AGENTUL ECONOMIC

Se vor face precizari privind clasele si nivelurile de secretizare a informatiilor clasificate detinute de institutia/agentul economic (in cazul celor primite de la alti emitenti se va mentiona baza juridica a detinerii, respectiv tipul contractului si daca s-au asumat obligatii de protejare a secretului prin incheierea de acorduri intre parti).

2. LISTA INFORMATIILOR CLASIFICATE, APROBATE PRIN HOTARARE A GUVERNULUI (DOCUMENTE, DATE, OBIECTE SAU ACTIVITATI, INDIFERENT DE SUPORT SAU FORMA), PE CLASE SI NIVELURI DE SECRETIZARE, DETINUTE DE UNITATEA IN CAUZA

Institutiile/agentii economici vor intocmi lista cuprinzand categoriile informatiilor clasificate, pe care le detin, pe clase si niveluri de secretizare. Lista va fi actualizata ori de cate ori situatia o impune (clasificarea sau declasificarea unor informatii).

3. LOCURI UNDE SE CONCENTREAZA, DE REGULA ORI TEMPORAR, DATE, INFORMATII, DOCUMENTE CLASIFICATE SAU SE DESFASOARA ASTFEL DE ACTIVITATI (CONFORM ANEXEI NR. 10/A)

Vor fi mentionate: - spatiile destinate pastrarii documentelor clasificate; - spatiul destinat sistemului/retelelor informatice de procesare automata a datelor care preia, prelucreaza, stocheaza si transmite date si informatii clasificate; - alte locuri unde se gestioneaza sau se manipuleaza asemenea date, informatii si documente clasificate sau se desfasoara astfel de activitati.

CAPITOLUL IV

1. LISTA FUNCTIILOR CARE NECESITA ACCES LA INFORMATII CLASIFICATE
Vor fi precizate functiile care necesita accesarea informatiilor clasificate, pe clase si niveluri de secretizare, cu respectarea stricta a principiului "nevoii de a cunoaste".

2. PREZENTAREA PERSOANEI/STRUCTURII DESEMNATE SA INDEPLINEASCA ATRIBUTII PE LINIA PROTECTIEI ACTIVITATILOR, DATELOR, INFORMATIILOR SI DOCUMENTELOR CLASIFICATE
2.1. Pentru fiecare persoana in parte se vor preciza: - numele si prenumele; - datele de identificare (prenumele parintilor, nume anterioare, data si locul nasterii, profesia si locul de munca, domiciliul, telefonul); 2.2. Atributiile si competentele privind asigurarea protectiei informatiilor clasificate. Nominalizarea se va face de catre conducatorul institutiei/agentului economic respectiv, situatia fiind prezentata pe niveluri de acces, care va fi acordat numai in urma obtinerii abilitarii.

3. PREZENTAREA PERSOANELOR CARE AU SAU URMEAZA SA AIBA ACCES LA INFORMATII CLASIFICATE, PE NIVELURI DE SECRETIZARE
Va fi intocmita lista cu persoanele care au sau urmeaza sa aiba acces la informatii clasificate, nominalizate de catre conducatorul institutiei/agentului economic (inclusiv cele care lucreaza in sistemul informatic si de telecomunicatii, destinat prelucrarii, prelucrarii, stocarii si transmiterii de informatii clasificate)*) Va fi intocmita, de asemenea, lista cu persoanele carora li se acorda acces temporar la informatii clasificate din cadrul sau din afara institutiei/agentului economic (inclusiv cele apartinand firmelor prestatoare de servicii pentru intretinerea sau instalarea programelor, care vor fi avizate corespunzator nivelului maxim de secretizare a informatiilor din sistemele informatice si de telecomunicatii)**) Accesul la informatii clasificate va fi permis numai dupa obtinerea Pentru fiecare persoana nominalizata vor fi precizate: - numele, prenumele si (datele de identificare (prenumele parintilor, nume anterioare, data si locul nasterii, profesia si locul de munca, domiciliul, telefonul); - informatiile clasificate care ii sunt absolut necesare indeplinirii atributiilor de serviciu, cu precizarea clasei si nivelului de secretizare a acestuia.

***)** Numarul persoanelor nominalizate in lista respectiva va fi cel mult egal cu cel al functiilor ce necesita acces la informatiile clasificate.

****)** Listele respective vor fi actualizate, cu indeplinirea procedurilor legale de avizare, in raport de necesitati (extinderea sau limitarea accesului unor persoane la informatii clasificate, in functie de modificarea atributiilor de serviciu).

CAPITOLUL V

1. MASURI DE PROTECTIE FIZICA A CLADIRILOR, SPATIILOR/LOCURILOR UNDE SE PASTREAZA SAU SE CONCENTREAZA INFORMATII CLASIFICATE ORI SE DESFASOARA ASTFEL DE ACTIVITATI (CONFORM ANEXEI NR. 10/B)
Vor fi stipulate masuri vizand: - securitatea cladirilor; - controlul intrarilor si iesirilor; - paza; - containerele si incaperile de securitate; - incuietorile; - controlul cheilor si combinatiilor; - dispozitivele de detectare a intrusilor; - protectia fizica a copiatoarelor si dispozitivelor telefax; - planurile de urgenta.

2. MASURI PROCEDURALE DE PROTECTIE A DATELOR, INFORMATIILOR, DOCUMENTELOR ORI A ACTIVITATILOR CLASIFICATE
Vor fi prezentate: - reguli de evidenta, procesare, manipulare, accesare, multiplicare, transmitere, pastrare si stocare a datelor, informatiilor si documentelor clasificate indiferent de suport (aprobate de conducerea institutiei/agentului economic); - reguli de acces pentru personalul propriu; - reguli de acces pentru personalul/persoanele din afara institutiei/agentului economic, inclusiv pentru straini sau reprezentanti mass-media.

CAPITOLUL VI

PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC SI DE TELECOMUNICATII DESTINAT PRELUARII, PRELUCRARII, STOCARII SI TRANSMITERII DE DATE SI INFORMATII CLASIFICATE

Vor fi prezentate echipamentele de comunicatii si birotica (telefoane, fax, telex, copiatoare) prin care vor fi transmise/prelucrate informatii clasificate.
Vor fi prezentate, de asemenea, echipamentul informatic existent, calculatoarele conectate la Internet, sistemele de protectie utilizate si firma prestatoare de servicii pentru intretinerea sau instalarea programelor (conform anexei nr. 10/C).
In situatia in care unele dintre aceste echipamente nu sunt protejate corespunzator, se va face precizarea ca folosirea acestora pentru prelucrarea informatiilor clasificate este interzisa.

CAPITOLUL VII

MASURI DE PROTECTIE IMPOTRIVA OBSERVARII SI ASCULTARII*)

_____

***)** Zonele in care se elaboreaza si/sau se discuta informatii clasificate secret de stat trebuie protejate impotriva observarii si ascultarii pasive si/sau active. Responsabilitatea inlaturarii riscurilor privind observarea si ascultarea revine institutiei/agentului economic, care elaboreaza sau, dupa caz, gestioneaza informatii clasificate (conform anexei nr. 10/D)

CAPITOLUL VIII

1. CONTROALE, ACTIVITATI DE ANALIZA SI EVALUARE A MODULUI IN CARE SE RESPECTA PREVEDERILE LEGALE REFERITOARE LA PROTECTIA INFORMATIILOR CLASIFICATE

Vor fi prezentate tematica si periodicitatea controalelor (inopinate, periodice), cine le executa, documentele ce se intocmesc si sanctiunile ce se vor aplica in cazurile de incalcare a reglementarilor privind protectia informatiilor clasificate.
Se va intocmi planificarea, activitatilor de evaluare si analiza a starii de protectie a informatiilor clasificate si se va prevedea ca anual, dupa incheierea operatiunii de inventariere a suportilor de informatii clasificate sa se analizeze si sa se evalueze modul in care au fost respectate prevederile programului, prevazandu-se si masurile care se impun si termenele de remediere a unor nereguli constatate.

2. SOLUTIONAREA CAZURILOR DE INCALCARE A REGLEMENTARILOR PRIVIND PROTECTIA INFORMATIILOR CLASIFICATE (CONFORM ANEXEI Nr. 10/E)

Se vor face referiri la: - masurile ce vor fi luate in cazul constatarii incalcarii reglementarilor privind protectia informatiilor clasificate; - evidenta incalcarilor reglementarilor de securitate; - comunicarea compromiterilor; - scoaterea din evidenta a documentelor clasificate pierdute sau distruse.

CAPITOLUL IX

MASURI DE INSTRUIRE SI EDUCATIE PROTECTIVA A PERSOANELOR CARE AU ATRIBUTII PE LINIA PROTECTIEI INFORMATIILOR CLASIFICATE SI A CELOR CARE AU ACCES LA ASTFEL DE INFORMATII (CONFORM ANEXEI Nr. 10/F)*)

| Se vor preciza: |
| - situatii care impun asemenea masuri; |
| - responsabilitati; |
| - mijloace si metode de instruire si pregatire contrainformativa. |

Intocmit
(numele, prenumele si semnatura
functionarului de securitate)

Raspunderea pentru intocmirea, avizarea si aplicarea programului de prevenire a scurgerii de informatii clasificate revine conducatorului unitatii detinatoare.

Programul de prevenire a scurgerii de informatii clasificate se actualizeaza, anual sau ori de cate ori se impune (identificarea unor noi riscuri si vulnerabilitati, aparitia unor noi situatii sau acte normative), modificarile efectuate aducandu-se de fiecare data la cunostinta institutiei abilitate, unde se transmite sub forma de completare pentru a fi avizat.

Se intocmeste in 2 exemplare (un exemplar la beneficiar si unul la institutia abilitata).

_____

***)** Planul specific de pregatire a personalului este elaborat la inceputul fiecarui an. In continutul acestuia vor fi mentionate responsabilitatile, termenele, mijloacele si metodele de instruire si educatie protectiva. Functionarul sau structura de securitate va tine evidenta instruirilor/activitatilor de educatie protectiva si va asigura pregatirea tuturor persoanelor avizate pentru acces la informatii clasificate, care nu au participat la instruirile organizate.

ANEXA Nr. 10/A

LOCURI UNDE SE CONCENTREAZA, DE REGULA ORI TEMPORAR,
DATE, INFORMATII SI DOCUMENTE CLASIFICATE SAU
SE DESFASOARA ASTFEL DE ACTIVITATI

De la caz la caz, pentru fiecare zona administrativa, zona de securitate sau incinta in care se desfasoara activitati, se lucreaza cu/se gestioneaza informatii clasificate vor fi mentionate masurile de securitate protectiva existente si garantiile pe care le prezinta in protectia informatiilor si activitatilor clasificate. De asemenea, se vor mentiona sarcinile si atributiile ce trebuie indeplinite conform Regulamentului de organizare si functionare interna.

Masurile de protectie fizica a incaperilor si locurilor unde se pastreaza sau se manipuleaza informatii clasificate sau se desfasoara astfel de activitati se vor organiza si implementa in functie de zonele de securitate. Accesul in zonele de securitate si incaperile in care se deruleaza activitati ori se lucreaza cu informatii clasificate va fi permis exclusiv persoanelor abilitate, potrivit nivelurilor de clasificare, cu respectarea principiului "nevoii de a cunoaste".

Zonele in care sunt manipulate sau stocate informatii clasificate trebuie organizate si administrate in asa fel incat sa corespunda uneia dintre urmatoarele categorii:

a) Zona de securitate clasa I, care presupune ca orice persoana aflata in interiorul acesteia are acces la informatii secrete de stat, de nivelul "strict secret" si "strict secret de importanta deosebita".

O asemenea zona necesita:

- un perimetru clar definit si protejat, in care toate intrarile si iesirile sunt supravegheate;

- controlul sistemului de intrare, care sa permita numai accesul persoanelor verificate corespunzator si autorizate in mod special;

- indicarea clasei si nivelului de securitate a informatiilor existente in zona;

b) Zona de securitate clasa a II-a, care presupune ca gestionarea informatiilor de nivel secret se realizeaza prin aplicarea unor masuri specifice de protectie impotriva accesului persoanelor neautorizate.

O asemenea zona necesita:

- perimetru clar definit si protejat, in care toate intrarile si iesirile sunt supravegheate;

- controlul sistemului de intrare, pentru a permite accesul neinsotit numai persoanelor verificate si autorizate sa patrunda in aceasta zona. Pentru toate celelalte persoane trebuie sa existe reguli de insotire, supraveghere si prevenire a accesului neautorizat la informatii clasificate sau in sectoare in care sunt manipulate si stocate astfel de informatii.

Incintele in care nu se lucreaza zilnic 24 de ore vor fi inspectate dupa orele de program, pentru a verifica daca informatiile clasificate sunt asigurate in mod corespunzator.

c) Zona administrativa

In jurul zonelor de securitate clasa I sau clasa a II-a poate fi stabilita o zona administrativa cu perimetru vizibil definit, in interiorul careia sa existe posibilitatea de control al personalului si vehiculelor, in zona administrativa sunt permise manipularea si pastrarea numai a informatiilor secrete de serviciu.

ANEXA Nr. 10/B

MASURI DE PROTECTIE FIZICA A CLADIRILOR, SPATIILOR/LOCURILOR UNDE SE PASTREAZA SAU SE CONCENTREAZA DATE, INFORMATII SI DOCUMENTE CLASIFICATE ORI SE DESFASOARA ASTFEL DE ACTIVITATI

Securitatea cladirilor

Cladirile, spatiile/locurile in care se afla informatii clasificate trebuie protejate impotriva accesului neautorizat.

Masurile de protectie (grilaje la ferestre, incuietori la usi, paza la intrari, sisteme automate pentru controlul accesului, controale si patrule de securitate, sisteme de alarma sau pentru detectarea intrusilor etc.) vor fi dimensionate in raport cu:

a) clasa de securitate a informatiilor, suportul, volumul si modul de depozitare a acestora in cladire;

b) calitatea containerelor in care sunt depozitate informatiile clasificate;

c) locul de dispunere a spatiilor/locurilor unde se pastreaza sau se concentreaza date, informatii si documente clasificate ori se desfasoara astfel de activitati;

d) caracteristicile cladirii.

Controlul intrarilor si iesirilor

Intrarile in zonele de securitate clasa I si clasa a II-a vor fi controlate prin permis de intrare sau printr-un sistem special de recunoastere personala aplicat personalului permanent, in mod obligatoriu se va institui un sistem de control al vizitatorilor pentru prevenirea accesului neautorizat la informatiile clasificate.

Se recomanda ca permisul de intrare sa nu arate, in clar, identitatea organizatiei emitente sau locul in care detinatorul are acces. Controlul intrarilor si iesirilor poate fi insotit de un sistem de identificare automata, care trebuie considerat suplimentar, fara a presupune o inlocuire totala a pazei.

Daca se apreciaza necesar, la intrarea sau la iesirea din zonele de securitate clasa I sau clasa a II-a, se vor efectua controale pentru depistarea si/sau prevenirea tranzitarii fara drept a informatiilor si materialelor clasificate.

Paza

Folosirea paznicilor pentru asigurarea zonelor de securitate si a informatiilor clasificate se va face numai dupa ce au fost verificati, li s-a acordat abilitarea de securitate corespunzatoare zonei si li s-a efectuat pregatirea de specialitate. Vor fi precizate inclusiv masuri de control si supraveghere corespunzatoare a paznicilor.

Patrularile in zonele de securitate clasa I si clasa a II-a se vor realiza in afara orelor de program si in zilele nelucratoare, la intervale care vor fi stabilite in functie de amenintarea locala, pentru a exista garantia ca informatiile clasificate sunt protejate in mod corespunzator.

Pentru eficientizarea sistemelor de paza, in special in zonele de securitate unde, in interesul securitatii, paznicii nu pot avea intrare directa, trebuie asigurate masuri menite sa previna accesul neautorizat si sa detecteze eventualele incercari de patrundere fara drept in aceste perimetre, prin folosirea unor modalitati adecvate (televiziune cu circuit inchis, sisteme de alarma sau pentru inspectare vizuala). De la caz la caz, astfel de modalitati pot fi folosite si ca substitute ale patrulelor.

Containere si incaperi de securitate

Containerele folosite pentru pastrarea informatiilor clasificate se impart in trei clase:

- clasa A: containere aprobate la nivel national pentru depozitarea informatiilor strict secrete de importanta deosebita in zone de securitate clasa I sau clasa a II-a;
- clasa B: containere aprobate la nivel national pentru pastrarea informatiilor strict secrete si secrete in zone de securitate clasa I sau clasa a II-a;
- clasa C: mobilier de birou adecvat numai pentru pastrarea informatiilor secrete de serviciu.

Incaperile de securitate sunt construite (amenajate) in zone de securitate clasa I sau clasa a II-a, unde informatiile clasificate secret de stat sunt pastrate pe rafturi deschise sau sunt expuse pe harti, diagrame etc. Peretii, podelele, plafoanele, usile si incuietorile acestor incaperi vor oferi o protectie echivalenta clasei containerului de securitate aprobat pentru pastrarea informatiilor clasificate respective.

Incuietori

Incuietorile folosite la containerele si incaperile de securitate in care sunt pastrate informatii clasificate se impart in trei grupe astfel:

- grupa A: incuietori aprobate la nivel national pentru containerele din clasa A;
- grupa B: incuietori aprobate la nivel national pentru containerele din clasa B;
- grupa C: incuietori indicate numai pentru mobilierul de birou adecvat numai pentru pastrarea informatiilor secrete de serviciu (pentru clasa C).

Controlul cheilor si combinatiilor

Cheile containerelor si incaperilor de securitate nu trebuie scoase din cladirea sau zona de securitate in care se afla documentele clasificate.

Combinatiile incuietorilor (containerelor de securitate) vor fi cunoscute numai de persoanele abilitate.

Pentru cazurile de urgenta, un rand de chei suplimentare (o evidenta scrisa a fiecarei combinatii) vor fi pastrate in plicuri mate sigilate intr-un compartiment stabilit de conducerea institutiei/agentului economic, sub control corespunzator, in containere separate. Evidenta fiecarei combinatii trebuie pastrata in plic separat. Cheilor si plicurilor trebuie sa li se asigure protectie la nivelul de securitate a informatiilor clasificate la care acestea permit accesul.

Cunoasterea combinatiilor incuietorilor de la containerele de securitate va fi restransa la un numar minim de persoane. Cheile si combinatiile vor fi schimbate:

a) ori de cate ori are loc o schimbare de personal;

b) de fiecare data cand se constata ca a avut loc un compromis de natura sa le faca vulnerabile;

c) la intervale regulate, de preferinta o data la sase luni (fara a se depasi 12 luni).

Dispozitive de detectare a intrusilor

Cand se folosesc sisteme de alarma, televiziune cu circuit inchis sau alte dispozitive destinate supravegherii zonelor de securitate sau protectiei informatiilor clasificate, sursa de alimentare trebuie sa aiba atat conectare permanenta, cat si de rezerva (eventual, o baterie reincarcabila). Orice defectare sau interventie neautorizata asupra acestor sisteme trebuie sa declanseze o alarma sau un alt sistem de avertizare pentru personalul care monitorizeaza instalatia respectiva.

Protectia fizica a copiatoarelor si dispozitivelor telefax

Copiatoarele si dispozitivele telefax trebuie protejate fizic, in masura in care este necesar sa se garanteze folosirea lor numai de catre persoanele autorizate.

Planuri de urgenta

Fiecare autoritate si institutie/agent economic vor pregati planuri pentru protejarea informatiilor clasificate in cazuri de urgenta, care sa prevada inclusiv evacuarea si distrugerea acestora atunci cand este cazul.

Protectia, evacuarea si/sau distrugerea materialelor strict secrete si secrete, in cazuri de urgenta, nu trebuie sa afecteze protectia, evacuarea si/sau distrugerea materialelor strict secrete de importanta deosebita, sau a materialelor codificate, care vor avea totdeauna prioritate fata de alte documente clasificate.

ANEXA Nr. 10/C

PROTECTIA SISTEMELOR/SUBSISTEMELOR INFORMATICE DESTINATE PRELUARII, PRELUCRARII, STOCARII SI TRANSMITERII DE DATE SI INFORMATII CLASIFICATE SI A INCAPERILOR IN CARE ACESTEA SE AFLA AMPLASATE

- Administratorul si utilizatorii sistemului destinat preluarii, prelucrarii, stocarii si transmisiei de date si informatii clasificate sunt numiti de seful institutiei/agentului economic;

- Administratorul, utilizatorii si persoanele care au acces la date si informatii cu caracter secret de stat, procesate prin sisteme de prelucrare automata a datelor sunt supuse procedurilor de selectionare, verificare si avizare, potrivit nivelurilor de acces.

- Incaperile unde sunt amplasate sisteme/subsisteme informatice destinate preluarii, prelucrarii, stocarii si transmisiei de date si informatii cu caracter secret de stat vor fi asigurate cu sisteme de supraveghere si control-acces potrivit standardelor in vigoare, corespunzator nivelurilor de clasificare a informatiilor.

- Sistemul/subsistemul informatic destinat preluarii, prelucrarii, stocarii si transmisiei de date si informatii secrete de stat va fi prevazut cu sistem de secretizare prin metode, mijloace si echipamente pentru asigurarea integritatii, confidentialitatii si disponibilitatii acestora.

- Utilizarea sistemelor informatice care preiau, prelucreaza, stocheaza si transmit date cu caracter secret de stat se face pe baza de parole si coduri si chei de criptare care se pastreaza in plicuri sigilate la dispozitia sefului unitatii.

- Accesul in sistemul/subsistemul informatic destinat preluarii, prelucrarii, stocarii si transmiterii de date si informatii clasificate se atribuie, individual si diferentiat, in conformitate cu atributiile de serviciu ale fiecarui utilizator pentru pornirea, utilizarea si oprirea sistemului de calcul, introducerea, citirea, modificarea, stergerea sau transferul de date in/din bazele de date ale sistemului informatic gestionarea si manipularea cheilor de criptare/decriptare.

- Consultarea, introducerea, modificarea sau stergerea informatiilor din baza de date se executa numai cu aprobarea sefului institutiei/agentului economic, asigurandu-se o evidenta stricta, in scopul realizarii eventualei examinari ulterioare a activitatii, a interactiunii utilizatorilor cu sistemele de calcul, prin memorarea momentului, tipului operatiei, codului utilizatorului si datelor accesate de acesta.

- Elaborarea de lucrari din bazele de date ale sistemului/subsistemului destinat preluarii, prelucrarii, stocarii si transmiterii de date si informatii clasificate se efectueaza numai pe baza ordinelor rezolutive, ale conducerii unitatii, date pe adrese sau documente interne de lucru.

- Suportii de memorie externa (discurile, discurile portabile, dischetele, benzile magnetice, casetele de banda magnetica, compact-discurile, discurile optice sau magneto-optice), utilizati in sistemul/subsistemul

destinat preluarii, prelucrarii, stocarii si transmiterii de date si informatii clasificate, au regimul documentelor cu caracter secret de stat si se pastreaza la compartimentul de documente secrete, fiind supusi procedurilor restrictive identice acestora.

- Instalarea, depanarea sau modificarea configuratiei sistemului de calcul destinat destinat preluarii, prelucrarii, stocarii si transmiterii de date si informatii clasificate se executa de personal abilitat, verificat contrainformativ si controlat.
- Saptamanal, administratorul sistemului informatic destinat preluarii, prelucrarii, stocarii si transmiterii de date si informatii clasificate va elimina fisierele temporare de lucru sau iesite din uz si va verifica integritatea fisierelor stocate pe discuri.
- Intrarea si iesirea atat a persoanelor cat si a materialelor vor fi controlate.
- In incintele in care sistemul/subsistemul poate fi modificat nu se va permite accesul unui singur angajat autorizat (se va institui regula celor doi).
- Persoanele care solicita acces temporar sau intermitent in aceste incaperi vor obtine aprobare de vizitator de la administratorul de sistem; vizitatorii trebuie supravegheati permanent pentru a preveni accesul la echipamentele informatice in scopuri ilicite.

Un pericol in domeniul protectiei informatiilor clasificate procesate, stocate si transmise prin sistemul de prelucrare automata a datelor il reprezinta orice actiune, inactiune sau imprejurare de natura sa afecteze integritatea, disponibilitatea sau confidentialitatea datelor, precum si functionalitatea programelor si echipamentelor aferente unui sistem informatic.

Constituie pericole:

- pierderea, sustragerea, inlocuirea, alterarea sau distrugerea neautorizata ori accidentala a datelor, programelor, suportilor materiali ai acestora sau a echipamentelor aferente;
- operarea gresita in timpul preluarii, prelucrarii, transferului, stocarii sau arhivarii datelor;
- interceptarea si interpretarea transmisiilor efectuate in cadrul retelei de calculatoare;
- fortarea accesului, accesul neautorizat sau intarzierea accesului autorizat la date, programe, suportii materiali ai acestora sau la echipamentele aferente;
- eludarea restrictiilor privind accesul la date, prin modificarea neautorizata a configuratiilor instalate, programelor sau a drepturilor de acces;
- copierea neautorizata a datelor;
- interceptarea si interpretarea radiatiilor electromagnetice sau acustice produse de echipamentele de calcul, dispozitivele de transmisiuni sau canalele de comunicatie;
- interceptarea discutiilor sau convorbirilor telefonice referitoare la sistemul informatic;
- exploatarea informativa a personalului implicat in dezvoltarea, intretinerea sau exploatarea sistemului informatic;
- introducerea in exploatare de produse informatice fara o prealabila testare care sa ofere garantii de functionare corecta si controlata;
- pastrarea, amplasarea, exploatarea, intretinerea sau depozitarea in conditii improprii a sistemelor de calcul, suportilor materiali de date sau a dispozitivelor si echipamentelor destinate asigurarii protectiei si securitatii datelor;
- nerespectarea reglementarilor referitoare la secretul de stat sau a regulilor de compartimentare a muncii;
- nerespectarea regulilor privind depozitarea, manipularea sau distrugerea suportilor de memorie externa si a dispozitivelor si echipamentelor scoase din uz;
- nerespectarea prevederilor, metodologiilor si a documentatiilor tehnice de intretinere si exploatare a sistemelor informatice;
- aparitia de anomalii in functionarea sistemelor de operare, pachetelor de programe sau programelor de aplicatie;
- aparitia de anomalii in functionarea sistemelor informatice;
- aparitia de deranjamente ale canalelor de comunicatie;
- discutarea in conditii de insecuritate sau cu persoane neautorizate, a unor aspecte privind sistemele de calcul, informatiile si datele inmagazinate;
- producerea de calamitati naturale (cutremure, inundatii, alunecari de teren, etc.);
- producerea de evenimente cu efect distructiv (explozii, incendii, spargeri de conducte, acte de sabotaj, actiuni teroriste, acte de vandalism, socuri electromagnetice, etc);
- producerea pe orice cale de evenimente cu efecte similare.

POSIBILE PERICOLE, AMENINTARI ORI ATACURI LA ADRESA SECURITATII SISTEMULUI/RETELELOR INFORMATICE

- ascultare pasiva (atac contra confidentialitatii): accesarea sistemului in scopul modificarii informatiilor generate, transmise, stocate sau afisate pe componentele vulnerabile ale acestuia;
- interceptia: penetrarea neautorizata a sistemului, in scopul modificarii informatiilor transmise pe o cale de comunicatie;
- deducerea prin interferenta: actiunea unui utilizator autorizat de a corela informatiile la care are acces, in scopul deducerii unor informatii clasificate la care nu are dreptul de acces;
- deghizarea ("inselarea" mecanismelor de autentificare): insusirea si folosirea identitatii unui utilizator

autorizat, pentru accesarea sistemului;
- crearea si utilizarea unor canale disimulate ("ocolirea" controalelor de acces) in scopul transmiterii de informatii de la un utilizator autorizat catre unul neautorizat;
- utilizarea asa-zisei "porti secrete" (trap-desk) pentru evitarea controalelor de acces.

ANEXA Nr. 10/D

MASURI DE PROTECTIE IMPOTRIVA OBSERVARII SI ASCULTARII

Protectia impotriva ascultarilor pasive (posibile prin ascultare directa sau furnizate de comunicatii nesigure) se realizeaza pe baza asistentei tehnice din partea institutiilor abilitate, prin izolarea fonica a peretilor, usilor, podelelor si plafoanelor zonelor sensibile.

Protectia impotriva ascultarilor active (prin microfoane, radio-emitatori si alte dispozitive implantate) necesita inspectii de securitate tehnica si/sau fizica a structurii incaperii, accesoriilor, instalatiilor tehnico-sanitare, echipamentelor si mobilierului de birou, sistemelor de comunicatii etc. Aceste inspectii vor fi realizate de institutii competente.

Zone sigure din punct de vedere tehnic

Accesul in zonele protejate impotriva ascultarilor se va controla in mod special.

Incaperile vor fi incuiate sau pazite corespunzator standardelor de securitate fizica, inclusiv cand nu sunt ocupate, iar cheile vor fi tratate ca materiale clasificate. Periodic, se vor organiza inspectii fizice si/sau tehnice. De asemenea, astfel de inspectii se vor organiza, in mod obligatoriu, ca urmare a oricarei intrari neautorizate, a unei suspiciuni privind accesul personalului extern si dupa executarea lucrarilor de reparatii, intretinere, zugravire, redecorare etc. Nici un obiect nu se va introduce in aceste zone, fara a fi verificat de catre personal specializat in depistarea dispozitivelor de ascultare.

In mod curent, in zonele asigurate din punct de vedere tehnic nu se vor instala telefoane. Totusi, cand instalarea acestora este absolut necesara, trebuie prevazute cu un dispozitiv de deconectare pasiv.

Inspectiile de securitate tehnica in zonele unde se poarta discutii extrem de sensibile trebuie intreprinse in mod obligatoriu premergator inceperii convorbirilor, atat pentru identificarea fizica a dispozitivelor de ascultare cat si pentru verificarea sistemelor telefonice, electrice, sau de alta natura, care ar putea fi folosite ca mediu de atac.

Verificarea dotarilor electrice/electronice din birouri

Inainte de a fi folosite in zonele in care se lucreaza ori se discuta despre informatii strict secrete de importanta deosebita si strict secrete, echipamentele de comunicatii si dotarile de orice fel din birouri, in principal cele electrice si electronice, trebuie verificate de specialisti in securitatea comunicatiilor, pentru a preveni transmiterea ilicita sau din neglijenta a unor informatii inteligibile.

In aceste zone se va organiza o evidenta a tipului si numarului de inventar ale fiecarei piese de mobilier sau echipament introduse sau mutate din incaperi, care va fi pastrata sub cheie, iar cheile vor fi protejate corespunzator.

ANEXA Nr. 10/E

SOLUTIONAREA CAZURILOR DE INCALCARE A REGLEMENTARILOR PRIVIND PROTECTIA INFORMATIILOR CLASIFICATE

Cazurile de incalcare a reglementarilor de securitate vor fi comunicate imediat conducatorului institutiei/agentului economic si institutiilor abilitate.

Orice incalcare a reglementarilor de securitate va fi cercetata de persoane special desemnate, cu experienta in activitatea de securitate pentru a stabili:
- daca si in ce mod au fost compromise informatii clasificate;
- daca persoanele neautorizate care au avut, sau ar fi putut avea acces la informatii clasificate, prezinta suficienta incredere si loialitate, astfel incat rezultatul compromiterii sa nu creeze prejudicii;
- masurile de remediere, corective sau disciplinare (inclusiv juridice), care sunt recomandate.

In situatia in care persoanele care au luat cunostinta de continutul informatiilor clasificate prezinta incredere, vor fi instruite in mod corespunzator pentru a preveni diseminarea, in caz contrar se va proceda la evaluarea prejudiciului rezultat si vor fi intreprinse masurile necesare diminuarii acestuia.

Evidenta incalcarilor reglementarilor de securitate

In cadrul autoritatilor si institutiilor publice, agentilor economici cu capital integral sau partial de stat si altor persoane juridice de drept public sau privat, detinatoare de informatii clasificate, se va organiza evidenta cazurilor de incalcare a reglementarilor de securitate, a rapoartelor de investigatii si masurilor corective intreprinse, in consecinta. Aceste evidente vor fi pastrate timp de trei ani de catre structura/functionarul de securitate si vor fi puse la dispozitie in timpul controalelor efectuate de reprezentantii autorizati ai institutiilor abilitate.

Comunicarea compromiterilor

Informatiile clasificate sunt compromise cand continutul acestora (total sau partial) este cunoscut de persoane neautorizate (care nu au autorizare valabila de acces la acestea) ori cand au fost supuse riscului acestei cunoasteri neautorizate (informatiile clasificate pierdute, chiar si temporar, in afara unei zone de securitate sunt considerate a fi compromise).

Institutiile abilitate vor fi incunostiintate prin cel mai operativ sistem de comunicare asupra circumstantelor compromiterii unor astfel de informatii.

Scopul principal al comunicarii compromiterii este de a da posibilitatea recuperarii informatiilor, evaluarii prejudiciilor si intreprinderii actiunilor necesare sau aplicabile pentru minimalizarea consecintelor.

Informarea preliminara trebuie sa contina:

a) o descriere a informatiilor respective (clasificare si marcare, numarul de inregistrare, numarul de exemplare, continutul, data, emitentul);

b) o scurta prezentare a imprejurarilor in care a avut loc compromiterea, inclusiv data constatarii, perioada in care informatiile au fost expuse compromiterii si, daca se cunoaste, persoanele neautorizate care au avut sau ar fi putut avea acces la acestea;

c) precizari cu privire la eventuala informare a emitentului.

La solicitarea institutiilor abilitate, informarile preliminare vor fi completate pe masura derularii cercetarilor.

Evaluarile proprii ale institutiilor/agentilor economici, referitoare la prejudiciile si actiunile ce urmeaza a fi intreprinse pentru inlaturarea sau diminuarea acestora, vor fi prezentate in cel mai scurt timp institutiilor abilitate.

Scoaterea din evidenta a documentelor clasificate pierdute sau distruse

Cand exista indicii certe, confirmate in scris de institutiile abilitate cu atributii de control si investigare a compromiterii informatiilor clasificate, ca documentul dat in raspundere este iremediabil pierdut (si nu ratacit), acesta va fi scos din evidenta compartimentului care l-a gestionat, numai dupa finalizarea cercetarilor, cu avizul institutiilor abilitate.

ANEXA Nr. 10/F

MASURI DE INSTRUIRE SI EDUCATIE PROTECTIVA A PERSOANELOR CARE AU ATRIBUTII PE LINIA PROTECTIEI INFORMATIILOR CLASIFICATE SI A CELOR CARE AU ACCES LA ASTFEL DE INFORMATII

Educatia protectiva are ca principal obiectiv instruirea persoanelor care au acces la informatii clasificate in vederea aplicarii masurilor legale referitoare la protejarea informatiilor clasificate.

Educatia personalului se realizeaza prin derularea unor activitati specifice in cadrul carora persoanelor care acceseaza informatii clasificate le sunt prezentate:

- prevederile legislatiei in domeniul protectiei informatiilor clasificate;
- continutul programului de prevenire a scurgerilor de informatii clasificate;
- competentele institutiilor abilitate in domeniul protectiei datelor si informatiilor clasificate;
- aspectele semnificative pe linia protectiei secretelor de stat cu relevanta in domeniul specific de activitate;
- mijloacele si metodele utilizate de structurile specializate in culegerea de date si informatii clasificate;
- consecintele nerespectarii normelor legale in domeniu;
- alte elemente de interes pentru siguranta nationala.

Ca mijloace frecvent utilizate in procesul de educatie protectiva se pot folosi documentare, filme de specialitate, diapozitive, materiale publicitare etc.

ANEXA Nr. 11

ROMANIA
(UNITATEA)

_____

Compartimentul _____

CONDICA DE PREDARE - PRIMIRE
a cheilor de la incaperile si containerele de securitate

Nr. Crt.	Numele si prenumele persoanei careia i-a fost predata cutia cu chei	Data si ora primirii	Semnatura de primire	Nr. sigiliului	Numele si prenumele persoanei care ridica cutia cu chei	Semnatura de primire	Obs.

+----+----------------+--------+---------+----------+---------------+---------+----+
+----+----------------+--------+---------+----------+---------------+---------+----+
+----+----------------+--------+---------+----------+---------------+---------+----+
+----+----------------+--------+---------+----------+---------------+---------+----+

ANEXA Nr. 12

ROMANIA
(institutia)
_____
Compartimentul _____

CERTIFICAT DE SECURITATE
Seria _____ nr. _____ din _____

Prin prezentul certificat se autorizeaza accesul la informatii secrete de stat, nivelul _____, pentru dl./d-na (numele, prenumele, datele de identificare) _____, angajat al institutiei noastre in functia de _____.

Certificatul este valabil in perioada _____.

Seful institutiei,

_____
(semnatura, stampila)

Posesor: _____
(nume, prenume si semnatura)

ANEXA Nr. 13

ROMANIA
(institutia)
_____
Compartimentul _____

AUTORIZATIE DE ACCES LA INFORMATII CLASIFICATE
Seria _____ Nr. _____ din _____

Prin prezenta se autorizeaza accesul la informatii clasificate secret de stat, nivelul _____, pentru dl./d-na (numele, prenumele, datele de identificare) _____, angajat al institutiei noastre in functia de _____.

Autorizatia este valabila in perioada _____.

Seful institutiei,

_____
(semnatura, stampila)

Posesor: _____
(nume, prenume si semnatura)

ANEXA Nr. 14

ROMANIA
INSTITUTIA DETINATOARE
Nr. _____ din ___. ___._____

Catre
OFICIUL REGISTRULUI NATIONAL AL INFORMATIILOR SECRETE DE STAT

In vederea eliberarii certificatului de securitate/autorizatiei de acces la informatii clasificate, nivel _____, pentru (numele, prenumele si datele de identificare ale persoanei) _____, angajat al (denumirea completa a institutiei), in functia de _____, va rugam sa initiati procedurile de verificare necesare.

Mentionam ca in prezent persoana detine / nu detine certificat de securitate/ autorizatie de acces la informatii clasificate pentru nivelul _____.

Anexam in original chestionarul de securitate corespunzator nivelului

solicitat.

Semnatura
Sef institutie

ANEXA Nr. 15

Formular de baza - date personale
Nr. _____ din __.__.__

SECRET DE SERVICIU
(dupa completare)
Ex. unic

SPATIU REZERVAT INSTITUTIEI SOLICITANTE

Institutia solicitanta:

Nivelul de acces solicitat: [SECRET][ ] [S.S.][ ] [S.S.I.D.][ ]

Motivul solicitarii:

DATE GENERALE DESPRE SOLICITANT

NUME:

NUME ANTERIOARE:

PRENUME:

DATA NASTERII:

LOCUL NASTERII: sat: comuna:

oras/municipiu: judet:

CETATENIA: la nastere: actuala:

CARTE/BULETIN DE IDENTITATE:
Seria: Nr.: Eliberat de: La data:

Cod numeric personal:

DOMICILIUL PERMANENT:

Localitatea: Judetul/Sectorul:
Strada: Numarul: Bloc:
Scara: Etajul: Apartamentul: Codul postal:
Telefon fix: Telefon mobil:
Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Judetul/Sectorul:
Strada: Numarul: Bloc:
Scara: Etajul: Apartamentul: Codul postal:
Telefon fix: Telefon mobil:
Fax: E-mail:

DOMICILII PERMANENTE SI FLOTANTE IN ULTIMII CINCI ANI:

Tip de domiciliu: Permanent: Flotant:

Localitatea: Judetul/Sectorul:
Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Tip de domiciliu: Permanent: Flotant:

Localitatea: Judetul/Sectorul:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

ADRESE SI RESEDINTE IN STRAINATATE IN ULTIMII CINCI ANI:

(pentru perioade peste 3 luni)

Perioada: Tara: Localitatea:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Perioada: Tara: Localitatea:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

STUDII CIVILE SI MILITARE:

Nr. crt.	Perioada	Institutia	Felul studiilor

LIMBI STRAINE CUNOSCUTE

Nr. crt.	Limba	Nivelul

(In cazul atestatelor se vor indica institutia si data)

SITUATIA MILITARA:

Fara stagiu militar satisfacut: Militar activ: In rezerva:

Seria livretului militar: Numarul livretului militar:

Eliberat de centrul militar: la data:

PASAPOARTE:

Turistic
Seria: Numarul: Eliberat de: La data:

De serviciu
Seria: Numarul: Eliberat de: La data:

Diplomatic
Seria: Numarul: Eliberat de: La data:

CALATORII IN STRAINATATE IN ULTIMII CINCI ANI:

Nr. crt.	Tara	Localitatea	Perioada	Scopul

SITUATIA PROFESIONALA:

CIVIL:

Profesia:

Ministerul:

Institutia la care este incadrat:

De la data:

Functia:

De la data:

Adresa de la locul de munca:

Telefon: Fax: E-mail:

MILITAR:

Gradul: Functia:

Arma de baza: Arma de incadrare:

Unitatea:

Indicativul esalonului superior:

LOCURI DE MUNCA IN ULTIMII CINCI ANI:

Nr. crt.	INSTITUTIA	PERIOADA	FUNCTII DETINUTE

SITUATIA FAMILIALA ACTUALA

Celibatar(a): Casatorit(a): Concubinaj:

Despartit(a) in fapt: Divortat(a): Vaduv(a):

Recasatorit(a):

Alte situatii:

Date referitoare la data si locul incheierii casatoriei sau legate de situatia actuala:

DATE DESPRE PARTENERUL DE VIATA

(SOT/SOTIE, CONCUBIN/CONCUBINA)

NUME:

NUME ANTERIOARE:

PRENUME:

DATA NASTERII:

LOCUL NASTERII: comuna: oras: judet:

CETATENIA: la nastere: actuala:

PROFESIA:

LOCUL DE MUNCA:

DOMICILIUL PERMANENT:

Localitatea: Judetul/Sectorul:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Judetul/Sectorul:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

DOMICILII PERMANENTE SI FLOTANTE IN ULTIMII CINCI ANI:

Tip de domiciliu: Permanent: Flotant:

Localitatea: Judetul/Sectorul:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Tip de domiciliu: Permanent: Flotant:

Localitatea: Judetul/Sectorul:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

COPII (inclusiv cei din alte casatorii)

Nume si prenume	Data nasterii	Localitatea	Domiciliul	Locul de munca	Functia

DATE DESPRE PARINTI

TATAL

NATURA RELATIEI: tata natural: tata adoptiv: tata vitreg:

NUME:

NUME ANTERIOARE:

PRENUME:

PROFESIA:

DATA NASTERII:

LOCUL NASTERII: comuna: oras: judet:

CETATENIA: la nastere: actuala:

DOMICILIUL PERMANENT:

Localitatea: Judetul/Sectorul:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Judetul/Sectorul:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail:

MAMA

NATURA RELATIEI: mama naturala: mama adoptiva: mama vitrega:

NUME:

NUME ANTERIOARE:

PRENUME:

PROFESIA:

DATA NASTERII:

LOCUL NASTERII: comuna: oras: judet:

CETATENIA: la nastere: actuala:

DOMICILIUL PERMANENT:

Localitatea: Judetul/Sectorul:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Judetul/Sectorul:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: _____ Telefon mobil: _____

Fax: _____ E-mail: _____

DATE DESPRE FRATI/SURORI

NUME:

PRENUME:

DATA SI LOCUL NASTERII:

DOMICILIUL:

NUME:

PRENUME:

DATA SI LOCUL NASTERII:

DOMICILIUL:

NUME:

PRENUME:

DATA SI LOCUL NASTERII:

DOMICILIUL:

NUME:

PRENUME:

DATA SI LOCUL NASTERII:

DOMICILIUL:

ANTECEDENTE SI CAZIER

Ati fost vreodata retinut, arestat preventiv, anchetat, pus sub acuzare, judecat, condamnat (inclusiv la amenda penala sau interzicerea unor drepturi), gratiat, amnistiat, eliberat pe cautiune, eliberat conditionat? |DA| | |NU| |

Ati rost vreodata anchetat administrativ, sanctionat administrativ, amendat de catre politie sau autoritati civile (nu se mentioneaza amenzile pentru abateri minore, cum sunt cele pentru parcare, dar se mentioneaza cele pentru fapte grave, precum conducerea sub influenta alcoolului sau tulburarea ordinii publice)? |DA| | |NU| |

Ati fost vreodata judecat in Consiliul de Onoare, anchetat, judecat sau condamnat de o Curte Martiala, trimis intr-o unitate disciplinara in timpul cat v-ati aflat in serviciul militar? |DA| | |NU| |

Daca ati raspuns cu da la vreuna din intrebarile de mai sus, detaliati in spatiul de mai jos, inclusiv perioadele si institutiile care au sanctionat faptele dvs.:

Nr. crt.	FAPTA SAVARSITA	PERIOADA	INSTITUTIA

DATE PE SECURITATE

	Solicitantul	Partenerul de viata
Ati fost vreodata implicat in actiuni de: spionaj, terorism, tentative de subminare a ordinii democratice	[DA][ ]	[DA][ ]

prin mijloace violente? [NU][ ] [NU][ ]
Ati fost vreodata membru sau simpatizant al unei [DA][ ] [DA][ ]
grupari implicate in actiuni mentionate mai sus? [NU][ ] [NU][ ]
Ati fost vreodata in relatii apropiate cu o persoana [DA][ ] [DA][ ]
care a activat sau a simpatizat cu astfel de grupari? [NU][ ] [NU][ ]
Daca ati raspuns cu da la vreuna dintre intrebari detaliati mai jos:

	Solicitantul	Partenerul de viata
Ati colaborat cu organele fostei Securitati care au desfasurat activitati de politie politica?	[DA][ ] [NU][ ]	[DA][ ] [NU][ ]
Considerati ca ati atras atentia vreunui serviciu de informatii sau de securitate strain?	[DA][ ] [NU][ ]	[DA][ ] [NU][ ]
Considerati ca au fost facute presiuni asupra dumneavoastra sau asupra membrilor familiei dumneavoastra ca urmare a unui incident survenit pe teritoriul altei tari?	[DA][ ] [NU][ ]	[DA][ ] [NU][ ]
Sunteti in relatii permanente de natura profesionala sau personala cu cetateni straini?	[DA][ ] [NU][ ]	[DA][ ] [NU][ ]
Considerati ca vi s-a solicitat vreodata sa furnizati informatii clasificate in afara atributiilor de serviciu?	[DA][ ] [NU][ ]	[DA][ ] [NU][ ]

Daca ati raspuns cu da la vreuna dintre intrebari detaliati mai jos:

	Solicitantul	Partenerul de viata
Aveti rude apropiate, din cele mentionate mai sus, care locuiesc in strainatate sau care au locuit mai mult de trei luni in strainatate?	[DA][ ] [NU][ ]	[DA][ ] [NU][ ]

Daca ati raspuns cu da detaliati mai jos.

Nr. crt.	NUMELE SI PRENUMELE	GRADUL DE RUDENIE	TARA	PERIOADA

DECLARATIE

Subsemnatul, ...

Declar ca toate datele furnizate mai sus sunt reale.

Declar ca am luat cunostinta de cerintele procedurii de verificare si avizare pentru acces la informatiile nationale clasificate si le accept.

Consimt ca toate datele pe care le furnizez sa fie verificate, constient fiind de consecintele legale ale declaratiilor false sau omisiunilor cu buna stiinta.

Ma angajez sa furnizez orice date suplimentare care imi vor fi solicitate in eventualitatea unor neclaritati, precum si sa informez, din proprie initiativa, asupra oricarei modificari aparute in cele declarate mai sus.

Sunt de acord ca neacordarea avizului de securitate sa nu-mi fie motivata.

Data, Semnatura,

Data in prezenta

_____

(numele si prenumele functionarului de securitate)

Semnatura

ANEXA Nr. 16

FORMULAR SUPLIMENTAR
(se completeaza pentru nivelurile STRICT SECRET si STRICT SECRET DE IMPORTANTA DEOSEBITA)

SECRET DE SERVICIU
(dupa completare)
Ex. unic

Nr. _____ din ___.___.___

SPATIU REZERVAT INSTITUTIEI SOLICITANTE

Institutia solicitanta:

Nivelul de acces solicitat: [S.S.][ ] [S.S.I.D.][ ]

Motivul solicitarii:

DATE PERSONALE ALE SOLICITANTULUI

NUME:

PRENUME:

DATA NASTERII:

LOCUL NASTERII: sat: comuna:

oras/municipiu: judet:

CETATENIA actuala:

DATA COMPLETARII FORMULARULUI DE BAZA:

DATE SUPLIMENTARE DESPRE SOLICITANT

In afara domiciliilor, adreselor si resedintelor indicate in formularul de baza, in ultimii zece ani ati mai avut si altele?

IN ROMANIA

Perioada: Judet: Localitatea:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Judet: Localitatea:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Judet: Localitatea:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

IN STRAINATATE

Perioada: Tara: Localitatea:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Tara: Localitatea:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Tara: Localitatea:

Strada: Numarul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Tara: Localitatea:

Strada: _____ Numarul: _____ Bloc: _____

Scara: _____ Etajul: _____ Apartamentul: _____ Codul postal: _____

Perioada: _____ Tara: _____ Localitatea: _____

Strada: _____ Numarul: _____ Bloc: _____

Scara: _____ Etajul: _____ Apartamentul: _____ Codul postal: _____

RUDE

Cumnati/cumnate

GRAD DE RUDENIE				
NUMELE ACTUAL				
NUMELE LA NASTERE				
NUME ANTERIOARE				
PRENUMELE				
DATA NASTERII				
LOCUL NASTERII				
CETATENIA ACTUALA				
DOMICILIUL PERMANENT				
OCUPATIA ACTUALA				

Parintii partenerului de viata (naturali, vitregi sau adoptivi).

	TATAL		MAMA	
GRAD DE RUDENIE				
NUMELE ACTUAL				
NUMELE LA NASTERE				
NUME ANTERIOARE				
PRENUMELE				
DATA NASTERII				
LOCUL NASTERII				
CETATENIA ACTUALA				
DOMICILIUL PERMANENT				
OCUPATIA ACTUALA				

REFERINTE

Nominalizati date de identificare a minimum doua persoane, care sunt de acord sa prezinte referinte despre dumneavoastra si care va cunosc de cel putin cinci ani.

Numele si prenumele	Ocupatia	Locul de munca	Domiciliul permanent	Tel/Fax	Observatii

STARE DE SANATATE

Ati fost vreodata diagnosticat cu boala psihica?
Daca raspunsul este afirmativ, detaliati:

Ati suferit incidente de natura medicala care au provocat pierderea temporara a cunostintei?
Daca raspunsul este afirmativ, detaliati:

Sunteti constient de vreo alta problema medicala, neacoperita de raspunsurile anterioare, care ar putea afecta protectia informatiilor clasificate?
Daca raspunsul este afirmativ, detaliati:

Ati avut sau aveti probleme legate de consumul de alcool?
Daca raspunsul este afirmativ, detaliati:

Ati consumat sau consumati substante care creeaza dependenta sau droguri?
Daca raspunsul este afirmativ, detaliati:

RELATIILE DE FAMILIE

> Aveti neintelegeri dese in familie:
[DA][ ] [NU][ ]
Detaliati cu privire la motivul acestora:

> Aveti persoane in intretinere din afara casatoriei?
[DA][ ] [NU][ ] [CUNOSCUTE][ ] [NECUNOSCUTE][ ]
> Faceti referire cu privire la relatiile pe care le aveti cu cumnatii/cumnatele stabiliti/stabilite in strainatate, precum si la parintii partenerului de viata stabiliti in strainatate.

DECLARATIE

Subsemnatul .....

Declar ca toate datele furnizate mai sus sunt reale.

Declar ca am luat cunostinta de cerintele procedurii de verificare si avizare pentru acces la informatiile nationale clasificate si le accept.

Consimt ca toate datele pe care le furnizez sa fie verificate, constient fiind de consecintele legale ale declaratiilor false sau omisiunilor cu buna stiinta.

Ma angajez sa furnizez orice date suplimentare care imi vor fi solicitate in eventualitatea unor neclaritati, precum si sa informez, din proprie initiativa, asupra oricarei modificari aparute in cele declarate mai sus.

Sunt de acord ca neacordarea avizului de securitate sa nu-mi fie motivata.

Data, Semnatura,

Data in prezenta

_____

(numele si prenumele functionarului de securitate)
Semnatura

ANEXA Nr. 17

Formular financiar — SECRET DE SERVICIU

Nr. ___ din ___.___.___ — (dupa completare)

(Se completeaza numai pentru S.S.I.D.) — Ex. unic

SPATIU REZERVAT INSTITUTIEI SOLICITANTE

Institutia solicitanta: +----------+

+----------+

Motivul solicitarii: +----------+

+----------+

DATE GENERALE DESPRE SOLICITANT

NUME: +----------+

+----------+

NUME ANTERIOARE: +----------+

+----------+

PRENUME: +----------+

+----------+

DATA NASTERII: +----------+

+----------+

LOCUL NASTERII: sat: +----------+ comuna: +----------+

+----------+ +----------+

oras/municipiu: +----------+ judet: +----------+

+----------+ +----------+

CETATENIA: actuala: +----------+

+----------+

SITUATIA FAMILIALA

> Cum va apreciati situatia financiara?

Confortabila: [ ] Acceptabila: [ ] Dificila: [ ] Nu pot aprecia: [ ]

Locuinta

> Locuinta pe care o folositi impreuna cu ceilalti membri ai familiei este:

Proprietate personala: [ ] Inchiriata: [ ] Locuinta de serviciu: [ ]

PROPRIETATI MOBILE/IMOBILE

> Detaliati:

+----------+

| |

+----------+

Venituri si cheltuieli lunare tipice pentru dumneavoastra si partenerul de viata

> Venit anual net realizat in urma activitatii principale. +----------+

+----------+

> Venituri suplimentare realizate din alte activitati. +----------+

+----------+

> Total venituri anuale pe gospodarie. +----------+

+----------+

> Evaluati care este valoarea totala a debitelor curente care va greveaza. +----------+

Sunteti dvs. sau partenerul de viata beneficiarii unor castiguri provenind din jocuri de noroc sau alt gen de astfel de castiguri:

[DA][ ] [NU][ ]

Daca Da detaliati:

+----------+

| |

+----------+

Dumneavoastra si partenerul dumneavoastra de viata economisiti

Curent [ ] Ocazional [ ] Rar [ ]

Comparativ cu anul anterior aveti obligatii si datorii financiare:

Mai mari: [ ] Mai mici: [ ] Cam la fel: [ ]

Sunteti interesat, dvs. sau partenerul de viata in colaborarea cu anumite societati comerciale inregistrate in tara? [DA][ ] [NU][ ]

Daca "da", detaliati:

- denumirea societatii comerciale, adresa, domeniul de activitate
- caracterul interesului (asociere, membru in Consiliul de administratie, consilier etc.)

+----------+

| |

+----------+

Aveti relatii, dvs. sau partenerul de viata cu firme inregistrate in strainatate? [DA][ ] [NU][ ]

Daca da, detaliati:

- denumirea firmei, adresa, domeniul de activitate

- caracterul interesului (asociere, membru in Consiliul de administratie, consilier, contracte de colaborare, concesionare, comision etc.)
- tara de inmatriculare.

Impotriva dvs. sau a asociatilor dvs. au fost initiate, in ultimii 10 ani, proceduri de executare silita? [DA][ ] [NU][ ]
Daca da, detaliati:
- motivul procedurii
- instanta judecatoreasca care a hotarat masura
- autoritatea care a pus-o in aplicare

Aveti interese financiare care ar putea intra in conflict cu indatoririle dumneavoastra de serviciu? [DA][ ] [NU][ ]
Detaliati:

Detaliati alte aspecte care ne-ar putea ajuta sa intelegem mai bine situatia dumneavoastra financiara?
Detaliati:

DECLARATIE

Subsemnatul, ...

Declar ca toate datele furnizate mai sus sunt reale.

Declar ca am luat cunostinta de cerintele procedurii de verificare si avizare pentru acces la informatiile nationale clasificate si le accept.

Consimt ca toate datele pe care le furnizez sa fie verificate, constient fiind de consecintele legale ale declaratiilor false sau omisiunilor cu buna stiinta.

Ma angajez sa furnizez orice date suplimentare care imi vor fi solicitate in eventualitatea unor neclaritati, precum si sa informez, din proprie initiativa, asupra oricarei modificari aparute in cele declarate mai sus.

Sunt de acord ca neacordarea avizului de securitate sa nu-mi fie motivata.

Data, Semnatura,

Data in prezenta

_____

(numele si prenumele functionarului de securitate)

Semnatura

ANEXA Nr. 18

ROMANIA

_____

(Institutia)

Compartimentul _____

REGISTRUL

pentru evidenta certificatelor de securitate/autorizatiilor de acces la informatii clasificate

Nr. crt.	Numele, prenumele si datele de identificare ale posesorului	Functia si departamentul/ compartimentul in care isi desfasoara activitatea	Nivelul de acces	Data eliberarii certificatului/ autorizatiei	Seria si numarul certificatului/ autorizatiei	Perioada de valabilitate	Data retragerii	Motivul retragerii	Obs.

ANEXA Nr. 19

ROMANIA
OFICIUL REGISTRULUI NATIONAL
AL INFORMATIILOR SECRETE DE STAT
Nr. ___ din ___.___.___
Catre
(Autoritatea desemnata de securitate)

In vederea eliberarii avizului de securitate, nivel _____, pentru (numele, prenumele si datele de identificare ale persoanei) _____, angajat al (denumirea completa a institutiei) _____, in functia de _____ va rugam sa initiati procedurile de verificare necesare.

Mentionam ca in prezent persoana detine/nu detine certificat de securitate/ autorizatie de acces la informatii clasificate pentru nivelul _____.

Anexam in original chestionarul de securitate corespunzator nivelului solicitat.

Directorul general al Oficiului Registrului National
al Informatiilor Secrete de Stat,
(Semnatura)

ANEXA Nr. 20

ROMANIA
(Autoritatea desemnata de securitate)
Nr. _____ din _____.____.____
Catre
OFICIUL REGISTRULUI NATIONAL AL INFORMATIILOR SECRETE DE STAT

La adresa dumneavoastra nr. _____ din _____ va comunicam avizarea pozitiva/negativa a accesului la informatii secrete de stat de nivel _____ pentru (numele, prenumele si datele de identificare ale persoanei) _____ angajat al institutiei _____ (denumirea institutiei solicitante _____ in functia de _____

Seful Autoritatii desemnate de securitate,

ANEXA Nr. 21

ROMANIA
OFICIUL REGISTRULUI NATIONAL
AL INFORMATIILOR SECRETE DE STAT
Nr. _____ din _____.____.____
Catre
(Institutia solicitanta)

La adresa dumneavoastra nr. _____ din _____ va comunicam avizarea pozitiva/negativa a accesului la informatii secrete de stat de nivel _____ pentru (numele, prenumele si datele de identificare ale persoanei) _____ angajat al institutiei dvs., in functia de _____

Directorul general al Oficiului Registrului National
al Informatiilor Secrete de Stat,
(Semnatura)

ANEXA Nr. 22

ROMANIA
(Institutia)
_____
Nr. _____ din _____.____.____
Catre
OFICIUL REGISTRULUI NATIONAL AL INFORMATIILOR SECRETE DE STAT

Va comunicam eliberarea la data de _____ a certificatului de securitate/autorizatiei de acces la informatii clasificate cu seria _____, nr. _____ pentru dl/d-na (numele, prenumele, datele de identificare) _____ _____, angajat al institutiei noastre in functia de _____.

Certificatul/autorizatia este valabil/a in perioada _____, pentru accesul la informatii clasificate de nivel _____.

Seful institutiei,

_____

(semnatura, stampila)

ANEXA Nr. 23

ROMANIA
(Institutia)

_____

Compartimentul _____

REGISTRUL
pentru evidenta autorizatiilor speciale

Nr. crt.	Numele, prenumele si datele de identificare ale posesorului	Denumirea si adresa completa a unitatii detinatorului	Data eliberarii autorizatiei	Numarul si seria autorizatiei	Perioada de valabilitate	Obs.

ANEXA Nr. 24

ANTETUL INSTITUTIEI/AGENTULUI ECONOMIC
Adresa Tel./Fax

Catre ORNISS

CERERE
pentru eliberarea autorizatiei de securitate industriala

Va rugam sa eliberati autorizatia de securitate industriala pentru

_____

(denumirea completa a institutiei/agentului economic)

cu sediul in _____

_____

(adresa completa)

in vederea participarii la proceduri de atribuire a contractelor clasificate.

Anexam, in original, chestionarul de securitate industriala pentru obtinerea autorizatiei de securitate.

Directorul institutiei/agentului economic,

_____

(semnatura, stampila)

ANEXA Nr. 25

Secret de serviciu
(dupa completare)

(SE COMPLETEAZA NUMAI PENTRU ELIBERAREA AUTORIZATIEI DE SECURITATE INDUSTRIALA)

CHESTIONAR
de securitate industriala

1. AGENTUL ECONOMIC SOLICITANT

Denumire completa:
Nr. din Registrul Comertului:

|Data ultimei actualizari la Registrul Comertului: |
+---+
|Denumiri anterioare (daca este cazul): |
| |
+---+
|Cod fiscal: Cod SIRUES: |
+---+
|Stare Firma |
+---+
|Adresa completa pentru sediul social: |
|Str. ..... nr. ..... |
|Sectorul/judetul ..... Localitatea ..... |
|Nr. telefon ..... fax: ..... |
|Telex ..... e-mail ..... |
|Adresa site Internet ..... |
|Cod postal (Casuta postala, daca este cazul): ..... |
+---+
|Adrese anterioare (daca este cazul): |
| |
+---+
|Statutul juridic: |
| |
+---+
|Forma de proprietate: |
| |
+---+
|Capitalul |
| Capitalul social: ..... |
| Data ultimei modificari a capitalului social: ..... |
| Capital subscris varsat: ..... |
| Capital disponibil ..... |
| Nr. actiuni: ..... Valoare actiuni: ..... |
| Actiune nominativa. Exista? [ ] Da [ ] Nu |
| Autoritatea/persoana care o detine ..... |
| Adresa site Internet ..... |
| Crestere preconizata ..... la data de: ..... |
| Organigrama societatii (se ataseaza la chestionar) |
+---+
|Actionari persoane fizice (care detin peste 5% din capitalul social) |
| Numar ..... |
| 1. Nume, prenume ..... |
| Data si locul nasterii ..... |
| Nr. si seria actului de identitate |
| Adresa completa: |
| Str. ..... nr. ..... |
| Sectorul/judetul ..... oras/ municipiu ..... |
| Nr. telefon ..... fax: ..... |
| Telex ..... e-mail ..... |
| Adresa site Internet ..... |
| Cod postal (casuta postala, daca este cazul): ..... |
| Tara ..... |
| Procentul de actiuni/parti sociale detinut ___% incepand cu anul: ..... |
| (In cazul in care sunt mai multi se pot prezenta in anexa, dupa prezentul |
| model) |
+---+
|Actionari persoane juridice |
|..... |
|..... |
+---+
|Agenti economici la care firma solicitanta este actionar |
|Numarul de agenti economici: .....|
| Ce reprezinta pentru dvs.? |
| [ ] Furnizor |
| [ ] Client |
| [ ] Altceva |
| Procentul de actiuni detinut _____% incepand cu anul: .....|
+---+
|Firmele la care persoane din consiliul de administratie sunt actionari: |
| 1. Numele si prenumele persoanei: |
| Denumirea completa a firmei: |
| Nr. din Registrul Comertului |

2. CONDUCEREA AGENTULUI ECONOMIC SI FUNCTIONARUL/STRUCTURA DE SECURITATE RESPONSABIL/RESPONSABILA

Director general
- Nume si prenume: .....
- Prenumele tatalui: .....
- Data numirii in functie: .....
- Pregatire profesionala: .....
- Data nasterii: ..... locul: ..... tara: .....
- Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar (denumire, adresa completa)

Director economic
- Nume si prenume: .....
- Prenumele tatalui: .....
- Data numirii in functie: .....
- Pregatire profesionala: .....
- Data nasterii: ..... locul: ..... tara: .....
- Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar (denumire, adresa completa)

Director stiintific/tehnic/comercial
- Nume si prenume: .....
- Prenumele tatalui: .....
- Data numirii in functie: .....
- Pregatire profesionala: .....
- Data nasterii: ..... locul: ..... tara: .....
- Firme la care este D actionar, D in conducere, D proprietar (denumire, adresa completa)

Membrii consiliului de administratie
1. Nume si prenume: .....
   - Prenumele tatalui: .....
   - Data numirii in functie: .....
   - Pregatire profesionala: .....
   - Data nasterii: ..... locul: ..... tara: .....
   - Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar (denumire, adresa completa): a)
     b)
     c) .....
2.
3.
4.
5.
3.
4.
5.
6.

Functionarul/Structura de securitate responsabil/responsabila cu protectia informatiilor secrete de stat din cadrul agentului economic solicitant:
- Nume si prenume: .....
- Prenumele tatalui: .....
- Functia: .....
- Pregatire profesionala: .....
- Data nasterii: ..... locul: ..... tara: .....
- Firme la care este [ ] actionar [ ] in conducere [ ] proprietar (denumire, adresa completa)

(Datele de la aceasta rubrica se vor completa de catre toate persoanele din structura de securitate a agentului economic)

3. DATE DESPRE PROFILUL SI ACTIVITATEA DESFASURATA

Obiectul(ele) principal(e) de activitate:

Numar de angajati permanent:

Intreprinderea dvs. este distribuitorul autorizat al altor agenti economici?

|(situatia in ultimii 5 ani)
| [ ] Da [ ] Nu
| Numele si adresa completa (daca este cazul)
|

4. SCURT RAPORT PENTRU ULTIMII 3 ANI DE EXERCITIU FINANCIAR

Sfarsit perioada financiara				
Active fixe - TOTAL				
Conturi In lei:				
Conturi In valuta:				
Creante:				
Stocuri:				
Active circulante - TOTAL:				
Capital social:				
Capital varsat:				
Imprumuturi pe termen lung:				
Imprumuturi pe termen scurt:				
Datorii - TOTAL				
Total pasiv:				
Cifra de afaceri:				
Total venituri				
Total cheltuieli:				
Profit brut:				
Pierderi (unde este cazul):				

5. BONITATE SI GARANTII BANCARE

|Banci cu care lucrati (se vor completa urmatoarele informatii pentru fiecare banca):
| Denumire: .....
| Adresa completa:
| Str. ..... nr. .....
| Sectorul/judetul ..... localitatea .....
| Nr. telefon ..... fax: .....
| Telex ..... e-mail .....
| Adresa site Internet .....
| Numar cont: .....
| Data deschiderii contului: .....
| Creditul este: [ ] garantat [ ] negarantat
| Marimea creditului: .....

|Mijloace de plata la cumparare
| [ ] acreditiv [ ] ordin de plata [ ] transfer bancar
| [ ] conditii speciale [ ] Altele: .....

|Exista reclamatii impotriva firmei pentru platile cu furnizorii sau clientii?
| [ ] Da [ ] Nu
| Daca DA:
| Numarul reclamatiilor:
| Data inregistrarii:
| .....
| .....
| Pentru suma de (valoarea fiecarei plati contestate):

Reclamatia a fost rezolvata? [ ] Da [ ] Nu
Alte comentarii legate de aceasta:

6. INFORMATII DE SECURITATE

	DA	NU
Considerati ca firma dumneavoastra a atras atentia unui serviciu de informatii sau de securitate strain?		
Au existat cazuri cand au fost solicitate informatii cu caracter sensibil in afara atributiilor de serviciu? Institutia sau vreunul dintre angajati a fost implicat(a) sau a sprijinit activitati de:		
- spionaj		
- terorism		
- sabotaj?		
Ati avut vreodata angajati care au sprijinit sau au fost implicati in una dintre activitatile de mai sus?		
Aveti cunostinta de orice alte imprejurari, conditii (factori de risc), nedeclarate in raspunsurile precedente, care au putut influenta activitatea dvs. sau a personalului din subordine, cum ar fi: obisnuinta utilizarii unor substante psihotrope, dependenta de alcool, dificultati financiare deosebite?		

7. DATE REFERITOARE LA SISTEMUL DE PROTECTIE A INFORMATIILOR SECRETE DE STAT

7.1. PROTECTIA INFORMATIILOR

MENTIONATI NIVELUL DE CLASIFICARE A INFORMATIILOR GESTIONATE:
[ ] secrete de stat - S.S.I.D. [ ] [ ] secrete de serviciu
- S.S. [ ]
- S [ ]

7.1.1. LOCUL/LOCURILE UNDE SE CONCENTREAZA DATE SI INFORMATII SECRETE DE STAT		
	DA	NU
- incapere destinata numai protectiei informatiilor		
- incapere destinata numai sistemului/subsistemului de calcul destinat preluarii, prelucrarii, stocarii si transmisiei datelor si informatiilor secrete de stat		
- incaperile sunt prevazute cu:		
- pereti antifonati		
- usi si incuietori speciale		
- podele si tavane speciale pentru zone sensibile		
- alte locuri unde se concentreaza date si informatii sau se desfasoara activitati cu caracter secret de stat		

In legatura cu acestea se vor face precizari privind pozitia fata de punctul de acces si control, imprejurimi, garantiile ce le prezinta in asigurarea protectiei datelor si informatiilor ori activitatilor secrete de stat

.....

.....

.....

7.1.2. MASURI DE PROTECTIE FIZICA A INCAPERILOR SAU LOCURILOR UNDE SE PASTREAZA SAU SE CONCENTREAZA DATE SI INFORMATII SECRETE DE STAT ORI ACTIVITATI CU CARACTER SECRET DE STAT		
	DA	NU

Zone de securitate existente: > Zona de securitate clasa I/II (pentru gestionarea informatiilor secrete de stat)			
- perimetrul este clar definit si protejat, avand toate intrarile si iesirile controlate			
- accesul persoanelor neautorizate este permis conform prevederilor interne, cu escorta sau prin controale specifice			
> Zona administrativa (pentru manipularea si depozitarea informatiilor SECRETE DE SERVICIU)			
- perimetrul ofera posibilitatea de control al personalului si/sau vehiculelor			
- sunt utilizate:			
• registre si jurnale speciale pentru corespondenta, evidenta, transport etc.			
• mape speciale de pastrare			
• sigilii			
• fise de predare-primire			
• ecusoane de acces			
• mobila de birou adecvata zonei administrative			
7.1.3. PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC SI DE TELECOMUNICATII DESTINAT PRELUARII, PRELUCRARII, STOCARII SI TRANSMISIEI DE DATE SI INFORMATII SECRETE DE STAT			
Echipament de comunicatie si de birotica existent (telefoane, fax, telex, xerox)			
- in zona de securitate clasa I			
- in zona de securitate clasa a II-a			
Echipament informatic			
- aveti acces la Internet			
- este utilizat un sistem de securizare			
• pe server-ul principal			
• la nivel de utilizator			
7.1.4. MASURI PROCEDURALE DE PROTECTIE A INFORMATIILOR SECRETE DE STAT SAU A ACTIVITATILOR CU CARACTER SECRET DE STAT			
Aveti elaborate proceduri privind:			
- clasificarea informatiilor dupa niveluri de securitate			
- accesul pentru personalul propriu			
- accesul pentru personalul din afara, inclusiv straini si reprezentanti ai mass-media			
- multiplicarea, transportul si circulatia documentelor in interiorul si in afara institutiei, atat in timpul, cat si in afara programului de lucru			

- protectia sistemului/subsistemului informatic si de telecomunicatii		
- controlul intern, activitatea de analiza si evaluare a modului in care se respecta prevederile legale in vigoare, din care sa reiasa periodicitatea controalelor, cine le executa, documentele ce se intocmesc si cum se valorifica, raspunderi si sanctiuni		
- instruirea personalului autorizat a avea acces		

7.2. PROTECTIA PERSONALULUI

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZA SA AIBA ACCES LA INFORMATII SECRETE DE STAT

NR. CRT.	NUME, PRENUME	PRENUME PARINTI	DATA, LOC NASTERE	PROFESIE, FUNCTIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVATII**)

**) Se va inscrie ca mentiune daca are/urmeaza sa aiba acces si orice alte observatii considerate necesare.

8. DATE CU PRIVIRE LA PROCESE PENALE SAU CONTRAVENTII CA URMARE A INCALCARII LEGILOR

	DA	NU
In ultimii 10 ani a fost declansata impotriva intreprinderii dvs. o actiune in justitie care sa se fi soldat printr-o hotarare definitiva ce a afectat grav activitatea acesteia?		
In caz de raspuns afirmativ, precizati cand, de ce, denumirea instantei judecatoresti, sentinta, pedeapsa si perioada de executare.		
In ultimii 5 ani intreprinderea pe care o conduceti a fost acuzata de incalcarea legii si, drept urmare, sa fiti sanctionat cu amenda?		
In caz de raspuns afirmativ, aratati cand, cum, de ce, autoritatea care a constatat fapta si cuantumul amenzii.		

Orice schimbare referitoare la datele cuprinse in chestionar se transmite imediat sub forma de completare la chestionar.

Functia, numele, prenumele si semnatura conducatorului unitatii solicitante .....
Stampila unitatii solicitante .....
Localitatea si data completarii chestionarului .....

ANGAJAMENT

Subsemnatul(a) .....
(numele, initiala tatalui, prenumele - cu majuscule)
in calitate de ..... la .....
(functia) (denumirea completa a institutiei/agentului economic)
cu sediul in .....
(adresa completa)
certific pe propria-mi raspundere ca informatiile declarate in prezentul chestionar sunt exacte.

Declar ca personalul angajat care are/va avea acces la informatii secrete de stat a luat la cunostinta de prevederile legale referitoare la protectia informatiilor secrete de stat si ma angajez ca le voi respecta.
Am cunostinta de faptul ca, daca, prin imprudenta si/sau neglijenta noastra, o informatie, un procedeu sau un fisier al carui depozitar suntem si care are un nivel de clasificare, va fi distrus, deturnat, sustras, reprodus sau adus la cunostinta fie publicului, fie unei persoane neautorizate, cei vinovati vor suporta consecintele potrivit legislatiei in vigoare.

Data ..... Semnatura .....

ANEXA Nr. 26

Secret de serviciu
(dupa completare)

(SE COMPLETEAZA NUMAI PENTRU ELIBERAREA
CERTIFICATULUI DE SECURITATE INDUSTRIALA
DE NIVEL "SECRET")

CHESTIONAR
de securitate industriala

Autorizare pentru nivelul de securitate:
[ ] SECRET

1. AGENTUL ECONOMIC SOLICITANT

Denumirea completa:

Nr. din Registrul Comertului:

Data ultimei actualizari la Registrul Comertului:

Denumiri anterioare (daca este cazul):

Cod Fiscal: Cod SIRUES:

Stare Firma

Adresa completa pentru sediul social:
Str. ..... nr. .....
Sectorul/judetul ..... localitatea .....
Nr. telefon ..... fax: .....
Telex ..... e-mail .....
Adresa site Internet .....
Cod postal (Casuta postala, daca este cazul): .....

Adrese anterioare (daca este cazul):

Statutul juridic:

Forma de proprietate:

Capitalul
- Capitalul social: .....
- Data ultimei modificari a capitalului social: .....
- Capitalul subscris varsat: .....
- Capital disponibil: .....
- Nr. actiuni/parti sociale: ..... Valoarea unei actiuni/parti sociale: .....
- Actiune nominativa. Exista? [ ] Da [ ] Nu
- Autoritatea/persoana care o detine .....
- Adresa site Internet .....
- Crestere preconizata ..... la data de: .....
- Organigrama societatii (se ataseaza la chestionar)

Actionari persoane fizice (care detin peste 5% din capitalul social)
- Numar .....
- 1. Nume, prenume .....
  - Data si locul nasterii .....
  - Nr. si seria actului de identitate .....
  - Adresa completa:

| Str. ..... nr. ..... |
| Sectorul/judetul ..... localitatea ..... |
| Nr. telefon ..... fax: ..... |
| Telex ..... e-mail ..... |
| Adresa site Internet ..... |
| Cod postal (Casuta postala, daca este cazul): ..... |
| Tara ..... |
| Procentul de actiuni/parti sociale detinut ____% incepand cu anul: ..... |
| ..... |
| (In cazul in care sunt mai multi, se pot prezenta in anexa dupa prezentul model) |

| Actionari persoane juridice: |
| ..... |
| ..... |

| Agenti economici la care firma solicitanta este actionar |
| Numarul de agenti economici: ..... |
| |
| Ce reprezinta pentru dvs.? |
| [ ] Furnizor |
| [ ] Client |
| [ ] Altceva |
| Procentul de actiuni/parti sociale detinut __% incepand cu anul: ..... |

| Firmele la care persoane din consiliul de administratie sunt actionari: |
| 1. Numele si prenumele persoanei: |
| Denumirea completa a firmei: |
| Nr. din Registrul Comertului |

2. AUTORIZAREA DEJA OBTINUTA

| Autorizatie: [ ] Da [ ] Nu |
| |
| Numarul si seria autorizatiei de securitate: |
| ..... |
| |
| Valabila de la: ..... la ..... |
| |
| Autoritatea emitenta: ..... |

3. CONDUCEREA INTREPRINDERII SI FUNCTIONARUL/STRUCTURA DE SECURITATE RESPONSABIL/RESPONSABILA

| Director general |
| Nume si prenume: ..... |
| Prenumele tatalui ..... |
| Data numirii in functie: ..... |
| Pregatire profesionala ..... |
| Data nasterii: ..... locul: ..... tara ..... |
| Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar (denumire, adresa completa) |

| Director economic |
| Nume si prenume: ..... |
| Prenumele tatalui ..... |
| Data numirii in functie ..... |
| Pregatire profesionala ..... |
| Data nasterii: ..... locul: ..... tara ..... |
| Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar (denumire, adresa completa) |

| Director stiintific/tehnic/comercial |
| Nume si prenume: ..... |
| Prenumele tatalui ..... |
| Data numirii in functie: ..... |
| Pregatire profesionala ..... |
| Data nasterii: ..... locul: ..... tara ..... |
| Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar |
| Membrii Consiliului de Administratie |
| 1. Nume si prenume: ..... |

| Prenumele tatalui ..... |
| Data numirii in functie ..... |
| Pregatire profesionala ..... |
| Data nasterii: ..... locul: ..... tara ..... |
| Firme la care este D actionar, D in conducere, D proprietar |
| (denumire, adresa completa): a) |
| b) |
| c) .... |
| 2. |
| 3. |
| 4. |
| 5. |
| 6. |

Functionarul/Structura de securitate responsabil/responsabila cu protectia informatiilor secrete de stat din intreprinderea solicitanta:
Nume si prenume: .....
Prenumele tatalui .....
Functia: .....
Pregatire profesionala .....
Data nasterii: ..... locul: ..... tara .....
Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar
(denumire, adresa completa)
(Datele de la aceasta rubrica se vor completa de catre toate persoanele din structura de securitate a agentului economic.)

4. DATE DESPRE PROFILUL SI ACTIVITATEA DESFASURATA

Obiectul(ele) principal(e) de activitate:
Numar de angajati permanent:
Intreprinderea dvs. este distribuitorul autorizat al altor agenti economici? (situatia in ultimii 5 ani)
[ ] Da [ ] Nu
Numele si adresa completa (daca este cazul)
Marci inregistrate
Nume si descriere (ce reprezinta)
Carui tip de clienti se adreseaza activitatea/serviciile/produsele dvs.?

5. BONITATE SI GARANTII BANCARE

Banci cu care lucrati (se vor completa urmatoarele informatii pentru fiecare banca):
Denumire: .....
Adresa completa:
Str. ..... nr. .....
Sectorul/judetul ..... localitatea .....
Nr. telefon ..... fax: .....
Telex ..... e-mail .....
Adresa site Internet .....
Numar cont: .....
Data deschiderii contului: .....
Creditul este: [ ] garantat [ ] negarantat
Marimea creditului: .....
Mijloace de plata la cumparare
[ ] acreditiv [ ] ordin de plata [ ] transfer bancar [ ] conditii speciale
[ ] Altele: .....
Exista reclamatii impotriva firmei pentru platile cu furnizorii sau clientii?
[ ] Da [ ] Nu
Daca DA:

Numarul reclamatiilor:
Data inregistrarii:
.....
.....
Pentru suma de (valoarea fiecarei plati contestate):
Reclamatia a fost rezolvata? [ ] Da [ ] Nu
Alte comentarii legate de aceasta:

6. SCURT RAPORT PENTRU ULTIMII 3 ANI DE EXERCITIU FINANCIAR

Sfarsit perioada financiara				
Active fixe - TOTAL				
Conturi in lei:				
Conturi in valuta:				
Creante:				
Stocuri:				
Active circulante - TOTAL:				
Capital social:				
Capital varsat:				
Imprumuturi pe termen lung:				
Imprumuturi pe termen scurt				
Furnizori si conturi asimilate:				
Datorii - TOTAL				
Total pasiv:				
Cifra de afaceri:				
Total venituri				
Total cheltuieli:				
Profit brut:				
Pierderi (unde este cazul):				
Venituri din export				
Trezoreria neta:				

7. INFORMATII DE SECURITATE

	DA	NU
Considerati ca firma dumneavoastra a atras atentia unui serviciu de informatii sau de securitate strain?		
Au existat cazuri cand au fost solicitate informatii cu caracter sensibil in afara atributiilor de serviciu?		
Intreprinderea sau vreunul dintre angajati a fost implicat(a) sau a sprijinit activitati de:		
- spionaj		

- terorism		
- sabotaj?		
Ati avut vreodata angajati care au sprijinit sau au fost implicati in una dintre activitatile de mai sus?		
Aveti cunostinta de orice alte imprejurari, conditii (factori de risc), nedeclarate in raspunsurile precedente, care au putut influenta activitatea dvs. sau a personalului din subordine, cum ar fi: obisnuinta utilizarii unor substante psihotrope, dependenta de alcool, dificultati financiare deosebite?		

8. DATE REFERITOARE LA SISTEMUL DE PROTECTIE A INFORMATIILOR SECRETE DE STAT

8.1. PROTECTIA INFORMATIILOR

8.1.1. LOCUL/LOCURILE UNDE SE CONCENTREAZA DATE SI INFORMATII SECRETE DE STAT

	DA	NU
- incapere destinata numai protectiei informatiilor		
- incapere destinata numai sistemului/subsistemului de calcul destinat preluarii, prelucrarii, stocarii si transmisiei datelor si informatiilor secrete de stat		
- incaperile sunt prevazute cu:		
- pereti antifonati		
- usi si incuietori speciale		
- podele si tavane speciale pentru zone sensibile		
- alte locuri unde se concentreaza date si informatii sau se desfasoara activitati cu caracter secret de stat		

In legatura cu acestea se vor face precizari privind pozitia fata de punctul de acces si control, imprejurimi, garantiile ce le prezinta in asigurarea protectiei datelor si informatiilor ori activitatilor secrete de stat.

.....

.....

8.1.2. MASURI DE PROTECTIE FIZICA A INCAPERILOR SAU LOCURILOR UNDE SE PASTREAZA SAU SE CONCENTREAZA DATE SI INFORMATII SECRETE DE STAT ORI ACTIVITATI CU CARACTER SECRET DE STAT

	DA	NU
Zone de securitate existente:		
> Zona de securitate clasa a II-a (pentru gestionarea informatiilor pana la nivelul SECRET, cu acces neautorizat conform prevederilor interne, cu escorta sau prin controale specifice)		
- perimetrul este clar definit si protejat, avand toate intrarile si iesirile controlate		
- accesul persoanelor neautorizate este permis conform prevederilor interne, cu escorta sau prin controale specifice		
> Zona administrativa (pentru manipularea si depozitarea informatiilor SECRETE DE SERVICIU)		
- perimetrul ofera posibilitatea de control al personalului si/sau al vehiculelor		
- sunt utilizate:		

• registre si jurnale speciale pentru corespondenta, evidenta, transport etc.		
• mape speciale de pastrare		
• sigilii		
• fise de predare-primire		
• ecusoane de acces		
• mobila de birou adecvata zonei administrative		
8.1.3. PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC SI DE TELECOMUNICATII DESTINAT PRELUARII, PRELUCRARII, STOCARII SI TRANSMISIEI DE DATE SI INFORMATII SECRETE DE STAT		
Echipament de comunicatie si de birotica existent (telefoane, fax, telex, xerox)		
- in zona de securitate clasa I		
- in zona de securitate clasa a II-a		
Echipament informatic		
- aveti acces la Internet		
- este utilizat un sistem de securizare		
• pe server-ul principal		
• la nivel de utilizator		
8.1.4. MASURI PROCEDURALE DE PROTECTIE A INFORMATIILOR SECRETE DE STAT SAU A ACTIVITATILOR CU CARACTER SECRET DE STAT		
Aveti elaborate proceduri privind:		
- clasificarea informatiilor dupa niveluri de securitate		
- accesul pentru personalul propriu		
- accesul pentru personalul din afara, inclusiv straini si reprezentanti ai mass-media		
- multiplicarea, transportul si circulatia documentelor in interiorul si in afara institutiei, atat in timpul, cat si in afara programului de lucru		
- protectia sistemului/subsistemului informatic si de telecomunicatii		
- controlul intern, activitatea de analiza si evaluare a modului in care se respecta prevederile legale in vigoare, din care sa reiasa periodicitatea controalelor, cine le executa, documentele ce se intocmesc si cum se valorifica, raspunderi si sanctiuni		
- instruirea personalului autorizat a avea acces		

8.2. PROTECTIA PERSONALULUI

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZA SA AIBA ACCES LA INFORMATII SECRETE DE STAT							

NR. CRT.	NUME, PRENUME PARINTI	PRENUME	DATA, LOC NASTERE	PROFESIE, FUNCTIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVATII**)

**) Se va inscrie ca mentiune daca are/urmeaza sa aiba acces si orice alte observatii considerate necesare.

9. DATE CU PRIVIRE LA PROCESE PENALE SAU CONTRAVENTII CA URMARE A INCALCARII LEGILOR

	DA	NU
In ultimii 10 ani a fost declansata impotriva intreprinderii dvs. o actiune in justitie?		
In caz de raspuns afirmativ, precizati cand, de ce, denumirea instantei judecatoresti, sentinta, pedeapsa si perioada de executare.		
In ultimii 5 ani intreprinderea pe care o conduceti a fost acuzata de incalcarea legii?		
In caz de raspuns afirmativ, aratati cand, cum, de ce, autoritatea care a constatat fapta si cuantumul amenzii.		

Orice schimbare referitoare la datele cuprinse in chestionar se transmite imediat sub forma de completare la chestionar.

Functia, numele, prenumele si semnatura conducatorului unitatii solicitante .....
Stampila unitatii solicitante .....
Localitatea si data completarii chestionarului .....

ANGAJAMENT

Subsemnatul(a) .....
(numele, initiala tatalui, prenumele - cu majuscule)
in calitate de ..... la .....
(functia) (denumirea completa a institutiei/agentului economic)
cu sediul in .....
(adresa completa)
certific pe propria-mi raspundere ca informatiile declarate in prezentul chestionar sunt exacte.
Declar ca personalul angajat care are/va avea acces la informatii secrete de stat a luat la cunostinta de prevederile legale referitoare la protectia informatiilor secrete de stat si ma angajez ca le voi respecta.
Am cunostinta de faptul ca, daca, prin imprudenta si/sau neglijenta noastra, o informatie, un procedeu sau un fisier al carui depozitar suntem si care are un nivel de clasificare va fi distrus, deturnat, sustras, reprodus sau adus la cunostinta fie publicului, fie unei persoane neautorizate, cei vinovati vor suporta consecintele potrivit legislatiei in vigoare.

Data ..... Semnatura .....

ANEXA Nr. 27

Secret de serviciu
(dupa completare)

(SE COMPLETEAZA NUMAI PENTRU ELIBERAREA CERTIFICATULUI DE SECURITATE INDUSTRIALA DE NIVEL "STRICT SECRET" si "STRICT SECRET DE IMPORTANTA DEOSEBITA")
Observatie! Pentru nivelul "STRICT SECRET DE IMPORTANTA DEOSEBITA" se completeaza si rubricile cu "*".

CHESTIONAR
de securitate industriala

Autorizare pentru nivelul de securitate:
[ ] STRICT SECRET
* [ ] STRICT SECRET DE IMPORTANTA DEOSEBITA

1. AGENTUL ECONOMIC SOLICITANT

|Denumire completa: |
| |
+--+
|Nr. din Registrul Comertului: |
+--+
|Data ultimei actualizari la Registrul Comertului: |
+--+
|Denumiri anterioare (daca este cazul): |
| |
+--+
|Cod fiscal: Cod SIRUES: |
+--+
|Stare Firma |
+--+
|Adresa completa pentru sediul social: |
|Str. ..... nr. ..... |
|Sectorul/judetul ..... localitatea ..... |
|Nr. telefon ..... fax: ..... |
|Telex ..... e-mail ..... |
|Adresa site Internet ..... |
|Cod postal (casuta postala, daca este cazul): ..... |
+--+
|Adrese anterioare (daca este cazul): |
| |
+--+
|Statutul juridic |
| |
+--+
|Forma de proprietate: |
| |
+--+
|Capitalul |
| Capitalul social: ..... |
| Data ultimei modificari a capitalului social: ..... |
| Capitalul subscris varsat: ..... |
| Capital disponibil ..... |
| Nr. actiuni/parti sociale: ..... Valoarea unei actiuni/parti sociale: .... |
| Actiune nominativa. Exista?   [ ]   Da   [ ]   Nu |
| Autoritatea/persoana care o detine ..... |
| Adresa site Internet ..... |
| Crestere preconizata ..... la data de: ..... |
| Organigrama societatii (se ataseaza la chestionar) |
+--+
|Asociati persoane fizice (care detin peste 5% din capitalul social) |
| Numar ..... |
| 1. Nume, prenume ..... |
| Data si locul nasterii ..... |
| Nr. si seria actului de identitate ..... |
| Adresa completa: |
| Str. ..... nr. ..... |
| Sectorul/judetul ..... localitatea ..... |
| Nr. telefon ..... fax: ..... |
| Telex ..... e-mail ..... |
| Adresa site Internet ..... |
| Cod postal (casuta postala, daca este cazul): ..... |
| Tara ..... |
| Procentul de actiuni/parti sociale detinut ___ % incepand cu anul: .... |
| (In cazul in care sunt mai multi, se pot prezenta in anexa, dupa prezentul |
| model.) |
+--+
|Asociati persoane juridice |
| Se completeaza un chestionar identic cu cel al agentului economic |
|solicitant, pana la capitolul 7 inclusiv, de catre actionarii care nu detin |
|autorizatie/certificat de securitate. |
+--+
|* Agenti economici la care firma solicitanta este asociata |
|Numarul de agenti economici: .....|
|Pentru fiecare agent economic se vor completa urmatoarele date: |
| Denumirea: ..... |
| Adresa completa: |
| Str. ..... nr. ..... |
| Sectorul/judetul ..... localitatea ..... |
| Nr. telefon ..... fax: ..... |
| Telex ..... e-mail ..... |
| Adresa site Internet ..... |
| Cod postal (casuta postala, daca este cazul): ..... |
| Tara ..... |
+--+
| Ce reprezinta pentru dvs.? |
| [ ] Furnizor |
| [ ] Client |
| [ ] Altceva |
|Procentul de actiuni/parti sociale detinut ___% incepand cu anul: ..... |
+--+
|* Firmele la care persoane din consiliul de administratie sunt actionari |
| 1. Numele si prenumele persoanei: |
| Denumirea completa a firmei: |
| Nr. din Registrul Comertului |
+--+

2. NIVELUL DE AUTORIZARE DEJA OBTINUT

+--+
|Autorizatie/Certificat obtinut   [ ]   Da   [ ]   Nu |
| |
|Nivelul de acces al certificatului detinut: |
| [ ] |
| |
|Seria si numarul autorizatiei/certificatului de securitate: |
|..... |
|Valabil de la: ..... la ..... |
|Autoritatea emitenta: ..... |
+--+

3. CONDUCEREA INTREPRINDERII SI FUNCTIONARUL/STRUCTURA DE SECURITATE

+--+
|Director general |
| Nume si prenume: ..... |
| Prenumele tatalui ..... |
| Data numirii in functie: ..... |

| Pregatire profesionala ..... |
| Data nasterii: ..... locul: ..... tara ..... |
| Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar |
| (denumire, adresa completa) |

|Director economic |
| Nume si prenume: ..... |
| Prenumele tatalui ..... |
| Data numirii in functie ..... |
| Pregatire profesionala ..... |
| Data nasterii: ..... locul: ..... tara ..... |
| Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar |
| (denumire, adresa completa) |

|Director stiintific/tehnic/comercial |
| Nume si prenume: ..... |
| Prenumele tatalui ..... |
| Data numirii in functia: ..... |
| Pregatire profesionala ..... |
| Data nasterii: ..... locul: ..... tara ..... |
| Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar |
| (denumire, adresa completa) |

|Membrii consiliului de administratie |
| 1. Nume si prenume: ..... |
| Prenumele tatalui ..... |
| Data numirii in functie ..... |
| Pregatire profesionala ..... |
| Data nasterii: ..... locul:..... tara ..... |
| Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar |
| (denumire, adresa completa): a) |
| b) |
| c)... |
| 2. |
| 3. |
| 4. |
| 5. |
| 6. |

|Functionarul/Structura de securitate responsabil/responsabila cu protectia |
|informatiilor clasificate din institutia solicitanta: |
| Nume si prenume: ..... |
| Prenumele tatalui ..... |
| Functia: ..... |
| Pregatire profesionala ..... |
| Data nasterii: ..... locul: ..... tara ..... |
| Firme la care este [ ] actionar, [ ] in conducere, [ ] proprietar |
| (denumire, adresa completa) |
|(Datele de la aceasta rubrica se vor completa de catre toate persoanele din |
|structura de securitate a agentului economic.) |

* 4. SUCURSALE, FILIALE SAU PUNCTE DE LUCRU

|* Denumire completa: |

|Denumiri anterioare (daca este cazul): | Datele schimbarilor |
| | |

|* Adresa completa: |
|Str. ..... nr. ..... |
|Sectorul/judetul ..... localitatea ..... |
|Nr. telefon ..... fax: ..... |
|Telex ..... e-mail ..... |
|Adresa site Internet..... |
|Cod postal (casuta postala, daca este cazul): ..... |
|Tara ..... |

|Adrese anterioare (daca este cazul): |

| * Forma de detinere a spatiului: | [ ] proprietate Numarul actului si forma juridica: | [ ] inchiriata De la (denumire, adresa completa): |
| | | |

|* Agentul economic detine: |
|[ ] birouri [ ] magazine [ ] hoteluri [ ] fabrici [ ] depozite |
|[ ] ateliere [ ] laboratoare [ ] santiere [ ] spatii de prezentare |
|[ ] camere securizate Altele: |

|* Descrierea amplasamentului sediului: |
|[ ] zona comerciala centrala [ ] zona comerciala periferica [ ] zona rurala |
|[ ] zona industriala [ ] incinta comerciala |
|[ ] zona rezidentiala |

|* Spatii subinchiriate altor agenti economici, cu specificarea denumirii si |
|obiectului lor de activitate: |

5. DATE DESPRE PROFILUL SI ACTIVITATEA DESFASURATA

|Obiectul(ele) principal(e) de activitate: |

|Numar de angajati permanent: |
| Cu studii superioare: |
| Cu studii medii: |
| Personal auxiliar: |

|Numar de colaboratori |
| Persoane fizice ..... |
| Persoane juridice ..... |
| |

|* Vanzari la intern (situatia in ultimii 5 ani) |
| Procentul din vanzarile totale ..... |
| Termenele de livrare (in zile) ..... |
| Conditii de plata (numerar, cec, ordin de plata, cont curent etc.) |
| ..... |

|* Importuri (situatia in ultimii 5 ani) |

| Procentul importurilor la realizarea produselor ..... |
| Ce se importa (materie prima si/sau ansamble, subansamble, produse |
| finite) ..... |
| Tarile de unde se importa: ..... |
| ..... |
| ..... |
| Termene de import (in zile) ..... |
| Conditii de plata (numerar, cec, ordin de plata, cont curent etc.) |
| ..... |

|* Exporturi (situatia in ultimii 5 ani) |
| Procent din activitate reprezentat de importuri: ..... |
| Ce se exporta (materie prima si/sau ansamble, subansamble, produse |
| finite) ..... |
| Tarile in care se exporta: ..... |
| ..... |
| ..... |
| Termene de export (in zile) ..... |
| Conditii de plata (numerar, cec, ordin de plata, cont curent etc.) |
| ..... |

|Institutia dvs. este distribuitorul autorizat al altor agenti economici? |
|(situatia in ultimii 5 ani) |
| [ ] Da [ ] Nu |
| Numele si adresa completa (daca este cazul) |
| |

|Marci inregistrate |
| Nume si descriere (ce reprezinta) |
| |

|Caror tip de clienti se adreseaza activitatea/serviciile/produsele dvs.? |
| |

* Principalii clienti cu care institutia dvs. are contract (denumire, adresa completa)	Valoarea fiecarui contract	Perioada

6. BONITATE SI GARANTII BANCARE

|Banci cu care lucrati (se vor completa urmatoarele informatii pentru fiecare banca): |
| Denumire: ..... |
| Adresa completa: |
| Str. ..... nr. ..... |
| Sectorul/judetul ..... localitate ..... |
| Nr. telefon ..... fax: ..... |
| Telex ..... e-mail ..... |
| Adresa site Internet ..... |
| Numar cont: ..... |
| Data deschiderii contului: ..... |
| Creditul este: [ ] garantat [ ] negarantat |
| Marimea creditului: ..... |
| Natura garantiei (daca este credit "garantat"): |
| |
| |
| * Creditul este utilizat in totalitate? [ ] Da [ ] Nu |
| * Banca a acordat facilitatea de neacoperire a contului? [ ] Da [ ] Nu |
| * Daca DA, pana la ce suma poate merge neacoperirea: ..... |
| * Daca DA, aceasta facilitate este folosita? [ ] Da [ ] Nu |

|Mijloace de plata la cumparare |
| [ ] acreditiv [ ] ordin de plata [ ] transfer bancar |
| [ ] conditii speciale |
| [ ] Altele: ..... |

|Exista reclamatii impotriva firmei? |
| [ ] Da [ ] Nu |
| Daca DA: |
| Numarul reclamatiilor: ..... |
| Data inregistrarii: |
| ..... |
| ..... |
| Pentru suma de (valoarea fiecarei plati contestate): |
| Reclamatia a fost rezolvata: [ ] Da [ ] Nu |
| Alte comentarii legate de aceasta: |
| |
| |
| |

|* Planuri viitoare (noi investitii, patrundere pe noi piete etc.) |
| |
| |

7. SCURT RAPORT PENTRU ULTIMII 3 ANI DE EXERCITIU FINANCIAR

Sfarsit perioada financiara			
Active fixe - TOTAL			
Conturi in lei:			
Conturi in valuta:			
Creante:			
Stocuri:			
Active circulante - TOTAL:			
Total active:			
Capital social:			
Capital varsat:			

Capitaluri proprii:			
Imprumuturi pe termen lung:			
Imprumuturi pe termen scurt			
Furnizori si conturi asimilate:			
Datorii - TOTAL			
Total pasiv:			
Cifra de afaceri:			
Total venituri			
Total cheltuieli:			
Profit brut:			
Pierderi (unde este cazul):			
Venituri din export			
Trezoreria neta:			

8. INFORMATII DE SECURITATE

	DA	NU
Considerati ca firma dumneavoastra a atras atentia unui serviciu de informatii sau de securitate strain?		
Credeti ca au fost facute presiuni asupra firmei sau angajatilor ca urmare a unui incident survenit pe teritoriul altei tari?		
Sunt mentinute relatii permanente, profesionale, personale cu cetateni straini? Natura acestora.		
Au existat cazuri cand au fost solicitate informatii cu caracter sensibil in afara atributiilor de serviciu?		
Intreprinderea sau vreunul din angajati a fost implicat(a) sau a sprijinit activitati de:		
- spionaj		
- terorism		
- sabotaj?		
Ati avut vreodata angajati care au sprijinit sau au fost implicati intr-una dintre activitatile de mai sus?		
Aveti cunostinta de orice alte imprejurari, conditii (factori de risc), nedeclarate in raspunsurile precedente, care au putut influenta activitatea dvs. sau a personalului din subordine, cum ar fi: obisnuinta utilizarii unor substante psihotrope, dependenta de alcool, dificultati financiare deosebite?		

9. DATE REFERITOARE LA SISTEMUL DE PROTECTIE A INFORMATIILOR SECRETE DE STAT

9.1. PROTECTIA INFORMATIILOR

9.1.1. LOCUL/LOCURILE UNDE SE CONCENTREAZA DATE si INFORMATII SECRETE DE STAT	DA	NU
- incapere destinata numai protectiei informatiilor secrete de stat		
- incapere destinata numai sistemului/subsistemului de calcul destinat preluarii, prelucrarii, stocarii si transmisiei datelor si informatiilor secrete de stat		
- incaperile sunt prevazute cu:		
- pereti antifonati		
- usi si incuietori speciale		
- podele si tavane speciale pentru zone sensibile		
- alte locuri unde se concentreaza date si informatii sau se desfasoara activitati cu caracter secret de stat		

In legatura cu acestea se vor face precizari privind pozitia fata de punctul de acces si control, imprejurimi, garantiile ce le prezinta in asigurarea protectiei datelor si informatiilor ori activitatilor secrete de stat

.....

.....

.....

9.1.2. MASURI DE PROTECTIE FIZICA A INCAPERILOR SAU LOCURILOR UNDE SE PASTREAZA SAU SE CONCENTREAZA DATE SI INFORMATII SECRETE DE STAT ORI ACTIVITATI CU CARACTER SECRET DE STAT	DA	NU
Zone de securitate existente:		
> Zona de securitate clasa I (pentru gestionarea informatiilor pana la nivelul STRICT SECRET DE IMPORTANTA DEOSEBITA, cu acces autorizat)		
- perimetrul este clar definit si protejat, avand toate intrarile si iesirile controlate		

- este marcata zona, specificarea restrictiei si mentionarea zonei de securitate		
- exista control al sistemului de intrare, care sa permita doar accesul persoanelor autorizate pentru intrarea in zona		
(Daca DA, descrieti sistemul(ele) de protectie mecanica, electrica, electronica, informationala, optica, acustica etc.)		
- sistemul de protectie utilizat este omologat si/sau aprobat de un serviciu specializat		
(Daca DA, mentionati care.)		
> Zona de securitate clasa a II-a (pentru gestionarea informatiilor pana la nivelul SECRET, cu acces neautorizat conform prevederilor interne, cu escorta sau prin controale specifice)		
- perimetrul este clar definit si protejat, avand toate intrarile si iesirile controlate		
- accesul persoanelor neautorizate este permis conform prevederilor interne, cu escorta sau prin controale specifice		
> Zona administrativa (pentru manipularea si depozitarea informatiilor SECRETE DE SERVICIU)		
- perimetrul ofera posibilitatea de control a personalului si/sau vehiculelor		
- sunt utilizate:		
• registre si jurnale speciale pentru corespondenta, evidenta, transport etc.		
• mape speciale de pastrare		
• sigilii		
• fise de predare-primire		
• ecusoane de acces		
• mobila de birou adecvata zonei administrative		
9.1.3. PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC si DE TELECOMUNICATII DESTINAT PRELUARII, PRELUCRARII, STOCARII SI TRANSMISIEI DE DATE SI INFORMATII SECRETE DE STAT		
Echipament de comunicatie si de birotica existent (telefoane, fax, telex, xerox)		
- in zona de securitate clasa I		
- in zona de securitate clasa a II-a		
Echipament informatic		
- numar calculatoare		
- utilizati calculatoarele in retea Intranet		
- aveti acces la Internet		
- este utilizat un sistem de securizare		
• pe server-ul principal		
• la nivel de utilizator		
* Mentionati tipul server-ului principal si distribuitorul, administratorul (in cazul in care este o firma specializata care asigura servicii), precum si locul/locurile unde sunt amplasate calculatoarele conectate in retea la server-ul care stocheaza informatii clasificate		
9.1.4. MASURI PROCEDURALE DE PROTECTIE A INFORMATIILOR SECRETE DE STAT SAU A ACTIVITATILOR CU CARACTER SECRET DE STAT		
Aveti elaborate proceduri privind:		
- clasificarea informatiilor dupa niveluri de securitate		
- accesul pentru personalul propriu		
- accesul pentru personalul din afara, inclusiv straini si reprezentanti ai mass-media		
- multiplicarea, transportul si circulatia documentelor in interiorul si in afara intreprinderii, atat in timpul cat si in afara programului de lucru		
- protectia sistemului/subsistemului informatic si de telecomunicatii		
- controlul intern, activitatea de analiza si evaluare a modului in care se respecta prevederile legale in vigoare, din care sa reiasa periodicitatea controalelor, cine le executa, documentele ce se intocmesc si cum se valorifica, raspunderi si sanctiuni		

- instruirea personalului autorizat a avea acces		

9.2. PROTECTIA PERSONALULUI

9.2.1. LISTA PERSOANELOR CARE AU ACCES SAU URMEAZA SA AIBA ACCES LA INFORMATII SECRETE DE STAT							
NR. CRT.	NUME, PRENUME PARINTI	PRENUME	DATA, LOC NASTERE	PROFESIE, FUNCTIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVATII **)

**) Se va inscrie ca mentiune daca are/urmeaza sa aiba acces si orice alte observatii considerate necesare.

9.2.2. LISTA PERSOANELOR AUTORIZATE SA ADMINISTREZE SISTEMUL/SUBSISTEMUL INFORMATIC SI DE TELECOMUNICATII, PRECUM SI CEI CARE LUCREAZA IN RETEAUA INTRANET cu ACCES LA INFORMATII SECRETE DE STAT							
NR. CRT.	NUME, PRENUME PARINTI	PRENUME	DATA, LOC NASTERE	PROFESIE, FUNCTIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVATII **)

**) Se va inscrie echipamentul pe care-l administreaza sau faptul ca are acces Intranet.

10. DATE CU PRIVIRE LA PROCESE PENALE SAU CONTRAVENTII CA URMARE A INCALCARII LEGILOR

	DA	NU
In ultimii 10 ani a fost declansata impotriva intreprinderii dvs. o actiune in justitie?		
In caz de raspuns afirmativ precizati cand, de ce, denumirea instantei judecatoresti, sentinta, pedeapsa si perioada de executare.		
In ultimii 5 ani intreprinderea pe care o conduceti a fost acuzata de incalcarea legii?		
In caz de raspuns afirmativ aratati cand, cum, de ce, autoritatea care a constatat fapta si cuantumul amenzii.		

Orice schimbare referitoare la datele cuprinse in chestionar se transmite imediat sub forma de completare la chestionar.

Functia, numele, prenumele si semnatura conducatorului unitatii solicitante .....
Stampila unitatii solicitante .....
Localitatea si data completarii chestionarului .....

ANGAJAMENT([1])

Subsemnatul(a) .....
(numele, initiala tatalui, prenumele - cu majuscule)
in calitate de ..... la .....
(functia) (denumirea completa a institutiei/agentului economic)
cu sediul in .....
(adresa completa)

certific pe propria-mi raspundere ca informatiile declarate in prezentul chestionar sunt exacte.

Declar ca personalul angajat care are/va avea acces la informatii secrete de stat a luat la cunostinta de prevederile legale referitoare la protectia informatiilor secrete de stat si ma angajez ca le voi respecta.

Am cunostinta de faptul ca, daca, prin imprudenta si/sau neglijenta noastra, o informatie, un procedeu sau un fisier al carui depozitar suntem si care are un nivel de clasificare va fi distrus, deturnat, sustras, reprodus sau adus la cunostinta fie publicului, fie unei persoane neautorizate, cei vinovati vor suporta consecintele potrivit legislatiei in vigoare.

Data ..... Semnatura .....

([1]) Se completeaza atat pentru nivelul "STRICT SECRET", cat si pentru nivelul "STRICT SECRET DE IMPORTANTA DEOSEBITA".

ANEXA Nr. 28

ROMANIA
OFICIUL REGISTRULUI NATIONAL AL INFORMATIILOR SECRETE DE STAT

AUTORIZATIE DE SECURITATE INDUSTRIALA
Nr. _____ din _____

Oficiul Registrului National al Informatiilor Secrete de Stat autorizeaza

_____,
(denumirea completa a institutiei/agentului economic)

pentru participarea la proceduri de negociere a unui contract, in cadrul caruia sunt gestionate informatii clasificate.

Prezenta autorizatie este valabila pana la data de _____.

Directorul general al Oficiului Registrului National
al Informatiilor Secrete de Stat

_____

(semnatura, stampila)

ANEXA Nr. 29

ROMANIA
OFICIUL REGISTRULUI NATIONAL AL
INFORMATIILOR SECRETE DE STAT

CERTIFICAT DE SECURITATE INDUSTRIALA

Nr. _____ din _____

Oficiul Registrului National al Informatiilor Secrete de Stat certifica

_____

(denumirea completa a institutiei/agentului economic)

pentru derularea contractului in care sunt gestionate informatii secrete de stat de nivelul _____.

Prezentul certificat este valabil pe durata derularii contractului.

Directorul general al Oficiului Registrului National
al Informatiilor Secrete de Stat

_____

(semnatura, stampila)

ANEXA Nr. 30

ANTETUL INSTITUTIEI/AGENTULUI ECONOMIC

Adresa ..... Tel./Fax

Catre ORNISS

CERERE

pentru eliberarea certificatului de securitate industriala

Va rugam sa eliberati certificatul de securitate industriala nivel _____ pentru _____

(denumirea completa a institutiei/agentului economic)

cu sediul in _____

(adresa completa)

in vederea derularii contractului clasificat _____

Obiectul contractului este _____

_____

Beneficiarul este _____

_____

Mentionam ca in prezent intreprinderea noastra detine/nu detine autorizatie de securitate/certificat de securitate industriala pentru nivelul _____.

Anexam, in original, chestionarul de securitate industriala.

Directorul institutiei/agentului economic

_____

(semnatura, stampila)

ANEXA Nr. 31

ROMANIA
(Institutia)

Compartimentul _____

REGISTRUL

pentru evidenta autorizatiilor de securitate industriala

Nr.	Denumirea si adresa	Data eliberarii	Seria si numarul	Perioada de	Data	Motivul	Obs.

crt.	completa a obiectivului industrial	autorizatiei de securitate industriala	autorizatiei de securitate industriala	valabilitate	retragerii	retragerii	

ANEXA Nr. 32

ROMANIA
(Institutia)
_____
Compartimentul _____

REGISTRUL
pentru evidenta certificatelor de securitate industriala

Nr. crt.	Denumirea si adresa completa a obiectivului industrial	Nivelul de acces	Data eliberarii certificatului de securitate industriala	Seria si numarul certificatului de securitate industriala	Perioada de valabilitate	Data retragerii	Motivul retragerii	Obs.