

HOTĂRÂRE nr. 585 din 13 iunie 2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România

În temeiul prevederilor art. 107 din Constituția României, ale art. 6 alin. (1), art. 24 alin. (2), art. 30 și ale art. 42 din Legea nr. **182/2002** privind protecția informațiilor clasificate,

Guvernul României adoptă prezenta hotărâre.

Art. 1

Se aprobă Standardele naționale de protecție a informațiilor clasificate în România, prevăzute în anexa care face parte integrantă din prezenta hotărâre.

Art. 2

Autoritățile și instituțiile publice, agenții economici cu capital integral sau parțial de stat și celelalte persoane juridice de drept public sau privat care utilizează informații clasificate vor emite norme proprii în aplicarea prezentei hotărâri, în termen de 60 de zile de la publicarea acesteia în Monitorul Oficial al României, Partea I.

PRIM-MINISTRU

ADRIAN NĂSTASE

Contrasemnează:

Ministrul de interne,

Ioan Rus

p. Ministrul apărării naționale,

Sorin Encuțescu,

secretar de stat

Ministrul finanțelor publice,

Mihai Nicolae Tănăsescu

p. Ministrul afacerilor externe,

Cristian Diaconescu,

secretar de stat

Ministrul pentru coordonarea Secretariatului General al Guvernului,

Petru Șerban Mihăilescu

Directorul Serviciului Român de Informații,

Alexandru-Radu Timofte

Standarde naționale de protecție a informațiilor clasificate în România

Publicat în Monitorul Oficial cu numărul 485 din data de 5 iulie 2002

Standarde naționale din 13 iunie 2002 de protecție a informațiilor clasificate în România

CAPITOLUL I: DISPOZIȚII GENERALE

Art. 1

Standardele naționale de protecție a informațiilor clasificate în România cuprind normele de aplicare a Legii nr. **182/2002** privind protecția informațiilor clasificate referitoare la:

- a) clasificările informațiilor secrete de stat și normele privind măsurile minime de protecție în cadrul fiecărei clase;
- b) obligațiile și răspunderile autorităților și instituțiilor publice, ale agenților economici și ale altor persoane juridice de drept public sau privat privind protecția informațiilor secrete de stat;
- c) normele privind accesul la informațiile clasificate, precum și procedura verificărilor de securitate;
- d) regulile generale privind evidența, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea și distrugerea informațiilor secrete de stat;
- e) regulile de identificare și marcarea, inscripționările și mențiunile obligatorii pe documentele secrete de stat, în funcție de nivelurile de secretizare, cerințele de evidență a numerelor de exemplare și a destinatarilor, termenele și regimul de păstrare, interdicțiile de reproducere și circulație;
- f) condițiile de fotografiere, filmare, cartografiere și executare a unor lucrări de arte plastice în obiective sau locuri care prezintă importanță deosebită pentru protecția informațiilor secrete de stat;
- g) regulile privitoare la accesul străinilor la informațiile secrete de stat,
- h) protecția informațiilor clasificate care fac obiectul contractelor industriale secrete - securitatea industrială;
- i) protecția surselor generatoare de informații - INFOSEC.

Art. 2

(1) Prezentele standarde instituie sistemul național de protecție a informațiilor clasificate, în concordanță cu interesul național, cu criteriile și recomandările NATO și sunt obligatorii pentru toate persoanele juridice sau fizice care gestionează astfel de informații.

(2) Echivalența informațiilor naționale clasificate, pe niveluri de secretizare, cu informațiile NATO clasificate este:

- a) Strict secret de importanță deosebită - NATO top secret
- b) Strict secret - NATO secret
- c) Secret - NATO confidențial
- d) Secret de serviciu - NATO restricted

Art. 3

Termenii folosiți în prezentele standarde au următorul înțeles:

- Autoritate Desemnată de Securitate - ADS - instituție abilitată prin lege să stabilească, pentru domeniul său de activitate și responsabilitate, structuri și măsuri proprii privind coordonarea și

controlul activităților referitoare la protecția informațiilor secrete de stat. Sunt autoritați desemnate de securitate, potrivit legii: Ministerul Apărării Naționale, Ministerul de Interne, Ministerul Justiției, Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Proiecție și Pază, Serviciul de Telecomunicații Speciale;

- autorizație de acces la informații clasificate - document eliberat cu avizul instituțiilor abilitate, de conducătorul persoanei juridice deținătoare de astfel de informații, prin care se confirmă că, în exercitarea atribuțiilor profesionale, posesorul acestuia poate avea acces la informații secrete de stat de un anumit nivel de secretizare, potrivit principiului necesității de a cunoaște;
- autorizație de securitate industrială - document eliberat de Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS - unui obiectiv industrial, prin care se atestă că este abilitat să participe la procedura de negociere a unui contract clasificat;
- autorizație specială - document eliberat de către ORNISS prin care se atestă verificarea și acreditarea unei persoane de a desfășura activități de fotografiere, filmare, cartografiere și lucrări de arte plastice pe teritoriul României, în obiective, zone sau locuri care prezintă importanță deosebită pentru protecția informațiilor secrete de stat;
- aviz de securitate industrială - document eliberat de către ADS prin care se atestă că obiectivul industrial contractant a implementat toate măsurile de securitate necesare protecției informațiilor clasificate vehiculate în derularea contractului încheiat;
- certificat de securitate - document eliberat persoanei cu atribuții nemijlocite în domeniul protecției informațiilor clasificate, respectiv funcționarului de securitate sau salariatului din structura de securitate, care atestă verificarea și acreditarea de a deține, de a avea acces și de a lucra cu informații clasificate de un anumit nivel de secretizare;
- certificat de securitate industrială - document eliberat de ORNISS unui obiectiv industrial, prin care se atestă că este abilitat să deruleze activități industriale și/sau de cercetare ce presupun accesul la informații clasificate;
- clasificarea informațiilor - încadrarea informațiilor într-o clasă și nivel de secretizare,
- contract clasificat - orice contract încheiat între părți, în condițiile legii, în cadrul căruia se cuprind și se vehiculează informații clasificate;
- contractant unitate industrială, comercială, de execuție, de cercetare-proiectare sau prestatoare de servicii în cadrul unui contract clasificat;
- contractor - parte dintr-un contract clasificat, care are calitatea de beneficiar al lucrărilor sau serviciilor executate de contractant;
- controlul informațiilor clasificate - orice activitate de verificare a modului în care sunt gestionate documentele clasificate,
- declasificare - suprimarea mențiunilor de clasificare și scoaterea informației clasificate de sub incidența reglementărilor proiective prevăzute de lege;
- diseminarea informațiilor clasificate - activitatea de difuzare a informațiilor clasificate către unități sau persoane abilitate să aibă acces la astfel de informații;
- document clasificat - orice suport material care conține informații clasificate, în original sau copie, precum:
 - a) hârtie - documente olografe, dactilografiate sau tipărite, schițe, hărți, planșe, fotografii, desene, indigo, listing;
 - b) benzi magnetice, casete audio-video, microfilme;
 - c) medii de stocare a sistemelor informatici - dischete, compact-discuri, hard-discuri, memorii PROM și EPROM, riboane;
 - d) dispozitive de procesare portabile - agende electronice, laptop-uri - la care hard-discul este folosit pentru stocarea informațiilor;

- funcționar de securitate - persoană care îndeplinește atribuțiile de proiecție a informațiilor clasificate în cadrul autorităților, instituțiilor publice, agenților economici cu capital integral sau parțial de stat și altor persoane juridice de drept public sau privat;
- gestionarea informațiilor clasificate - orice activitate de elaborare, luare în evidență, accesare, procesare, multiplicare, manipulare, transport, transmitere, inventariere, păstrare, arhivare sau distrugere a informațiilor clasificate;
- incident de securitate - orice acțiune sau inacțiune contrară reglementărilor de securitate a cărei consecință a determinat sau este de natură să determine compromiterea informațiilor clasificate;
- indicator de interdicție - text sau simbol care semnalează interzicerea accesului sau derulării unor activități în zone, obiective, sectoare sau locuri care prezintă importanță deosebită pentru protecția informațiilor clasificate;
- informație clasificată compromisă - informație clasificată care și-a pierdut integritatea, a fost rătăcită, pierdută ori accesată, total sau parțial, de persoane neautorizate;
- instituție cu atribuții de coordonare a activității și de control al măsurilor privitoare la protecția informațiilor clasificate sau instituție abilită - Ministerul Apărării Naționale, Ministerul de Interne, Ministerul Justiției, Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Protecție și Pază, Serviciul de Telecomunicații Speciale, potrivit competențelor stabilite prin lege;
- marcare - activitatea de inscripționare a nivelului de secretizare a informației și de semnalare a cerințelor speciale de protecție a acesteia,
- material clasificat - document sau produs prelucrat ori în curs de prelucrare, care necesită a fi protejat împotriva cunoașterii neautorizate;
- necesitatea de a cunoaște - principiul conform căruia accesul la informații clasificate se acordă în mod individual numai persoanelor care, pentru îndeplinirea îndatoririlor de serviciu, trebuie să lucreze cu astfel de informații sau să aibă acces la acestea;
- negocieri - activitățile circumschise adjudecării unui contract sau subcontract, de la notificarea intenției de organizare a licitației, până la încheierea acesteia;
- obiectiv industrial - unitate de cercetare sau cu activitate de producție, care desfășoară activități științifice, tehnologice sau economice ce au legătură cu siguranța sau cu apărarea națională, ori prezintă importanță deosebită pentru interesele economice și tehnico-științifice ale României;
- obiectiv, sector sau loc de importanță deosebită pentru protecția informațiilor secrete de stat - incintă sau perimetru anume desemnat, în care sunt gestionate informații secrete de stat,
- parte contractantă - oricare dintre părțile care convin să negocieze, să încheie sau să deruleze un contract clasificat;
- protecția surselor generatoare de informații - ansamblul măsurilor destinate protecției informațiilor elaborate, stocate sau transmise prin sisteme ori rețele de prelucrare automată a datelor și/sau de comunicații;
- securitate industrială - sistemul de norme și măsuri care reglementează protecția informațiilor clasificate în domeniul activităților contractuale;
- sistem de protecție a informațiilor clasificate - ansamblul de măsuri de natură juridică, procedurală, fizică, de protecție a personalului și a surselor generatoare de informații, destinate securității materialelor și documentelor clasificate;
- structură de securitate - compartiment specializat în protecția informațiilor clasificate, organizat în cadrul autorităților, instituțiilor publice, agenților economici cu capital integral sau parțial de stat și al altor persoane juridice de drept public sau privat,

- subcontractant - parte care își asumă executarea unei părți a contractului clasificat sub coordonarea contractantului;
- trecerea la un alt nivel de clasificare sau de secretizare - schimbarea clasificării, respectiv a nivelului de secretizare a informațiilor secrete de stat;
- unitate deținătoare de informații clasificate sau unitate - autoritate sau instituție publică, agent economic cu capital integral sau parțial de stat ori o altă persoană juridică de drept public sau privat care, potrivit legii, are dreptul de a deține informații clasificate;
- verificare de securitate - totalitatea măsurilor întreprinse de autoritățile desemnate de securitate, conform competențelor, pentru stabilirea onestității și profesionalismului persoanelor, în scopul avizării eliberării certificatului de securitate sau autorizației de acces la informații clasificate;
- zonă de securitate - perimetru delimitat și special amenajat unde sunt gestionate informații clasificate.

CAPITOLUL II: CLASIFICAREA ȘI DECLASIFICAREA INFORMAȚIILOR. MĂSURI MINIME DE PROTECȚIE SPECIFICE CLASELOR ȘI NIVELURILOR DE SECRETIZARE

SECȚIUNEA 1: Clasificarea informațiilor

Art. 4

(1) Potrivit legii, informațiile sunt clasificate secrete de stat sau secrete de serviciu, în raport de importanță pe care o au pentru securitatea națională și de consecințele ce s-ar produce ca urmare a dezvăluirii sau diseminării lor neautorizate.

(2) Informațiile secrete de stat sunt informațiile a căror divulgare poate prejudicia siguranța națională și apărarea țării și care, în funcție de importanța valorilor protejate, se includ în următoarele niveluri de secretizare prevăzute de lege:

- a) strict secret de importanță deosebită;
- b) strict secret;
- c) secret.

(3) Informațiile a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat se clasifică secrete de serviciu.

Art. 5

(1) Autoritățile publice care elaborează ori lucrează cu informații secrete de stat au obligația să întocmească un ghid pe baza căruia se va realiza clasificarea corectă și uniformă a acestora.

(2) Ghidul prevăzut la alin. (1) se aprobă personal și în scris de către împăterniciții sau, după caz, funcționarii superiori abilitați să atribuie nivelurile de secretizare, conform legii.

Art. 6

Autoritățile și instituțiile publice întocmesc liste proprii cuprinzând categoriile de informații secrete de stat în domeniile lor de activitate, care se aprobă și se actualizează prin hotărâre a Guvernului.

Art. 7

Listele cu informații secrete de serviciu se stabilesc de conducătorii unităților deținătoare de astfel de informații.

Art. 8

În listelete cu informații secrete de serviciu vor fi incluse informațiile care se referă la activitatea unității și care, fără a constitui, în înțelesul legii, secrete de stat, nu trebuie cunoscute decât de persoanele cărora le sunt necesare pentru îndeplinirea atribuțiilor de serviciu, divulgarea lor putând prejudicia interesul unității

Art. 9

Unitățile care gestionează informații clasificate au obligația să analizeze ori de câte ori este necesar listelete informațiilor secrete de stat și, după caz, să prezinte Guvernului spre aprobare propunerile de actualizare și completare a acestora, conform legii.

Art. 10

Atribuirea clasei și nivelului de secretizare a informațiilor se realizează prin consultarea ghidului de clasificare, a listelor cu informații secrete de stat și a listelor cu informații secrete de serviciu, elaborate potrivit legii.

Art. 11

Şeful ierarhic al emitentului are obligația să verifice dacă informațiile au fost clasificate corect și să ia măsuri în consecință, când constată că au fost atribuite niveluri de secretizare necorespunzătoare.

Art. 12

(1) Termenele de clasificare a informațiilor secrete de stat vor fi stabilite de emitent, în funcție de importanța acestora și de consecințele care s-ar produce ca urmare a dezvăluirii sau diseminării lor neautorizate.

(2) Termenele de clasificare a informațiilor secrete de stat, pe niveluri de secretizare, cu excepția cazului când acestea necesită o protecție mai îndelungată, sunt de până la:

- 100 de ani pentru informațiile clasificate strict secret de importanță deosebită;
- 50 de ani pentru informațiile clasificate strict secret;
- 30 de ani pentru informațiile clasificate secret.

(3) Termenele prevăzute la alin. (2) pot fi prelungite prin hotărâre a Guvernului, pe baza unei motivații temeinice, la solicitarea conducerilor unităților deținătoare de informații clasificate sau, după caz, a împuternicitorilor și funcționarilor superiori abilități să atribuie nivelurile de secretizare.

Art. 13

Fiecare împuternicit ori funcționar superior abilitat să atribuie niveluri de secretizare va dispune verificarea periodică a tuturor informațiilor secrete de stat cărora le-au atribuit nivelurile de secretizare, prilej cu care, dacă este necesar, vor fi reevaluate nivelurile și termenele de clasificare.

14

(1) Documentul elaborat pe baza prelucrării informațiilor cu niveluri de secretizare diferite va fi clasificat conform noului conținut, care poate fi superior originalelor.

(2) Documentul rezultat din cumularea neprelucrată a unor extrase provenite din informații clasificate va primi clasa sau nivelul de secretizare corespunzător conținutului extrasului cu cel mai înalt nivel de secretizare.

(3) Rezumatele, traducerile și extrasele din documentele clasificate primesc clasa sau nivelul de secretizare corespunzător conținutului.

Art. 15

Marcarea informațiilor clasificate are drept scop atenționarea persoanelor care le gestionează sau le accesează că sunt în posesia unor informații în legătură cu care trebuie aplicate măsuri specifice de acces și protecție, în conformitate cu legea.

Art. 16

Cazurile considerate supraevaluări ori subevaluări ale clasei sau nivelului de secretizare vor fi supuse atenției emitentului, iar dacă acesta decide să reclasifice informațiile va informa deținătorii.

Art. 17

(1) Informațiile vor fi clasificate numai în cazul în care se impune protecția acestora, iar nivelurile de secretizare și termenele de clasificare subzistă atât timp cât dezvăluirea sau diseminarea lor neautorizată ar putea prejudicia siguranța națională, apărarea țării, ordinea publică sau interesele persoanelor juridice de drept public sau privat.

(2) Supraevaluarea sau subevaluarea nivelului de secretizare a informațiilor și a duratei pentru care au fost clasificate se pot contesta de către orice persoană fizică sau juridică română, în contencios administrativ.

Art. 18

(1) În termen de 12 luni de la intrarea în vigoare a prezentei hotărâri, deținătorii de informații secrete de stat și secrete de serviciu, stabilite astfel potrivit H.C.M. nr. 19 din 14 ianuarie 1972, vor prezenta persoanelor sau autorităților publice împuternicite să atribuie niveluri de secretizare propuneri privind încadrarea acestor informații în noi clase și niveluri de secretizare, după caz.

(2) Până la stabilirea noilor niveluri de secretizare, informațiile secrete de stat și secrete de serviciu menționate la alin. (1) își păstrează nivelul și termenul de secrelizare și vor fi protejate potrivit prezentelor standarde.

SECȚIUNEA 2: Declasificarea și trecerea informațiilor clasificate la un nivel inferior de secretizare

Art. 19

Informațiile secrete de stat pot fi declasificate prin hotărâre a Guvernului, la solicitarea motivată a emitentului.

Art. 20

(1) Informațiile se declasifică dacă:

- a) termenul de clasificare a expirat;
- b) dezvăluirea informațiilor nu mai poate prejudicia siguranța națională, apărarea țării, ordinea publică, ori interesele persoanelor de drept public sau privat deținătoare;
- c) a fost atribuit de o persoană neîmputernicită prin lege.

(2) Declasificarea sau trecerea la un alt nivel de secretizare a informațiilor secrete de stat se realizează de împuterniciții și funcționarii superiori abilitați prin lege să atribuie niveluri de secretizare, cu avizul prealabil al instituțiilor care coordonează activitatea și controlul măsurilor privitoare la protecția informațiilor clasificate, potrivit competențelor materiale.

(3) Emitenții documentelor secrete de stat vor evalua periodic necesitatea menținerii în nivelurile de secretizare acordate anterior și vor prezenta împuterniciților și funcționarilor superiori abilitați prin lege să atribuie niveluri de secretizare, propuneri în consecință.

Art. 21

Ori de câte ori este posibil, emitentul unui document clasificat trebuie să precizeze dacă acesta poate fi declasificat ori trecut la un nivel inferior de secretizare, la o anumită dată sau la producerea unui anumit eveniment.

Art. 22

(1) La schimbarea clasei sau nivelului de secretizare atribuit inițial unei informații, emitentul este obligat să încunoștințeze structura/funcționarul de securitate, care va face mențiunile necesare în registrele de evidență.

(2) Data și noua clasă sau nivel de secretizare vor fi marcate pe document deasupra sau sub vechea inscripție, care va fi anulată prin trasarea unei linii oblice.

(3) Emitentul informațiilor declasificate ori trecute în alt nivel de clasificare se va asigura că gestionarii acestora sunt anunțați la timp, în scris, despre acest lucru.

Art. 23

(1) Informațiile clasificate despre care s-a stabilit cu certitudine că sunt compromise sau iremediabil pierdute vor fi declasificate.

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

Art. 24

Informațiile secrete de serviciu se declasifică de conducătorii unităților care le-au emis, prin scoaterea de pe listele prevăzute la art. 8, care vor fi reanalizate ori de câte ori este necesar.

SECȚIUNEA 3: Măsuri minime de protecție a informațiilor clasificate

Art. 25

Măsurile de protecție a informațiilor clasificate vor fi stabilite în raport cu:

- a) clasele și nivelurile de secretizare a informațiilor;
- b) volumul și suportul informațiilor;
- c) calitatea, funcția și numărul persoanelor care au sau pot avea acces la informații, potrivit certificatului de securitate și autorizației de acces și cu respectarea principiului necesității de a cunoaște;
- d) amenințările, riscurile și vulnerabilitățile ce pot avea consecințe asupra informațiilor clasificate.

Art. 26

Transmiterea informațiilor clasificate către alți utilizatori se va efectua numai dacă aceștia dețin certificate de securitate sau autorizații de acces corespunzătoare nivelului de secretizare.

Art. 27

Certificatele de securitate aparținând persoanelor al căror comportament, atitudini sau manifestări pot crea premise de insecuritate pentru informațiile secrete de stat vor fi imediat retrase, cu încunoștințarea instituțiilor investite cu atribuții de coordonare a activității și de control al măsurilor privitoare la protecția informațiilor clasificate, potrivit competențelor.

Art. 28

Conducătorii unităților și persoanele care gestionează informații clasificate au obligația de a aduce la cunoștință instituțiilor cu atribuții de coordonare și control în domeniu orice indicii din care pot rezulta premise de insecuritate pentru astfel de informații.

SECȚIUNEA 4: Structura/funcționarul de securitate

Art. 29

- (1) Pentru implementarea măsurilor de protecție a informațiilor clasificate, în unitătile deținătoare de astfel de informații se înființează, în condițiile legii, structuri de securitate cu atribuții specifice.
- (2) În situația în care unitatea deține un volum redus de informații clasificate, atribuțiile structurii de securitate vor fi îndeplinite de funcționarul de securitate.
- (3) Structura de securitate se organizează și se încadrează potrivit legii.
- (4) Șeful structurii de securitate, respectiv funcționarul de securitate, este un adjunct al conducătorului persoanei juridice sau un membru al consiliului de administrație al unității.

Art. 30

Şeful structurii de securitate, respectiv funcționarul de securitate, deține certificat de securitate corespunzător celui mai înalt nivel de clasificare a informațiilor secrete de stat gestionate de unitate.

Art. 31

- (1) Structura/funcționarul de securitate are următoarele atribuții generale:
- a) elaborează și supune aprobării conducerii unității normele interne privind protecția informațiilor clasificate, potrivit legii;
 - b) întocmește programul de prevenire a surgerii de informații clasificate și îl supune avizării instituțiilor abilitate, iar după aprobare, acționează pentru aplicarea acestuia;
 - c) coordonează activitatea de protecție a informațiilor clasificate, în toate componentele acesteia;
 - d) asigură relaționarea cu instituția abilită să coordoneze activitatea și să controleze măsurile privitoare la protecția informațiilor clasificate, potrivit legii;
 - e) monitorizează activitatea de aplicare a normelor de protecție a informațiilor clasificate și modul de respectare a acestora;
 - f) consiliază conducerea unității în legătură cu toate aspectele privind securitatea informațiilor clasificate;
 - g) informează conducerea unității despre vulnerabilitățile și risurile existente în sistemul de protecție a informațiilor clasificate și propune măsuri pentru înălțarea acestora;
 - h) acordă sprijin reprezentanților autorizați ai instituțiilor abilitate, potrivit competențelor legale, pe linia verificării persoanelor pentru care se solicită accesul la informații clasificate;
 - i) organizează activități de pregătire specifică a persoanelor care au acces la informații clasificate;
 - j) asigură păstrarea și organizează evidența certificatelor de securitate și autorizațiilor de acces la informații clasificate;
 - k) actualizează permanent evidența certificatelor de securitate și a autorizațiilor de acces;
- 1) întocmește și actualizează listele informațiilor clasificate elaborate sau păstrate de unitate, pe clase și niveluri de secretizare;
- m) prezintă conducătorului unității propuneri privind stabilirea obiectivelor, sectoarelor și locurilor de importanță deosebită pentru protecția informațiilor clasificate din sfera de responsabilitate și, după caz, solicită sprijinul instituțiilor abilitate;

- n) efectuează, cu aprobarea conducerii unității, controale privind modul de aplicare a măsurilor legale de protecție a informațiilor clasificate,
- o) exercită alte atribuții în domeniul protecției informațiilor clasificate, potrivit legii.

(2) Atribuțiile personalului din structura de securitate, respectiv ale funcționarului de securitate, se stabilesc prin fișa postului, aprobată de conducătorul unității.

Art. 32

Persoanele care lucrează în structura de securitate sau, după caz, funcționarul de securitate vor fi incluse în programe permanente de pregătire organizate de instituțiile investite cu atribuții de coordonare a activității și de control al măsurilor privitoare la protecția informațiilor clasificate, potrivit legii.

SECȚIUNEA 5: Accesul la informațiile clasificate

Art. 33

Accesul la informații clasificate este permis cu respectarea principiului necesității de a cunoaște numai persoanelor care dețin certificat de securitate sau autorizație de acces, valabile pentru nivelul de secretizare al informațiilor necesare îndeplinirii atribuțiilor de serviciu.

Art. 34

Persoanele care au acces la informații strict secrete de importanță deosebită, în condițiile prevăzute de prezentele standarde, vor fi înregistrate în fișa de consultare, prevăzută la anexa nr. I, care va fi păstrată la deținătorul de drept al documentului.

Art. 35

(1) Persoanele cărora le-au fost eliberate certificate de securitate sau autorizații de acces vor fi instruite, atât la acordarea acestora, cât și periodic, cu privire la conținutul reglementărilor privind protecția informațiilor clasificate.

(2) Activitățile de instruire vor fi consemnate de structura/funcționarul de securitate, sub semnătură, în fișa de pregătire individuală, prezentată la anexa nr. 2.

(3) Persoanele prevăzute la alin. (1) vor semna angajamentul de confidențialitate prevăzut la anexa nr. 3.

Art. 36

(1) În cazuri excepționale, determinate de situații de criză, calamități sau evenimente imprevizibile, conducătorul unității poate acorda acces temporar la informații clasificate anumitor persoane care nu dețin certificat de securitate sau autorizație de acces, cu condiția asigurării unui sistem corespunzător de evidență.

(2) Persoanele care primesc dreptul de acces temporar la informații secrete de stat vor semna angajamentul de confidențialitate și vor fi comunicate la ORNISS, în cel mai scurt timp posibil, pentru efectuarea verificărilor de securitate, potrivit procedurilor.

Art. 37

În cazul informațiilor strict secrete de importanță deosebită, accesul temporar va fi acordat, pe cât posibil, persoanelor care dețin deja certificate de securitate pentru acces la informații strict secrete sau secrete.

Art. 38

(1) Transmiterea informațiilor clasificate între unități se va efectua cu aprobarea emitentului și cu respectarea principiului necesității de a cunoaște.

(2) Predarea-primirea informațiilor clasificate între unitatea deținătoare și unitatea primitoare se face cu respectarea măsurilor de protecție prevăzute în prezentele standarde.

Art. 39

Structura/funcționarul de securitate al unității deținătoare se va asigura că reprezentantul unității primitoare deține certificatul de securitate sau autorizația de acces corespunzătoare nivelului de secretizare a informațiilor clasificate ce fac obiectul predării-primirii.

CAPITOLUL III: REGULI GENERALE PRIVIND EVIDENȚA, ÎNTOCMIREA, PĂSTRAREA, PROCESAREA, MULTIPLICAREA, MANIPULAREA, TRANSPORTUL, TRANSMITEREA ȘI DISTRUGEREA INFORMAȚIILOR CLASIFICATE

Art. 40

(1) în unitățile deținătoare de informații clasificate se organizează compartimente speciale pentru evidența, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea și distrugerea acestora în condiții de siguranță.

(2) Activitatea compartimentelor speciale prevăzute la alin. (1) este coordonată de structura/funcționarul de securitate.

Art. 41

La redactarea documentelor ce conțin informații clasificate se vor respecta următoarele reguli:

- a) menționarea, în antet, a unității emitente, a numărului și datei înregistrării, a clasei sau nivelului de secretizare, a numărului de exemplare și, după caz, a destinatarului;
- b) numerele de înregistrare se înscriu pe toate exemplarele documentului și pe anexele acestora, fiind precedate de un zero (0) pentru documentele secrete, de două zerouri (00) pentru cele strict secrete, de trei zerouri (000) pentru cele strict secrete de importanță deosebită și de litera "S" pentru secrete de serviciu;
- c) la sfârșitul documentului se înscriu în clar, după caz, rangul, funcția, numele și prenumele conducătorului unității emitente, precum și ale celui care îl întocmește, urmate de semnăturile acestora și stampila unității;
- d) înscrierea, pe fiecare pagină a documentului, a clasei sau nivelului de secretizare atribuit acestuia;
- e) pe fiecare pagină a documentelor ce conțin informații clasificate se înscriu numărul curent al paginii, urmat de numărul total al acestora.

Art. 42

(1) în situația în care documentul de bază este însotit de anexe, la sfârșitul textului se indică, pentru fiecare anexă, numărul de înregistrare, numărul de file al acesteia și clasa sau nivelul de secretizare.

(2) Anexele se clasifică în funcție de conținutul lor și nu de cel al documentelor pe care le însotesc.

(3) Adresa de însotire a documentului nu va cuprinde informații detaliate referitoare la conținutul documentelor anexate.

(4) Documentele anexate se semnează, dacă este cazul, de persoanele care au semnat documentul de bază.

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

Art. 43

(1) Când documentele ce conțin informații clasificate se semnează de o singură persoană, datele privind rangul, funcția, numele și prenumele acesteia se înscriu sub text, în centrul paginii.

(2) Când semnează două sau mai multe persoane, rangul, funcția, numele și prenumele conducerii unității se înscriu în partea stângă, iar ale celorlalți semnatari în partea dreaptă, în ordinea rangurilor și funcțiilor.

Art. 44

Când documentele care conțin informații clasificate se emit în comun de două sau mai multe unități, denumirile acestora se înscriu separat în antet, iar la sfârșit se semnează de către conducerii unităților respective, de la stânga la dreapta, aplicându-se stampilele corespunzătoare.

Art. 45

Informațiile clasificate vor fi marcate, insriptionate și gestionate numai de către persoane care au autorizație sau certificat de securitate corespunzător nivelului de clasificare a acestora.

Art. 46

(1) Toate documentele, indiferent de formă, care conțin informații clasificate au înscrise, pe fiecare pagină, nivelul de secretizare.

(2) Nivelul de secretizare se marchează prin stampilare, dactilografiere, tipărire sau olograf, astfel:

- a) în partea dreaptă sus și jos, pe exteriorul copertelor, pe pagina cu titlul și pe prima pagină a documentului;
- b) în partea de jos și de sus, la mijlocul paginii, pe toate celealte pagini ale documentului;
- c) sub legendă, titlu sau scara de reprezentare și în exterior - pe verso - atunci când acestea sunt pliate, pe toate schemele, diagramele, hărțile, desenele și alte asemenea documente.

Art. 47

Porțiunile clar identificabile din documentele clasificate complexe, cum sunt secțiunile, anexele, paragrafele, titlurile, care au niveluri diferite de secretizare sau care nu sunt clasificate, trebuie marcate corespunzător nivelului de clasificare și secretizare.

Art. 48

Marcajul de clasificare va fi aplicat separat de celealte marcaje, cu caractere și/sau culori diferite.

Art. 49

(1) Toate documentele clasificate aflate în lucru sau în stadiu de proiect vor avea înscrise mențiunile "Document în lucru" sau "Proiect" și vor fi marcate potrivit clasei sau nivelului de secretizare a informațiilor ce le conțin.

(2) Gestionarea documentelor clasificate aflate în lucru sau în stadiu de proiect se face în aceleași condiții ca și a celor în formă definitivă.

Art. 50

Documentele sau materialele care conțin informații clasificate și sunt destinate unei persoane strict determinate vor fi insriptionate, sub destinatar, cu mențiunea „Personal”.

Art. 51

(1) Fotografiile, filmele, microfilmele și negativele lor, rolele, bobinele sau containerele de păstrare a acestora se marchează vizibil cu o etichetă care indică numărul și data înregistrării, precum și clasa sau nivelul de secretizare.

(2) Microfilmele trebuie să aibă afișat la cele două capete clasa sau nivelul de secretizare, iar la începutul rolei, lista elementelor de conținut.

Art. 52

(1) Clasa sau nivelul de secretizare a informațiilor înregisterate pe benzi audio se imprimă verbal, atât la începutul înregistrării, cât și la sfârșitul acesteia.

(2) Marcarea clasei sau a nivelului de secretizare pe benzi video trebuie să asigure afișarea pe ecran a clasei sau a nivelului de secretizare. În cazul în care nu se poate stabili cu exactitate clasa sau nivelul de secretizare, înainte de înregistrarea benzilor, marcajul se aplică prin inserarea unui segment de bandă la începutul și la sfârșitul benzii video.

(3) Benzile audio și video care conțin informații clasificate păstrează clasa sau nivelul de secretizare cel mai înalt atribuit până în momentul:

a) distrugerii printr-un procedeu autorizat;

b) atribuirii unui nivel superior prin adăugarea unei înregistrări cu nivel superior de secretizare.

Art. 53

Proiecțiile de imagini trebuie să afișeze, la începutul și sfârșitul acestora, numărul și data înregistrării, precum și clasa sau nivelul de secretizare.

Art. 54

(1) Rolele, bobinele sau containerele de păstrare a benzilor magnetice, inclusiv cele video, pe care au fost imprimate informații secrete de stat, vor avea înscris, la loc vizibil, clasa sau nivelul de secretizare cel mai înalt atribuit acestora, care va rămâne aplicat până la distrugerea sau demagnetizarea lor.

(2) La efectuarea unei înregistrări pe bandă magnetică, atât la începutul, cât și la sfârșitul fiecărui pasaj, se va menționa clasa sau nivelul de secretizare.

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

Art. 55

În toate cazurile, ambalajele sau suportii în care se păstrează documente sau materiale ce conțin informații clasificate vor avea inscripționat clasa sau nivelul de secretizare, numărul și data înregistrării în evidență și li se va ataşa o listă cu denumirea acestora.

Art. 56

(1) Atunci când se utilizează documente clasificate ca surse pentru întocmirea unui alt document, marcajele documentelor sursă le vor determina pe cele ale documentului rezultat.

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

Art. 57

Numărul și dala initială a înregistrării documentului clasificat trebuie păstrate, chiar dacă i se aduc amendamente, până când documentul respectiv va face obiectul reevaluării clasei sau a nivelului de secretizare.

Art. 58

Conducătorii unităților vor asigura măsurile necesare de evidență și control al informațiilor clasificate, astfel încât să se poată stabili, în orice moment, locul în care se află aceste informații.

Art. 59

(1) Evidența materialelor și documentelor care conțin informații clasificate se ține în registre speciale, întocmite potrivit modelelor prevăzute în anexele nr. 4, 5 și 6.

(2) Fiecare document sau material va fi inscripționat cu numărul de înregistrare și data când este înscris în registrele de evidență.

(3) Numerele de înregistrare sunt precedate de numărul de zerouri corespunzător nivelului de secretizare atribuit sau de litera "S" pentru secrete de serviciu.

(4) toate registrele, condicile și borderourile se înregistrează în registrul unic de evidență a registrelor, condicilor, borderourilor și a caietelor pentru însemnări clasificate, conform modelului din anexa nr. 7.

(5) Fac excepție actele de gestiune, imprimatele inseriate și alte documente sau materiale cuprinse în forme de evidență specifice.

Art. 60

(1) Documentele sau materialele care conțin informații clasificate înregistrate în registrele prevăzute în art. 59 nu vor fi înregistrate în alte forme de evidență.

(2) Emitenți și detinătorii de informații clasificate sunt obligați să înregistreze și să țină evidență tuturor documentelor și materialelor primite, expediate sau a celor întocmite de unitatea proprie, potrivit legii.

(3) În registrele pentru evidență informațiilor clasificate vor fi menționate numele și prenumele persoanei care a primit documentul, iar aceasta va semna de primire pe condica prevăzută în anexa nr. 8.

Art. 61

(1) Atribuirea numerelor de înregistrare în registrele pentru evidență se face consecutiv, pe parcursul unui an calendaristic.

(2) Numerele de înregistrare se înscriu obligatoriu pe toate exemplarele documentelor sau materialelor care conțin informații clasificate, precum și pe documentele anexate.

(3) Anual, documentele se clăseză în dosare, potrivit problematicii și termenelor de păstrare stabilite în nomenclatoare arhivistice, potrivit legii.

(4) Clasarea documentelor sau materialelor care conțin informații clasificate se face separat, în funcție de suportul și formatul acestora, cu folosirea mijloacelor de păstrare și protejare adecvate.

Art. 62

(1) Informațiile strict secrete de importanță deosebită vor fi compartimentate fizic și înregistrate separat de celelalte informații.

(2) Evidența documentelor strict secrete și secrete poate fi operată în același registru.

Art. 63

Hărțile, planurile topografice, asamblajele de hărți și alte asemenea documente se înregistrează în registrele pentru evidență informațiilor clasificate prevăzute în anexele nr. 4, 5 și 6.

Art. 64

Atribuirea același număr de înregistrare unor documente cu conținut diferit este interzisă.

Art. 65

Registrele de evidență vor fi completate de persoana desemnată care deține autorizație sau certificat de securitate corespunzător.

Art. 66

(1) Multiplicarea prin dactilografie și procesare la calculator a documentelor clasificate poate fi realizată numai de către persoane autorizate să aibă acces la astfel de informații.

(2) Multiplicarea documentelor clasificate poate fi realizată de persoane autorizate, numai în încăperi special destinate.

Art. 67

(1) Documentelor care conțin informații clasificate rezultate în procesul de multiplicare li se atribuie numere din registrul de evidență a informațiilor clasificate multiple, conform modelului din anexa nr. 9.

(2) Numerele se atribuie consecutiv, începând cu cifra I, pe parcursul unui an calendaristic și se înscrui obligatoriu pe toate exemplarele documentului.

Art. 68

(1) Evidențierea operațiunii de multiplicare se face prin marcare atât pe original, cât și pe toate copiile rezultate.

(2) Pe documentul original marcarea se aplică în partea dreaptă jos a ultimei pagini.

(3) Pe copiile rezultate, marcarea se aplică pe prima pagină, sub numărul de înregistrare al documentului.

(4) În cazul copierii succesive, la date diferite, a unui document clasificat, documentul original va fi marcat la fiecare operațiune, ce va fi, de asemenea, înscrisă în registru.

(5) Exemplarele rezultate în urma copierii documentului secret de stat se numerotează în ordine succesivă, chiar dacă operațiunea se efectuează de mai multe ori și la date diferite.

Art. 69

(1) Multiplicarea documentelor clasificate se face în baza aprobării conducătorului unității deținătoare, cu avizul structurii/funcționarului de securitate, ambele înscrise pe cererea pentru copiere sau pe adresa de însoțire în care se menționează necesitatea multiplicării.

(2) Parchetele, instanțele și comisiile de cercetare pot multiplica documente care conțin informații clasificate numai în condițiile prezenterelor standarde.

(3) Extrasul dintr-un document care conține informații clasificate se face în baza cererii pentru copiere, cu aprobarea conducătorului unității, iar documentul rezultat va avea menționat sub numărul de exemplar cuvântul „Extras” și numărul de înregistrare al documentului original.

(4) Clasa sau nivelul de secretizare atribuit unui document original se aplică, în mod identic, reproducărilor sau traducerilor.

Art. 70

(1) Dacă emitentul dorește să aibă control exclusiv asupra reproducării, documentul va conține o indicație vizibilă cu următorul conținut: "Reproducerea acestui document, totală sau parțială, este interzisă".

(2) Informațiile clasificate înscrise pe documente cu regim restrictiv de reproducere care au mențiunea „Reproducerea interzisă” nu se multiplică.

Art. 71

În cazul copierii unui document care conține informații clasificate se procedează astfel:

- a) se stabilește numărul de exemplare în care va fi multiplicat;
- b) se completează și se aprobă cererea pentru multiplicare, potrivit art. 69 alin. (1), după care aceasta se înregistrează în registrul de evidență - anexa nr. 4 sau anexa nr. 5, după caz;
- c) documentul original se predă operatorului pe bază de semnătură;
- d) după verificarea exemplarelor rezultate, beneficiarul semnează în registrul de evidență a informațiilor clasificate multiple, conform modelului din anexa nr. 9;
- e) repartitia în vederea difuzării exemplarelor copiate se consemnează de către structura/funcționarul de securitate pe spatele cererii pentru copiere;
- f) cererea pentru copiere împreună cu exemplarele copiate se predau pe bază de semnătură structurii/funcționarului de securitate în vederea difuzării sau expedierii.

Art. 72

(1) Când se dactilografiază, se procesează la calculator sau se copiază documente care conțin informații clasificate, în mai mult de două exemplare, pe spatele exemplarului original sau al cererii pentru copiere se înscriu destinatarii documentelor și numărul exemplarelor.

(2) Atunci când numărul destinatarilor este mare se întocmește un tabel de difuzare, care se înregistrează ca document anexat la original.

(3) Numerotarea exemplarelor copiate se va face consecutiv pentru fiecare copie, indiferent de data executării, avându-se în vedere și numărul de exemplare rezultat în urma dactilografierii sau procesării la calculator.

Art. 73

Documentele clasificate pot fi microfilmate sau stocate pe discuri optice ori pe suporti magnetici în următoarele condiții:

- a) procesul de microfilmare sau stocare să fie realizat cu aprobarea emitentului, de personal autorizat pentru clasa sau nivelul de secretizare a informațiilor respective,
- b) microfilmelor, discurilor optice sau suportilor magnetici de stocare să li se asigure aceeași protecție ca a documentului original;
- c) toate microfilmele, discurile optice sau suportii magnetici de stocare să fie înregistrate într-o evidență specifică și supuse, ca și documentele originale, verificării anuale.

Art. 74

(1) Difuzarea informațiilor clasificate multiplicate se face obligatoriu cu avizul structurii/funcționarului de securitate.

(2) Informațiile clasificate pot fi redifuzate de către destinatarul initial la alți destinatari, cu respectarea normelor din prezentele standarde.

(3) Emitentul este obligat să indice clar toate restricțiile care trebuie respectate pentru difuzarea unei informații clasificate. Când se impun astfel de restricții, destinatarii pot proceda la o redifuzare numai cu aprobarea scrisă a emitentului.

Art. 75

În cazul în care un document secret de stat este studiat de o persoană abilitată, pentru care s-a stabilit necesitatea de a accesa astfel de documente în vederea îndeplinirii sarcinilor de serviciu, această activitate trebuie consemnată în fișă de consultare, conform modelului din anexa nr. I.

Art. 76

(1) Informațiile clasificate ieșite din termenul de clasificare se arhivează sau se distrug.

(2) Arhivarea sau distrugerea unui document clasificat se menționează în registrul de evidență principal, prin consemnarea cotei arhivistice de regăsire sau, după caz, a numărului de înregistrare a procesului-verbal de distrugere.

(3) Distrugerea informațiilor clasificate înlocuite sau perimate se face numai cu avizul emitentului.

(4) Distrugerea documentelor clasificate sau a ciornelor care conțin informații cu acest caracter se face astfel încât să nu mai poată fi reconstituite.

Art. 77

(1) Documentele de lucru, ciornele sau materialele acumulate sau create în procesul de elaborare a unui document, care conțin informații clasificate, de regulă, se distrug.

(2) În cazul în care se păstrează, acestea vor fi date, marcate cu clasa sau nivelul de secretizare cel mai înalt al informațiilor conținute, arhivate și protejate corespunzător clasei sau nivelului de secretizare a documentului final.

Art. 78

(1) Informațiile strict secrete de importanță deosebită destinate distrugerii vor fi înapoiate unității emitente cu adresă de restituire.

(2) Fiecare asemenea informație va fi trecută pe un proces-verbal de distrugere, care va fi aprobat de conducerea unității și semnat de șeful structurii/funcționarul de securitate și de persoana care asistă la distrugere, autorizată să aibă acces la informații strict secrete de importanță deosebită.

(3) În situații de urgență, protecția, inclusiv prin distrugere, a materialelor și documentelor strict secrete de importanță deosebită va avea întotdeauna prioritate față de alte documente sau materiale.

(4) Procesele-verbale de distrugere și documentele de evidență ale acestora vor fi arhivate și păstrate cel puțin 10 ani.

Art. 79

(1) Distrugerea informațiilor strict secrete, secrete și secrete de serviciu va fi evidențiată într-un proces-verbal semnat de două persoane asistente autorizate să aibă acces la informații de acest nivel, avizat de structura/funcționarul de securitate și aprobat de conducătorul unității.

(2) Procesele-verbale de distrugere și documentele de evidență a informațiilor strict secrete, secrete și secrete de serviciu vor fi păstrate de compartimentul care a executat distrugerea, o perioadă de cel puțin trei ani, după care vor fi arhivate și păstrate cel puțin 10 ani.

Art. 80

(1) Distrugerea ciornelor documentelor secrete de stat se realizează de către persoanele care le-au elaborat.

(2) Procesul-verbal de distrugere a ciornelor se întocmește în situația în care acestea au fost înregistrate într-o formă de evidență.

Art. 81

(1) Documentele și materialele ce conțin informații clasificate se transportă, pe teritoriul României, prin intermediul unității specializate a Serviciului Român de Informații, potrivit normelor stabilite prin hotărâre a Guvernului.

(2) Documentele și materialele care conțin informații clasificate se transportă în străinătate prin valiza diplomatică, de către curieri diplomatici selecționați și pregătiți de Serviciul de Informații Externe.

(3) Este interzisă expedierea documentelor și materialelor ce conțin informații clasificate prin S.N. "Poșta Română" ori prin alte societăți comerciale de transport.

Art. 82

Conducătorii unităților deținătoare de informații clasificate vor desemna, din structura de securitate proprie, în condițiile prezentelor standarde, cel puțin un delegat împoternicit pentru transportul și executarea operațiunilor de predare-primire a corespondenței clasificate, între aceasta și unitatea specializată a Serviciului Român de Informații.

CAPITOLUL IV: PROTECȚIA INFORMAȚIILOR SECRETE DE STAT

SECȚIUNEA 1: Obligațiile și răspunderile ce revin autorităților și instituțiilor publice, agenților economici și altor persoane juridice pentru protecția informațiilor secrete de stat

Art. 83

Protecția informațiilor secrete de stat reprezintă o obligație ce revine tuturor persoanelor autorizate care le emit, le gestionează sau care intră în posesia lor.

Art. 84

(1) Conducătorii unităților deținătoare de informații secrete de stat sunt răspunzători de aplicarea măsurilor de protecție a informațiilor secrete de stat.

(2) Persoanele juridice de drept privat deținătoare de informații secrete de stat au obligația să respecte și să aplică reglementările în vigoare stabilite pentru autoritățile și instituțiile publice, în domeniul lor de activitate.

Art. 85

Până la înființarea și organizarea structurii de securitate sau, după caz, până la numirea funcționarului de securitate, conducătorii unităților deținătoare de informații secrete de stat vor desemna o persoană care să îndeplinească temporar atribuțiile specifice protecției informațiilor clasificate, prin cumul de funcții.

Art. 86

(1) Conducătorul unității care gestionează informații secrete de stat este obligat:

- a) să asigure organizarea activității structurii de securitate, respectiv a funcționarului de securitate și comportamentelor speciale pentru gestionarea informațiilor clasificate, în condițiile legii;
- b) să solicite instituțiilor abilitate efectuarea de verificări pentru avizarea eliberării certificatului de securitate și autorizației de acces la informații clasificate pentru angajații proprii;
- c) să notifice la ORNISS eliberarea certificatului de securitate sau autorizației de acces pentru fiecare angajat care lucrează cu informații clasificate;
- d) să aprobe liste cu personalul verificat și avizat pentru lucrul cu informațiile secrete de stat și evidența deținătorilor de certificate de securitate și autorizații de acces și să le comunice la ORNISS și la instituțiile abilitate să coordoneze activitatea și controlul măsurilor privitoare la protecția informațiilor clasificate, potrivit legii;
- e) să întocmească lista informațiilor secrete de stat și a termenelor de menținere în nivelurile de secretizare și să o supună aprobării Guvernului, potrivit legii;
- f) să stabilească obiectivele, sectoarele și locurile din zona de competență care prezintă importanță deosebită pentru protecția informațiilor secrete de stat și să le comunice Serviciului Român de Informații pentru a fi supuse spre aprobare Guvernului;
- g) să solicite asistență de specialitate instituțiilor abilitate să coordoneze activitatea și să controleze măsurile privitoare la protecția informațiilor secrete de stat;
- h) să supună avizării instituțiilor abilitate programul propriu de prevenire a scurgerii de informații clasificate și să asigure aplicarea acestuia;
- i) să elaboreze și să aplică măsurile procedurale de protecție fizică și de protecție a personalului care are acces la informații clasificate;
- j) să întocmească ghidul pe baza căruia se va realiza încadrarea corectă și uniformă în nivelurile de secretizare a informațiilor secrete de stat, în strictă conformitate cu legea și să îl prezinte,

spre aprobare, împăterniciților și funcționarilor superiori abilitați prin lege să atribuie nivelurile de secretizare;

k) să asigure aplicarea și respectarea regulilor generale privind evidența, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea și distrugerea informațiilor secrete de stat și a interdicțiilor de reproducere și circulație, în conformitate cu actele normative în vigoare;

l) să comunice instituțiilor abilitate, potrivit competențelor, lista funcțiilor din subordine care necesită acces la informații secrete de stat;

m) la încheierea contractelor individuale de muncă, a contractelor de colaborare sau convențiilor de orice natură să precizeze obligațiile ce revin părților pentru protecția informațiilor clasificate în interiorul și în afara unității, în timpul programului și după terminarea acestuia, precum și la încetarea activității în unitatea respectivă;

n) să asigure includerea personalului structurii/funcționarului de securitate în sistemul permanent de pregătire și perfecționare, conform prezentelor standarde;

o) să aprobe normele interne de aplicare a măsurilor privind protecția informațiilor clasificate, în toate componentele acesteia, și să controleze modul de respectare în cadrul unității;

p) să asigure fondurile necesare pentru implementarea măsurilor privitoare la protecția informațiilor clasificate, conform legii;

q) să analizeze, ori de câte ori este necesar, dar cel puțin semestrial, modul în care structura/funcționarul de securitate și personalul autorizat asigură protecția informațiilor clasificate;

r) să asigure inventarierea anuală a documentelor clasificate și, pe baza acesteia, să dispună măsuri în consecință, conform legii;

s) să sesizeze instituțiile prevăzute la art. 25 din Legea nr. **182/2002**, conform competențelor, în legătură cu incidentele de securitate și riscurile la adresa informațiilor secrete de stat;

t) să dispună efectuarea de cercetări și, după caz, să sesizeze organele de urmărire penală în situația compromiterii informațiilor clasificate.

(2) De la prevederile alin. (I) lit f) și h) se exceptează instituțiile prevăzute la art. 25 din Legea nr. **182/2002**.

SECȚIUNEA 2: Protecția juridică

Art. 87

Conducătorii unităților deținătoare de secrete de stat vor asigura condițiile necesare pentru ca toate persoanele care gestionează astfel de informații să cunoască reglementările în vigoare referitoare la protecția informațiilor clasificate.

Art. 88

(1) Conducătorii unităților deținătoare de informații secrete de stat au obligația de a înștiința, în scris, instituțiile prevăzute la art. 25 din Legea nr. **182/2002**, potrivit competențelor, prin cel mai operativ sistem de comunicare, despre compromiterea unor astfel de informații.

(2) Înștiințarea prevăzută la alin. (1) se face în scopul obținerii sprijinului necesar pentru recuperarea informațiilor, evaluarea prejudiciilor, diminuarea și înălțarea consecințelor.

(3) Înștiințarea trebuie să conțină:

a) prezentarea informațiilor compromise, respectiv clasificarea, marcarea, conținutul, data emiterii, numărul de înregistrare și de exemplare, emitentul și persoana sau compartimentul care le-a gestionat;

b) o scurtă prezentare a împrejurărilor în care a avut loc compromiterea, inclusiv data constatării, perioada în care informațiile au fost expuse compromiterii și persoanele neautorizate care au avut sau ar fi putut avea acces la acestea, dacă sunt cunoscute;

c) precizări cu privire la eventuala informare a emitentului.

(4) La solicitarea instituțiilor competente, însărcinările preliminare vor fi completate pe măsura derulării cercetărilor.

(5) Documentele privind evaluarea prejudiciilor și activitățile ce urmează a fi întreprinse ca urmare a compromiterii vor fi prezentate instituțiilor competente.

Art. 89

Pentru prejudiciile cauzate deținătorului informației secrete de stat compromise, acesta are dreptul la despăgubiri civile, potrivit dreptului comun.

Art. 90

(1) Orice încălcare a reglementărilor de securitate va fi cercetată pentru a se stabili:

a) dacă informațiile respective au fost compromise;

b) dacă persoanele neautorizate care au avut sau ar fi putut avea acces la informații secrete de stat prezintă suficientă încredere și loialitate, astfel încât rezultatul compromiterii să nu creeze prejudicii;

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

(2) În situația în care informațiile clasificate au fost accesate de persoane neautorizate, acestea vor fi instruite pentru a preveni producerea de eventuale prejudicii.

(3) În cazul săvârșirii de infracțiuni la protecția secretului de stat, unitățile deținătoare au obligația de a sesiza organele de urmărire penală și de a pune la dispoziția acestora datele și materialele necesare probării faptelor.

Art. 91

(1) Structura/funcționarul de securitate are obligația de a ține evidența cazurilor de încălcare a reglementărilor de securitate, a documentelor de cercetare și a măsurilor de soluționare și să le pună la dispoziția autorităților desemnate de securitate, conform competențelor ce le revin.

(2) Documentele menționate la alin. (1) se păstrează timp de cinci ani.

Art. 92

Litigiile cu privire la calitatea de emitent ori deținător sau cele determinate de conținutul informațiilor secrete de stat, inclusiv drepturile patrimoniale ce revin emitentului din contractele de cesiune și licență, precum și litigiile referitoare la nerespectarea dispozițiilor legale privind dreptul de autor și drepturile conexe, inventiile și inovațiile, protecția modelelor industriale, combaterea concurenței neloiale și a celor stipulate în tratatele, acordurile și înțelegerile la care România este parte, sunt de competența instanțelor judecătorești.

SECȚIUNEA 3: Protecția prin măsuri procedurale

Art. 93

Toate unitățile care dețin informații secrete de stat au obligația să stabilească norme interne de lucru și de ordine interioară destinate protecției acestor informații, potrivit actelor normative în vigoare.

Art. 94

(1) Măsurile procedurale de protecție a informațiilor secrete de stat vor fi integrate în programul de prevenire a scurgerii de informații clasificate, întocmit potrivit anexei nr. 10, care va fi

prezentat, spre avizare, autorității abilitate să coordoneze activitatea și să controleze măsurile privitoare la protecția informațiilor clasificate, potrivit legii.

(2) Sunt exceptate de obligativitatea prezentării, spre avizare, a programului de prevenire a scurgerii de informații, menționat la alin. (I), instituțiile prevăzute la art. 25 alin. (4) din Legea nr. [182/2002](#).

Art. 95

Angajamentele de confidențialitate întocmite potrivit reglementărilor în vigoare vor garanta că informațiile la care se acordă acces sunt protejate corespunzător.

SECȚIUNEA 4: Protecția fizică

Art. 96

Obiectivele, sectoarele și locurile în care sunt gestionate informații secrete de stat trebuie protejate fizic împotriva accesului neautorizat.

Art. 97

Măsurile de protecție fizică - gratii la ferestre, încuietori la uși, pază la intrări, sisteme automate pentru supraveghere, control, acces, patrule de securitate, dispozitive de alarmă, mijloace pentru detectarea observării, ascultării sau interceptării - vor fi dimensionale în raport cu:

- a) nivelul de secretizare a informațiilor, volumul și localizarea acestora;
- b) tipul containerelor în care sunt depozitate informațiile;
- c) caracteristicile clădirii și zonei de amplasare.

Art. 98

Zonele în care sunt manipulate sau stocate informații secrete de stat trebuie organizate și administrate în aşa fel încât să corespundă uneia din următoarele categorii:

a) zonă de securitate clasa I, care presupune că orice persoană aflată în interiorul acesteia are acces la informații secrete de stat, de nivel strict secret de importanță deosebită și strict secret, și care necesită:

- perimetru clar determinat și protejat, în care toate intrările și ieșirile sunt supravegheate;
- controlul sistemului de intrare, care să permită numai accesul persoanelor verificate corespunzător și autorizate în mod special;
- indicarea clasei și a nivelului de secretizare a informațiilor existente în zonă;

b) zonă de securitate clasa a II-a, care presupune că gestionarea informațiilor de nivel secret se realizează prin aplicarea unor măsuri specifice de protecție împotriva accesului persoanelor neautorizate și care necesită:

- perimetru clar delimitat și protejat, în care toate intrările și ieșirile sunt supravegheate;
- controlul sistemului de intrare care să permită accesul neînsotit numai persoanelor verificate și autorizate să pătrundă în această zonă;
- reguli de însurățire, supraveghere și prevenire a accesului persoanelor neautorizate la informații clasificate.

Art. 99

Incintele în care nu se lucrează zilnic 24 de ore vor fi inspectate imediat după terminarea programului de lucru, pentru a verifica dacă informațiile secrete de stat sunt asigurate în mod corespunzător.

Art. 100

în jurul zonelor de securitate clasa I sau clasa a II-a poate fi stabilită o zonă administrativă, cu perimetru vizibil delimitat, în interiorul căreia să existe posibilitatea de control al personalului și al vehiculelor.

Art. 101

- (1) Accesul în zonele de securitate clasa I și clasa a II-a va fi controlat prin verificarea permisului de acces sau printr-un sistem de recunoaștere individuală aplicat personalului.
- (2) Unitățile deținătoare de informații secrete de stat vor institui un sistem propriu de control al vizitatorilor, destinat interzicerii accesului neautorizat al acestora în zonele de securitate.

Art. 102

Permisul de acces nu va specifica, în clar, identitatea unității emitente sau locul în care deținătorul are acces.

Art. 103

Unitățile vor organiza, la intrarea sau la ieșirea din zonele de securitate clasa I sau clasa a II-a, controale planificate și inopinate ale bagajelor, inclusiv colete, genti și alte tipuri de suporturi în care s-ar putea transporta materiale și informații secrete de stat.

Art. 104

Personalul inclus în sistemul de pază și apărare a obiectivelor, sectoarelor și locurilor în care sunt gestionate informații secrete de stat trebuie să dețină autorizație de acces corespunzător nivelului de secretizare a informațiilor necesare îndeplinirii atribuțiilor ce îi revin.

Art. 105

Este interzis accesul cu aparate de fotografiat, filmat, înregistrat audio-video, de copiat din baze de date informatici sau de comunicare la distanță, în locurile în care se află informații secrete de stat.

Art. 106

Conducătorii unităților deținătoare de informații secrete de stat vor stabili reguli cu privire la circulația și ordinea interioară în zonele de securitate, astfel încât accesul să fie permis exclusiv posesorilor de certificate de securitate și autorizații de acces, cu respectarea principiului necesității de a cunoaște.

Art. 107

Accesul pentru intervenții tehnice, reparații sau activități de deservire în locuri în care se lucrează cu informații secrete de stat ori în care se păstrează, se prelucrează sau se multiplică astfel de informații este permis numai angajaților unității care dețin autorizații de acces, corespunzător celui mai înalt nivel de secretizare a informațiilor pe care le-ar putea cunoaște.

Art. 108

- (1) Pentru a distinge persoanele care au acces în diferite locuri sau sectoare în care sunt gestionate informații secrete de stat, acestea vor purta însemne sau echipamente specifice.
- (2) În locurile și sectoarele în care sunt gestionate informații secrete de stat, însemnele și echipamentele distinctive se stabilesc prin regulamente de ordine interioară
- (3) Evidența legitimațiilor, permiselor și a altor însemne și echipamente distinctive va fi ținută de structura/funcționarul de securitate al unității.

Art. 109

- (1) Persoanele care pierd permisele de acces în unitate, însemnele sau echipamentele specifice sunt obligate să anunțe de îndată șeful ierarhic.

(2) în situațiile menționate la alin. (1), conducătorul instituției va dispune cercetarea împrejurărilor în care s-au produs și va informa autoritatea desemnată de securitate competentă

(3) Structura/funcționarul de securitate va lua măsurile ce se impun pentru a preveni folosirea permiselor de acces, însemnelor sau echipamentelor specifice de către persoane neautorizate.

110

Accesul fiecărui angajat al unității deținătoare de informații secrete de stat în zone de securitate clasa I sau clasa a II-a se realizează prin intrări anume stabilite, pe baza permisului de acces, semnat de conducătorul acesteia.

Art. 111

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

(2) Permisele de acces se vizează semestrial.

(3) La încetarea angajării permisele de acces vor fi retrase și anulate.

Art. 112

Este interzis accesul altor persoane, în afara celor care dispun de permis de acces, în locurile în care sunt gestionate informații secrete de stat.

Art. 113

Accesul persoanelor din afara unității în zona administrativă sau în zonele de securitate este permis numai dacă sunt însotite de persoane anume desemnate, cu bilet de intrare eliberat pe baza documentelor de legitimare de conducătorul unității.

Art. 114

(1) Accesul angajaților agentilor economici care efectuează lucrări de construcții, reparații și întreținere a clădirilor, instalațiilor sau utilităților în zonele administrative ori în zonele de securitate se realizează cu documente de acces temporar eliberate de conducătorii unităților beneficiare, pe baza actelor de identitate, la solicitarea reprezentanților autorizați ai agenților economici în cauză.

(2) Locurile în care se efectuează lucrările menționate la alin. (1) se supraveghează de către persoane anume desemnate din unitatea beneficiară.

(3) Documentul de acces temporar are valabilitate pe durata executării lucrarilor și se vizează trimestrial, iar la terminarea activităților se restituie emitentului.

(4) Pierderea documentului de acces temporar va fi luată în evidență structurii/funcționarului de securitate care va dispune măsurile necesare de prevenire a folosirii lui de către persoane neautorizate.

Art. 115

Reprezentanții instituțiilor care, potrivit competențelor legale, au atribuții de coordonare și control pe linia protecției informațiilor clasificate au acces la obiectivele, sectoarele și locurile în care sunt gestionate informații clasificate, pe baza legitimației de serviciu și a delegației speciale, semnată de conducătorul autoritatii pe care o reprezintă.

Art. 116

Persoanele aflate în practică de documentare, stagii de instruire sau schimb de experiență au acces numai în locurile stabilite de conducătorul unității, pe baza permiselor de acces eliberate în acest sens.

Art. 117

Persoanele care solicită angajări, audiențe, ori care prezintă reclamații și sesizări vor fi primite în afara zonelor administrative sau în locuri special amenajate, cu aprobatia conducătorului unității.

Art. 118

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

Art. 119

(1) Sistemele de pază, supraveghere și control-acces trebuie să asigure prevenirea pătrunderii neautorizate în obiectivele, sectoarele și locurile unde sunt gestionate informații clasificate.

(2) Timpul de reacție a personalului de pază și apărare va fi testat periodic pentru a garanta intervenția operativă în situații de urgență.

Art. 120

(1) Unitățile care gestionează informații secrete de stat vor întocmi planul de pază și apărare a obiectivelor, sectoarelor și locurilor care prezintă importanță deosebită pentru protecția informațiilor clasificate.

(2) Planul de pază și apărare menționat la alin. (1) va fi înregistrat potrivit celui mai înalt nivel de secretizare a informațiilor protejate și va cuprinde totalitatea măsurilor de securitate luate pentru prevenirea accesului neautorizat la acestea.

(3) Planul de pază și apărare va fi anexat programului de prevenire a scurgerii de informații clasificate și va cuprinde:

- a) date privind delimitarea și marcarea zonelor de securitate, dispunerea posturilor de pază și măsurile de supraveghere a perimetruului protejat;
- b) sistemul de control al accesului în zonele de securitate;
- c) măsurile de avertizare și alarmare pentru situații de urgență;
- d) planul de evacuare a documentelor și modul de acțiune în caz de urgență;
- e) procedura de raportare, cercetare și evidență a incidentelor de securitate.

Art. 121

Informațiile secrete de stat se păstrează în containere speciale, astfel:

- a) containere clasa A, autorizate la nivel național pentru păstrarea informațiilor strict secrete de importanță deosebită în zona de securitate clasa I;
- b) containere clasa B, autorizate la nivel național pentru păstrarea informațiilor strict secrete și secrete în zone de securitate clasa I sau clasa a II-a.

Art. 122

(1) Containerele din clasele A și B vor fi construite astfel încât să asigure protecția împotriva pătrunderii clandestine și deteriorării sub orice formă a informațiilor.

(2) Standardele în care trebuie să se încadreze containerele din clasele A și B se stabilesc de ORNISS.

Art. 123

(1) Încăperile de securitate sunt încăperile special amenajate în zone de securitate clasa I sau clasa a II-a, în care informațiile secrete de stat pot fi păstrate pe rafturi deschise sau pot fi expuse pe hărți, planșe ori diagrame.

(2) Pereții, podelele, plafoanele, ușile și încuietorile încăperilor de securitate vor asigura protecția echivalentă clasei containerului de securitate aprobat pentru păstrarea informațiilor clasificate potrivit nivelului de secretizare.

Art. 124

(1) Ferestrele încăperilor de securitate dispuse la parter sau ultimul etaj vor fi protejate obligatoriu cu bare încastrate în beton sau asigurate antiefractie.

(2) În afara programului de lucru, ușile încăperilor de securitate vor fi sigilate, iar sistemul de aerisire asigurat împotriva accesului neautorizat și introducerii materialelor incendiare.

Art. 125

În situații de urgență, dacă informațiile secrete de stat trebuie evacuate, se vor utiliza lăzi metalice autorizate la nivel național din clasa corespunzătoare nivelului de secretizare a acestor informații.

Art. 126

Încuietorile folosite la containerele și încăperile de securitate în care sunt păstrate informații secrete de stat se împart în trei grupe, astfel:

- a) grupa A - încuietori autorizate pentru containerele din clasa A;
- b) grupa B - încuietori autorizate pentru containerele din clasa B;
- c) grupa C - încuietori pentru mobilierul de birou.

Art. 127

Standardele mecanismelor de închidere, a sistemelor cu cifru și încuietorilor, pe grupe de utilizare, se stabilesc de ORNISS.

Art. 128

Cheile containerelor și încăperilor de securitate nu vor fi scoase din zonele de securitate.

Art. 129

(1) În afara orelor de program, cheile de la încăperile și containerele de securitate vor fi păstrate în cutii sigilate, de către personalul care asigură paza și apărarea.

(2) Predarea și primirea cheilor de la încăperile și containerele de securitate se vor face, pe bază de semnatură, în condiție specială destinată - anexa nr. 11.

Art. 130

(1) Pentru situațiile de urgență, un rând de chei suplimentare sau, după caz, o evidență scrisă a combinațiilor încuietorilor, vor fi păstrate în plicuri mate sigilate, în containere separate, într-un compartiment stabilit de conducerea unității, sub control corespunzător.

(2) Evidența fiecărei combinații se va păstra în plic separat.

(3) Cheilor și plicurilor cu combinații trebuie să li se asigure același nivel de protecție ca și informațiilor la care permit accesul.

Art. 131

Combinațiile încuietorilor de la încăperile și containerele de securitate vor fi cunoscute de un număr restrâns de persoane desemnate de conducerea unității.

Art. 132

Cheile și combinațiile încuietorilor vor fi schimbate:

- a) ori de câte ori are loc o schimbare de personal;
- b) de fiecare dată când se constată că au intervenit situații de natură să le facă vulnerabile;
- c) la intervale regulate, de preferință o dată la șase luni, fără a se depăși 12 luni.

Art. 133

(1) Sistemele electronice de alarmare sau de supraveghere destinate protecției informațiilor secrete de stat vor fi prevăzute cu surse de alimentare de rezervă.

(2) Orice defecțiune sau intervenție neautorizată asupra sistemelor de alarmă sau de supraveghere destinate protecției informațiilor secrete de stat trebuie să avertizeze personalul care le monitorizează.

(3) Dispozitivele de alarmare trebuie să intre în funcțiune în cazul penetrării pereților, podelelor, tavanelor și deschizăturilor, sau la mișcări în interiorul încăperilor de securitate.

Art. 134

Copiatorele și dispozitivele telefax se vor instala în încăperi special destinate și se vor folosi numai de către persoanele autorizate, potrivit nivelului de secretizare a informațiilor la care au acces.

Art. 135

Unitățile deținătoare de informații secrete de stat au obligația de a asigura protecția acestora împotriva ascultărilor neautorizate, pasive sau active.

Art. 136

(1) Protecția împotriva ascultării pasive a discuțiilor confidentiale se realizează prin izolarea fonica a încăperilor.

(2) Protecția împotriva ascultărilor active, prin microfoane, radio-emiteitori și alte dispozitive implantate, se realizează pe baza inspecțiilor de securitate a încăperilor, accesoriilor, instalațiilor, sistemelor de comunicații, echipamentelor și mobilierului de birou, realizate de unitățile specializate, potrivit competențelor legale.

Art. 137

(1) Accesul în încăperile protejate împotriva ascultărilor se va controla în mod special.

(2) Periodic, personalul specializat în depistarea dispozitivelor de ascultare va efectua inspecții fizice și tehnice.

(3) Inspecțiile fizice și tehnice vor fi organizate, în mod obligatoriu, în urma oricărei intrări neautorizate sau suspiciuni privind accesul persoanelor neautorizate și după executarea lucrărilor de reparații, întreținere, zigravire sau redecorare.

(4) Nici un obiect nu va fi introdus în încăperile protejate împotriva ascultării, fără a fi verificat în prealabil de către personalul specializat în depistarea dispozitivelor de ascultare.

Art. 138

(1) În zonele în care se poartă discuții confidentiale și care sunt asigurate din punct de vedere tehnic, nu se vor instala telefoane, iar dacă instalarea acestora este absolut necesară, trebuie prevăzute cu un dispozitiv de deconectare pasiv.

(2) Inspecțiile de securitate tehnică în zonele prevăzute în alin.(I) trebuie efectuate, în mod obligatoriu, înaintea începerii con vorbirilor, pentru identificarea fizică a dispozitivelor de ascultare și verificarea sistemelor telefonice, electrice sau de altă natură, care ar putea fi utilizate ca mediu de atac.

Art. 139

(1) Echipamentele de comunicații și dotările din birouri, în principal cele electrice și electronice, trebuie verificate de specialiști ai autorităților desemnate de securitate competente, înainte de a fi folosite în zonele în care se lucrează ori se discută despre informații strict secrete sau strict secrete de importanță deosebită, pentru a preveni transmiterea sau interceptarea, în afara cadrului legal, a unor informații inteligibile.

(2) Pentru zonele menționate la alin. (1) se va organiza o evidență a tipului și numerelor de inventar ale echipamentului și mobilei mutate în/din interiorul încăperilor, care va fi gestionată ca material secret de stat.

SECȚIUNEA 5: Protecția personalului

Art. 140

(1) Unitățile deținătoare de informații secrete de stat au obligația de a asigura protecția personalului desemnat să asigure securitatea acestora ori care are acces la astfel de informații, potrivit prezentelor standarde.

(2) Măsurile de protecție a personalului au drept scop:

- a) să prevină accesul persoanelor neautorizate la informații secrete de stat;
- b) să garanteze că informațiile secrete de stat sunt distribuite deținătorilor de certificate de securitate/autorizații de acces, cu respectarea principiului necesității de a cunoaște;
- c) să permită identificarea persoanelor care, prin acțiunile sau inacțiunile lor, pot pune în pericol securitatea informațiilor secrete de stat și să prevină accesul acestora la astfel de informații.

(3) Protecția personalului se realizează prin: selecționarea, verificarea, avizarea și autorizarea accesului la informațiile secrete de stat, revalidarea, controlul și instruirea personalului, retragerea certificatului de securitate sau autorizației de acces.

Art. 141

(1) Acordarea certificatului de securitate - anexa nr. 12 - și autorizației de acces la informații clasificate - anexa nr. 13, potrivit nivelului de secretizare, este condiționată de avizul autoritații desemnate de securitate.

(2) În vederea eliberării certificatului de securitate/autorizației de acces conducătorul unității solicită în scris ORNISS, conform anexei nr. 14, efectuarea verificărilor de securitate asupra persoanei care urmează să aibă acces la informații secrete de stat.

(3) Solicitarea menționată la alin. (2) va fi însotită de formularele tip, prevăzute la anexele nr. 15, 16 și 17, potrivit nivelului de secretizare a informațiilor, completate de persoana în cauză, introduse în plic separat, sigilat.

(4) În funcție de avizul comunicat de autoritatea desemnată, ORNISS va aproba eliberarea certificatului de securitate sau autorizației de acces și va încunoștința oficial conducătorul unității.

(5) După obținerea aprobării menționate la alin. (4), conducătorul unității va notifica la ORNISS și va elibera certificatul de securitate sau autorizația de acces, conform art. 154.

Art. 142

Certificatul de securitate sau autorizația de acces se eliberează numai în baza avizelor acordate de autoritatea desemnată de securitate în urma verificărilor efectuate asupra persoanei în cauză, cu acordul scris al acesteia.

Art. 143

În cadrul procedurilor de avizare trebuie acordată atenție specială persoanelor care:

- a) urmează să aibă acces la informații strict secrete și strict secrete de importanță deosebită;
- b) ocupă funcții ce presupun accesul permanent la un volum mare de informații secrete de stat;
- c) pot fi vulnerabile la acțiuni ostile, ca urmare a importanței funcției în care vor fi numite, a mediului de relații sau a locului de muncă anterior.

Art. 144

(1) Oportunitatea avizării va fi evaluată pe baza verificării și investigării biograficii celui în cauză.

(2) Când persoanele urmează să îndeplinească funcții care le pot facilita accesul la informații secrete de stat doar în anumite circumstanțe - paznici, curieri, personal de întreținere - se va acorda atenție primei verificări de securitate.

Art. 145

Unitățile care gestionează informații clasificate sunt obligate să țină un registru de evidență a certificatelor de securitate și autorizațiilor de acces la informații clasificate - anexa nr. 18.

Art. 146

(1) Ori de câte ori apar indicii că deținătorul certificatului de securitate sau autorizației de acces nu mai îndeplinește criteriile de compatibilitate privind accesul la informațiile secrete de stat, verificările de securitate se reiau la solicitarea conducătorului unității adresată ORNISS.

(2) ORNISS poate solicita reluarea verificărilor, la sesizarea autorităților competente, în situația în care sunt semnalate incompatibilități privind accesul la informații secrete de stat

Art. 147

Procedura de verificare în vederea acordării accesului la informații secrete de stat are drept scop identificarea riscurilor de securitate, aferente gestionării informațiilor secrete de stat.

Art. 148

(1) Structura/funcționarul de securitate are obligația să pună la dispoziția persoanei selecționate formularile tip corespunzătoare nivelului de acces pentru care se solicită eliberarea certificatului de securitate/autorizației de acces și să acorde asistență în vederea completării acestora.

(2) În funcție de nivelul de secretizare a informațiilor pentru care se solicită avizul de securitate, termenele de prezentare a răspunsului de către instituțiile abilitate să efectueze verificările de securitate sunt:

- a) pentru acces la informații strict secrete de importanță deosebită - 90 de zile lucrătoare;
- b) pentru acces la informații strict secrete - 60 de zile lucrătoare;
- c) pentru acces la informații secrete - 30 de zile lucrătoare.

Art. 149

ORNISS are obligația ca, în termen de 7 zile lucrătoare de la primirea solicitării, să transmită ADS competente cererea tip de începere a procedurii de verificare - anexa nr. 19, la care va anexa plicul sigilat cu formularile tip completate

Art. 150

(1) După primirea formularelor, instituția abilitată va efectua verificările în termenele prevăzute la art. 148 și va comunica, în scris - anexa nr. 20, la ORNISS, avizul privind acordarea certificatului de securitate sau autorizației de acces la informații clasificate.

(2) În cazul în care sunt identificate riscuri de securitate, ADS va evalua dacă acestea constituie un impediment pentru acordarea avizului de securitate.

(3) În situația în care sunt semnalate elemente relevante din punct de vedere al protecției informațiilor secrete de stat, în luarea deciziei de acordare a avizului de securitate vor avea prioritate interesele de securitate.

Art. 151

(1) În termen de 7 zile lucrătoare de la primirea răspunsului de la autoritatea desemnată de securitate, ORNISS va decide asupra acordării certificatului de securitate/autorizației de acces la informații secrete de stat și va comunica unității solicitante - anexa nr. 21.

(2) Adresa de comunicare a deciziei ORNISS se realizează în trei exemplare, din care unul se transmite unității solicitante, iar al doilea instituției care a efectuat verificările.

(3) Dacă avizul este pozitiv, conducătorul unității solicitante va elibera certificatul de securitate sau autorizația de acces persoanei în cauză, după notificarea prealabilă la ORNTSS - anexa nr. 22

Art. 152

(1) Verificarea în vederea avizării pentru accesul la informații secrete de stat se efectuează cu respectarea legislației în vigoare privind responsabilitățile în domeniul protecției unor asemenea informații, de către următoarele instituții:

a) Serviciul Român de Informații, pentru:

- personalul propriu;
- personalul autorităților și instituțiilor publice din zona de competență, potrivit legii;
- personalul agenților economici cu capital integral sau parțial de stat și al persoanelor juridice de drept public sau privat, altele decât cele date în competență instituțiilor menționate la lit. b), c) și d);

b) Ministerul Apărării Naționale, pentru:

- personalul militar și civil propriu;
- personalul Oficiului Central de Stat pentru Probleme Speciale, Administrației Naționale a Rezervelor de Stat și altor persoane juridice stabilite prin lege și personalul militar care își desfășoară activitatea în străinătate;

c) Serviciul de Informații Externe, pentru:

- personalul militar sau civil propriu;
- personalul român al reprezentanțelor diplomatice, misiunilor permanente, consulare, centrelor culturale, organismelor internaționale și altor reprezentanțe ale statului român în străinătate;
- cetățenii români aflați în străinătate în cadrul unor contracte, stagii de perfecționare, programe de cercetare sau în calitate de angajați la firme;

d) Ministerul de Interne, Ministerul Justiției, Serviciul de Protecție și Pază și Serviciul de Telecomunicații Speciale, pentru personalul propriu și al persoanelor juridice a căror activitate o coordonează.

(2) Instituțiile menționate la alin. (1) sunt abilitate să solicite și să primească informații de la persoane juridice și fizice, în vederea acordării avizului de acces la informații clasificate.

Art. 153

Instituțiile competente în realizarea verificărilor de securitate cooperează, pe bază de protocoale, în îndeplinirea sarcinilor și obiectivelor propuse.

Art. 154

Certificatul de securitate/autorizația de acces se emite în două exemplare originale, unul fiind păstrat de structura/funcționarul de securitate, iar celălalt se trimite la ORNISS, care va informa instituția competentă care a efectuat verificările.

Art. 155

Valabilitatea certificatului de securitate/autorizației de acces eliberate unei persoane este de până la patru ani, în această perioadă verificările putând fi reluate oricând sunt îndeplinite condițiile prevăzute la art.167.

Art. 156

Pentru cadrele proprii, Ministerul Apărării Naționale, Ministerul de Interne, Ministerul Justiției, Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază vor elabora instrucțiuni interne privind verificarea, avizarea, eliberarea și evidența certificatelor de securitate/autorizațiilor de acces.

Art. 157

Decizia privind avizarea eliberării certificatului de securitate/autorizației de acces va fi luată pe baza tuturor informațiilor disponibile și va avea în vedere.

- a) loialitatea indisutabilă a persoanei;
- b) caracterul, obiceurile, relațiile și discreția persoanei, care să ofere garanții asupra:
 - corectitudinii în gestionarea informațiilor secrete de stat;
 - oportunității accesului neînsotit în compartimente, obiective, zone și locuri de securitate în care se află informații secrete de stat;
 - respectării reglementărilor privind protecția informațiilor secrete de stat din domeniul său de activitate.

Art. 158

(1) Principalele criterii de evaluare a compatibilității în acordarea avizului pentru eliberarea certificatului de securitate/autorizației de acces vizează atât trăsăturile de caracter, cât și situațiile sau împrejurările din care pot rezulta riscuri și vulnerabilități de securitate.

(2) Sunt relevante și vor fi luate în considerare, la acordarea avizului de securitate, caracterul, conduita profesională sau socială, concepțiile și mediul de viață al soțului/soției sau concubinului/concubinei persoanei solicitante.

Art. 159

Următoarele situații imputabile atât solicitantului, cât și soțului/soției sau concubinului/concubinei acestuia reprezintă elemente de incompatibilitate pentru acces la informații secrete de stat.

- a) dacă a comis sau a intentionat să comită, a fost complice, a complotat sau a instigat la comiterea de acte de spionaj, terorism, trădare ori alte infracțiuni contra siguranței statului;
- b) dacă a încercat, a susținut, a participat, a cooperat sau a sprijinit acțiuni de spionaj, terorism ori persoane suspectate de a se încadra în această categorie sau de a fi membre ale unor organizații ori puteri străine inamice ordinii de drept din țara noastră;
- c) dacă este sau a fost membru al unei organizații care a încercat, încearcă sau susține răsturnarea ordinii constituționale prin mijloace violente, subversive sau alte forme ilegale;
- d) dacă este sau a fost un susținător al vreunei organizații prevăzute la lit c), este sau a fost în relații apropiate cu membrii unor astfel de organizații într-o formă de natură să ridice suspiciuni temeinice cu privire la încrederea și loialitatea persoanei.

Art. 160

Constituie elemente de incompatibilitate pentru accesul solicitantului la informații secrete de stat oricare din următoarele situații:

- a) dacă în mod deliberat a ascuns, a interpretat eronat sau a falsificat informații cu relevanță în planul siguranței naționale ori a mințit în completarea formularelor tip sau în cursul interviului de securitate;
- b) are antecedente penale sau a fost sanționat contraventional pentru fapte care indică tendințe infracționale;
- c) are dificultăți financiare serioase sau există o discordanță semnificativă între nivelul său de trai și veniturile declarate;
- d) consumă în mod excesiv băuturi alcoolice ori este dependent de alcool, droguri sau de alte substanțe interzise prin lege care produc dependență;
- e) are sau a avut comportamente imorale sau deviații de comportament care pot genera riscul ca persoana să fie vulnerabilă la șantaj sau presiuni;
- f) a demonstrat lipsă de loialitate, necinste, incorectitudine sau indiscreție;
- g) a încălcăt reglementările privind protecția informațiilor clasificate;

h) suferă sau a suferit de boli fizice sau psihice care îi pot cauza deficiențe de discernământ confirmate prin investigație medicală efectuată cu acordul persoanei solicitante;

i) poate fi supus la presiuni din partea rudelor sau persoanelor apropiate care ar putea genera vulnerabilități exploataibile de către serviciile de informații ale căror interese sunt ostile României și aliaților săi.

Art. 161

(1) Solicitările pentru efectuarea verificărilor de securitate în vederea avizării eliberării certificatelor de securitate/autorizațiilor de acces la informații secrete vor avea în vedere persoanele care:

- a) în exercitarea atribuțiilor profesionale lucrează cu date și informații de nivel secret;
- b) fac parte din personalul de execuție sau administrativ și, în virtutea acestui fapt, pot intra în contact cu date și informații de acest nivel;
- c) este de presupus că vor lucra cu date și informații de nivel secret, datorită funcției pe care o dețin;
- d) se presupune că nu pot avansa profesional în funcție, dacă nu au acces la astfel de informații.

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

- a) verificarea corectitudinii datelor menționate în formularul de bază, anexa nr. 15;
- b) referințe de la locurile de muncă și din mediile frecventate, de la cel puțin trei persoane.

(3) În situația în care este necesară clarificarea anumitor aspecte sau la solicitarea persoanei verificate, reprezentantul instituției abilitate să efectueze verificările de securitate poate avea o întrevedere cu aceasta.

Art. 162

(1) Pentru eliberarea certificatelor de securitate/autorizațiilor de acces la informații strict secrete se efectuează verificări asupra persoanelor care:

- a) în exercitarea atribuțiilor profesionale lucrează cu date și informații de nivel strict secret;
- b) fac parte din personalul de execuție sau administrativ și, în virtutea acestui fapt, pot intra în contact cu date și informații de acest nivel;
- c) este de presupus că vor lucra cu date și informații de nivel strict secret, datorită funcției pe care o dețin;
- d) se presupune că nu pot avansa profesional în funcție, dacă nu au acces la astfel de informații.

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

- a) verificarea corectitudinii datelor personale menționate în formularul de bază și în formularul suplimentar, anexele nr. 15 și 16;
- b) referințe minime de la locurile de muncă și din mediile frecventate de la cel puțin trei persoane;
- c) verificarea datelor prezentate în formular, despre membrii de familie;
- d) investigații la locul de muncă și la domiciliu, care să acopere o perioadă de zece ani anteriori datei avizului sau începând de la vîrsta de 18 ani;
- e) un interviu cu persoana verificată, dacă se consideră că ar putea clarifica aspecte rezultate din verificările efectuate.

Art. 163

(1) Pentru eliberarea certificatelor de securitate/autorizațiilor de acces la informații strict secrete de importanță deosebită se efectuează verificări asupra persoanelor care:

a) în exercitarea atribuțiilor profesionale lucrează cu date și informații de nivel strict secret de importanță deosebită;

b) fac parte din personalul de execuție sau administrativ și, în virtutea acestui fapt, pot intra în contact cu informații de acest nivel.

(2) Avizarea accesului la informațiile strict secrete de importanță deosebită se va baza pe:

a) verificarea corectitudinii datelor menționate în formularul de bază, formularul suplimentar și formularul finanțier, anexele nr. 15, 16 și 17;

b) investigații de cunoaștere a conduitelor la domiciliul actual și cele anterioare, la locul de muncă actual și la cele anterioare, precum și la instituțiile de învățământ următoare, începând de la vîrstă de 18 ani, investigații care nu se vor limita la audierea persoanelor indicate de solicitantul avizului;

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

d) un interviu cu persoana solicitantă, pentru a detalia aspectele rezultate din verificările efectuate;

e) în cazul în care, din verificările întreprinse, rezultă incertitudini cu privire la sănătatea psihică sau comportamentul persoanei verificate, cu acordul acesteia poate fi supusă unui test psihologic.

Art. 164

(1) Dacă în cursul verificărilor, pentru orice nivel, apar informații ce evidențiază riscuri de securitate, se va realiza o verificare suplimentară, cu folosirea metodelor și mijloacelor specifice instituțiilor cu atribuții în domeniul siguranței naționale.

(2) În cazul verificării suplimentare menționate la alin. (1) termenele de efectuare a verificărilor vor fi prelungite în mod corespunzător.

Art. 165

În funcție de nivelul de secretizare a informațiilor secrete de stat la care se acordă accesul, investigația de cunoaștere a antecedentelor va avea în vedere, gradual, următoarele:

a) consultarea registrelor de stare civilă pentru verificarea datelor personale în vederea stabilirii, fără dubiu, a identității persoanei solicitante;

b) verificarea cazierului judiciar, în evidențele centrale și locale ale poliției, în baza de date a Registrului Comerțului, precum și în alte evidențe;

c) stabilirea naționalității persoanei și cetățeniei prezente și anterioare;

d) confirmarea pregătirii în școlile, universitățile și alte instituții de învățământ următoare de titular, de la împlinirea vîrstei de 18 ani;

e) cunoașterea conduitelor la locul de muncă actual și la cele anterioare, cu referințe obținute din dosarele de angajare, aprecierile anuale asupra performanțelor și eficienței activității, ori furnizate de șefii instituțiilor, șefii de compartimente sau colegi;

f) organizarea de interviuri și discuții cu persoane care pot face aprecieri asupra trecutului, activității, comportamentului și corectitudinii persoanei verificate;

g) cunoașterea comportării pe timpul serviciului militar și a modalității în care a fost trecut în rezervă; h) existența unor riscuri de securitate datorate unor eventuale presiuni exercitate din străinătate;

i) solvabilitatea și reputația financiară a persoanei;

j) stabilirea indicilor și obținerea de probe conform cărora persoana solicitantă este sau a fost membru ori afiliat al unei organizații, asociații, mișcări, grupări străine sau autohtone, care au sprijinit sau au susținut comiterea unor acte de violență, în scopul afectării drepturilor altor persoane, sau care încearcă să schimbe ordinea de stat prin mijloace neconstituționale.

Art. 166

(1) În cazul în care o persoană deține certificat de securitate/autorizație de acces la informații naționale clasificate, acesteia i se poate elibera și certificat de securitate pentru acces la informații NATO clasificate valabil pentru același nivel de secretizare sau pentru un nivel inferior.

(2) Dacă informațiile NATO clasificate la care se solicită acces în condițiile alin. (1) sunt de nivel superior celui pentru care persoana în cauză deține certificat de securitate/autorizație de acces se vor efectua verificările necesare, potrivit standardelor în vigoare.

(3) Valabilitatea certificatului/autorizației eliberate în condițiile alin. (1) și (2) încetează la expirarea termenului de valabilitate al certificatului/autorizației inițiale.

Art. 167

(1) Revalidarea avizului privind accesul la informații clasificate presupune reverificarea persoanei deținătoare a unui certificat de securitate/autorizație de acces în vederea menținerii sau retragerii acesteia

(2) Revalidarea poate avea loc la solicitarea unității în care persoana își desfășoară activitatea, sau a ORNISS, în oricare din următoarele situații:

- a) atunci când pentru îndeplinirea sarcinilor de serviciu ale persoanei deținătoare este necesar accesul la informații de nivel superior;
- b) la expirarea perioadei de valabilitate a certificatului de securitate/autorizației de acces deținute anterior;
- c) în cazul în care apar modificări în datele de identificare ale persoanei;
- d) la apariția unor riscuri de securitate din punct de vedere al compatibilității accesului la informații clasificate.

Art. 168

La solicitarea revalidării nu se eliberează un nou certificat de securitate/autorizație de acces, în următoarele situații:

- a) în cazul în care se constată neconcordanțe între datele declarate în formularele tip și cele reale;
- b) în cazul în care, pe parcursul perioadei de valabilitate a certificatului de securitate/autorizației de acces s-au evidențiat riscuri de securitate;
- c) în cazul în care ORNISS solicită acest lucru, în mod expres.

Art. 169

Pentru revalidarea accesului la informații secrete de stat se derulează aceleași activități ca și la acordarea avizului initial, verificările raportându-se la perioada scursă de la eliberarea certificatului de securitate sau autorizației de acces anterioare.

Art. 170

(1) Persoanele cărora li se eliberează certificate de securitate/autorizații de acces vor fi instruite, obligatoriu, cu privire la protecția informațiilor clasificate, înaintea începerii activității și ori de câte ori este nevoie.

(2) Activitatea de pregătire se efectuează planificat, în scopul prevenirii, contracarării și eliminării riscurilor și amenințărilor la adresa securității informațiilor clasificate.

(3) Pregătirea personalului se realizează diferențiat, potrivit nivelului de secretizare a informațiilor la care certificatul de securitate sau autorizația de acces permite accesul și va fi înscrisă în fișă individuală de pregătire, care se păstrează la structura/funcționarul de securitate.

(4) Toate persoanele încadrate în funcții care presupun accesul la informații clasificate trebuie să fie instruite temeinic, atât în perioada premergătoare numirii în funcție, cât și la intervale prestabilite, asupra necesității și modalităților de asigurare a protecției acestor informații.

(5) După fiecare instruire, persoana care deține certificat de securitate sau autorizație de acces va semna că a luat act de conținutul reglementărilor privind protecția informațiilor secrete de stat.

Art. 171

(1) Pregătirea personalului urmărește însușirea corectă a standardelor de securitate și a modului de implementare eficientă a măsurilor de protecție a informațiilor clasificate.

(2) Organizarea și coordonarea activității de pregătire a structurilor/funcționarilor de securitate sunt asigurate de autoritățile desemnate de securitate.

Art. 172

(1) Planificarea și organizarea activității de pregătire a personalului se realizează de către structura/funcționarul de securitate.

(2) Autoritățile desemnate de securitate vor controla, potrivit competențelor, modul de realizare a activității de pregătire a personalului care accesează informații secrete de stat.

Art. 173

(1) Pregătirea individuală a persoanelor care dețin certificate de securitate/autorizații de acces se realizează în raport cu atribuțiile profesionale.

(2) Toate persoanele care gestionează informații clasificate au obligația să cunoască reglementările privind proiecția informațiilor clasificate și procedurile interne de aplicare a măsurilor de securitate specifice.

Art. 174

(1) Pregătirea personalului se realizează sub formă de lecții, informări, prelegeri, simpozioane, schimb de experiență, seminarii, ședințe cu caracter aplicativ și se poate finaliza prin verificări sau certificări ale nivelului de cunoștințe.

(2) Activitățile de pregătire vor fi organizate de structura/funcționarul de securitate, conform tematicilor cuprinse în programele aprobate de conducerea unității.

Art. 175

Certificatul de securitate sau autorizația de acces își încetează valabilitatea și se va retrage în următoarele cazuri:

- a) la solicitarea ORNISS;
- b) prin decizia conducerii unității care a eliberat certificatul/autorizația;
- c) la solicitarea autorității desemnate de securitate competente;
- d) la plecarea din unitate sau la schimbarea locului de muncă al deținătorului în cadrul unității, dacă noul loc de muncă nu presupune lucru cu astfel de informații secrete de stat,
- e) la schimbarea nivelului de acces.

Art. 176

La retragerea certificatului de securitate sau autorizației de acces, în cazurile prevăzute la art. 175 lit. a)-d), angajatului i se va interzice accesul la informații secrete de stat, iar conducerea unității va notifica despre aceasta la ORNISS.

Art. 177

După luarea deciziei de retragere, unitatea va solicita ORNISS înapoierea exemplarului 2 al certificatului de securitate sau al autorizației de acces, după care va distrugе ambele exemplare, pe bază de proces-verbal.

SECȚIUNEA 6: Accesul cetățenilor străini, al cetățenilor români care au și cetățenia altui stat, precum și al persoanelor apărătoare la informațiile secrete de stat și în locurile în care se desfășoară activități, se expun obiecte sau se execută lucrări din această categorie

Art. 178

Cetățenii străini, cetățenii români care au și cetățenia altui stat, precum și persoanele apărătoare pol avea acces la informații secrete de stat, cu respectarea principiului necesității de a cunoaște și a convențiilor, protocolelor, contractelor și altor înțelegeri încheiate în condițiile legii.

Art. 179

(1) Persoanele prevăzute la art. 178 vor fi verificate și avizate conform prezentelor standarde, la solicitarea conducerii unității în cadrul căreia acestea urmează să desfășoare activități care presupun accesul la informații secrete de stat.

(2) Conducătorul unității va elibera persoanelor respective o autorizație de acces corespunzătoare nivelului de secretizare a informațiilor la care urmează să aibă acces, valabilă numai pentru perioada desfășurării activităților comune, în baza acordului comunicat de ORNISS.

Art. 180

(1) Persoanele prevăzute la art. 178 care desfășoară activități de asistență tehnică, consultanță, colaborare științifică ori specializare vor purta ecusoane distincte față de cele folosite de personalul propriu și vor fi însotite permanent de persoane anume desemnate de conducerea unității respective.

(2) Conducătorul unității este obligat să delimitizeze strict sectoarele și compartimentele în care persoanele menționate la art. 178 pot avea acces și va stabili măsuri pentru prevenirea prezenței acestora în alte locuri în care se gestionează informații secrete de stat.

Art. 181

(1) Structura/funcționarul de securitate are obligația de a instrui persoanele prevăzute la art. 178 în legătură cu regulile pe care trebuie să le respecte privind proiecția informațiilor secrete de stat.

(2) Autorizația de acces se va elibera numai după însușirea reglementărilor privind protecția informațiilor clasificate și semnarea angajamentului de confidențialitate.

Art. 182

Nerespectarea de către persoanele prevăzute la art. 178 a regulilor privind protecția informațiilor clasificate va determina, obligatoriu, retragerea autorizației de acces.

CAPITOLUL V: CONDIȚIILE DE FOTOGRAFIERE, FILMARE, CARTOGRAFIERE ȘI EXECUȚARE A UNOR LUCRĂRI DE ARTE PLASTICE ÎN OBIECTIVE SAU LOCURI CARE PREZINTĂ IMPORTANȚĂ DEOSEBITĂ PENTRU PROTECȚIA INFORMAȚIILOR SECRETE DE STAT

Art. 183

(1) Este interzisă fotografierea, filmarea, cartografierea sau executarea de lucrări de arte plastice pe teritoriul României, în obiective, zone sau locuri de importanță deosebită 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 ministriilor sau conducatorilor institutiilor respective, pentru obiectivele, zonele sau locurile din competenta lor.

Art. 184

Trupele Ministerului Apărării Naționale, Ministerului de Interne și Serviciului Român de Informații, aflate la instrucție, în aplicații ori în interiorul obiectivelor prevazute la art. 17 din Legea nr. [182/2002](#), pot fi fotografiate sau filmate în scopuri educative și de pregătire militară, cu aprobarea conducătorilor acestor instituții sau a împuternicitorilor desemnați.

Art. 185

Fotografierea, filmarea, cartografierea sau executarea de lucrări de arte plastice în zonele de securitate și administrative ale unităților deținătoare de secrete de stat este permisă numai cu aprobarea scrisă a împuternicitorilor abilitați să atribuie niveluri de secretizare conform art. 19 din Legea [182/2002](#), potrivit competențelor materiale.

Art. 186

(1) Cererea adresată ORNISS pentru eliberarea autorizației speciale de filmare, fotografiere, cartografiere sau de executare a lucrărilor de arte plastice va cuprinde, obligatoriu, menționarea obiectului și locului activității, aparatura folosită, perioada de timp în care urmează a se realiza, datele de identitate ale persoanei care le va efectua, precum și aprobarea prevăzută la art. 185.

(2) Termenul de răspuns va fi de 60 de zile lucrătoare de la data primirii cererii.

(3) Titularii autorizației speciale sunt obligați să se prezinte, înaintea începerii lucrărilor, la conducătorii institutiilor unde acestea vor fi executate, pentru a se pune de acord cu privire la modalitatea de acțiune și verificarea aparaturii ce va fi folosită.

Art. 187

Dacă solicitantul posedă autorizatia de nivel corespunzător obiectivului vizat, autorizatia speciala va fi eliberata in termen de 15 zile lucrătoare de la data primirii solicitării, cu respectarea principiului nevoii de a cunoaște.

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 interdicție in acest sens, care vor fi instalate prin grija institutiilor cărora le aparțin, cu avizul de specialitate al organelor administrației publice locale.

Art. 189

(1) Emiterea, deținerea sau folosirea de date și documente geodezice, topo-fotogrammetrice și cartografice, ce constituie secrete de stat, urmează, în privința clasificării, marcării, inscripționării, procesării, manipulării, evidenței, întocmirii, multiplicării, transmiterii, păstrării, transportului și distrugerii acestora, regimul prevăzut de reglementările în vigoare privitoare la protecția informatiilor clasificate în România.

(2) Ministerele și celealte organe ale administrației publice centrale și locale, care întocmesc documente geodezice, topo-fotogrammetrice și cartografice cu caracter secret de stat, le vor nominaliza în liste proprie de informații clasificate, potrivit dispozițiilor legale în vigoare.

Art. 190

Aerofotografierea și aerofilmarea se vor efectua obligatoriu în prezența reprezentantului Ministerului Apărării Naționale, care, la încheierea acțiunilor, va prelua și va prelucra negativele, cu consultarea autorităților desemnate de securitate, și va prezenta materialul prelucrat la ORNISS, în vederea predării lui beneficiarilor.

CAPITOLUL VI: EXERCITAREA CONTROLULUI ASUPRA MĂSURILOR PRIVITOARE LA PROTECȚIA INFORMAȚIILOR CLASIFICATE

Art. 191

(1) Serviciul Român de Informații, prin unitatea sa specializată, are competență generală de exercitare a controlului asupra modului de aplicare a măsurilor de protecție de către instituțiile publice și unitățile deținătoare de informații clasificate.

(2) Activitatea de control în cadrul Ministerului Apărării Naționale, Ministerului de Interne, Ministerului de Justiție, Serviciului Român de Informații, Serviciului de Informații Externe, Serviciului de Protecție și Pază și Serviciului de Telecomunicații Speciale se reglementează prin ordine ale conducerilor acestor instituții, potrivit legii.

(3) Controlul privind măsurile de protecție a informațiilor clasificate în cadrul Parlamentului, Administrației Prezidențiale, Guvernului și Consiliului Suprem de Apărare a Țării se organizează conform legii.

(4) Activitatea de control în cadrul reprezentanțelor României în străinătate se reglementează și se realizează de către Serviciul de Informații Externe.

Art. 192

Controlul are ca scop:

a) evaluarea eficienței măsurilor concrete de protecție adoptate la nivelul deținătorilor de informații clasificate, în conformitate cu legea, cu prevederile prezentelor standarde și altor norme în materie, precum și cu programele de prevenire a surgerii de informații clasificate;

b) identificarea vulnerabilităților existente în sistemul de protecție a informațiilor clasificate, care ar putea conduce la compromiterea acestor informații, în vederea luării măsurilor de prevenire necesare;

c) luarea măsurilor de remediere a deficiențelor și de perfecționare a cadrului organizatoric și funcțional la nivelul structurii controlate;

d) constatarea cazurilor de nerespectare a normelor de protecție a informațiilor clasificate și aplicarea sancțiunilor contraventionale sau, după caz, sesizarea organelor de urmărire penală, în situația în care fapta constituie infracțiune;

e) informarea Consiliului Suprem de Apărare a Țării și Parlamentului cu privire la modul în care unitățile deținătoare de informații clasificate aplică reglementările în materie.

Art. 193

(1) Fiecare acțiune de control se încheie printr-un document de constatare, întocmit de echipa/persoana care 1-a efectuat.

(2) în cazul în care controlul relevă fapte și disfuncționalități de natură să reprezinte riscuri majore de securitate pentru protecția informațiilor clasificate va fi informat, de îndată, Consiliul Suprem de Apărare a Țării, iar instituția controlată va dispune măsuri imediate de remediere a deficiențelor constatate, va iniția cercetarea administrativă și, după caz, va aplica măsurile sancționatorii și va sesiza organele de urmărire penală, în situația în care rezultă indicii că s-ar fi produs infracțiuni.

Art. 194

În funcție de obiectivele urmărite, controalele pot fi:

- a) controale de fond, care urmăresc verificarea întregului sistem organizatoric, structural și funcțional de protecție a informațiilor clasificate;
- b) controale tematice, care vizează anumite domenii ale activității de protecție a informațiilor clasificate;
- c) controale în situații de urgență, care au ca scop verificarea unor aspecte punctuale, stabilitatea ca urmare a identificării unui risc de securitate.

Art. 195

În funcție de modul în care sunt stabilite și organizate, controalele pot fi:

- a) planificate;
- b) inopinate;
- c) determinate de situații de urgență.

Art. 196

Conducătorii unităților care fac obiectul controlului au obligația să pună la dispoziția echipelor de control toate informațiile solicitate privind modul de aplicare a măsurilor prevăzute de lege pentru protecția informațiilor clasificate.

Art. 197

Conducătorii unităților deținătoare de informații clasificate au obligația să organizeze anual și ori de câte ori este nevoie controale interne privind gestionarea acestora.

CAPITOLUL VII: SECURITATEA INDUSTRIALĂ

SECȚIUNEA 1: Dispoziții generale

Art. 198

Prevederile prezentului capitol se vor aplica tuturor persoanelor juridice de drept public sau privat care desfășoară ori solicită să desfășoare activități contractuale ce presupun accesul la informații clasificate.

SECȚIUNEA 2: Atribuțiile Oficiului Registrului Național al Informațiilor Secrete de Stat și ale autorităților desemnate de securitate în domeniul protecției informațiilor clasificate care fac obiectul activităților contractuale

Art. 199

În domeniul protecției informațiilor clasificate care fac obiectul activităților contractuale, ORNISS are următoarele atribuții:

- a) stabilește strategia de implementare unitară la nivel național a măsurilor de protecție a informațiilor clasificate care fac obiectul activităților contractuale;
- b) eliberează autorizația și certificatul de securitate industrială, la cererea persoanelor juridice interesate;
- c) gestionează, la nivel național, evidențele privind: persoanele juridice deținătoare de autorizații de securitate industrială; persoanele juridice deținătoare de certificate de securitate industrială; persoanele fizice care dețin certificate de securitate sau autorizații de acces eliberate în scopul negocierii sau executării unui contract clasificat.

Art. 200

În sfera lor de competență legală, autoritățile desemnate de securitate au următoarele atribuții:

- a) efectuează verificările de securitate necesare acordării avizului de securitate industrială, pe care îl transmite la ORNISS în vederea eliberării autorizației sau, după caz, a certificatului de securitate industrială;
- b) asigură asistență de specialitate obiectivelor industriale în vederea implementării standardelor de securitate în domeniul protecției informațiilor clasificate vehiculate în cadrul activităților industriale;
- c) desfășoară activități de pregătire a personalului cu atribuții pe linia protecției informațiilor clasificate, vehiculate în cadrul activităților industriale;
- d) efectuează verificări în situațiile în care s-au semnalat încălcări ale reglementărilor de protecție, distrugeri, dispariții, dezvăluiri neautorizate de informații clasificate, furnizate sau produse în cadrul unui contract clasificat;
- e) se asigură că fiecare obiectiv industrial, în cadrul căruia urmează să fie gestionate informații clasificate, a desemnat o structură/funcționar de securitate în vederea exercitării efective a atribuțiilor pe linia protecției acestora, în cadrul contractelor clasificate;
- f) monitorizează, în condițiile legii, modul de asigurare a protecției informațiilor clasificate în procesul de negociere și derulare a contractelor, iar în cazul în care constată factori de risc și vulnerabilități, informează imediat ORNISS și propune măsurile necesare;
- g) avizează programele de prevenire a surgerii informațiilor clasificate din obiectivele industriale, anexele de securitate ale contractelor clasificate și monitorizează respectarea prevederilor acestora;
- h) efectuează controale de securitate și informează ORNISS asupra concluziilor rezultate;
- i) verifică și prezintă ORNISS propunerile de soluționare a sesizărilor, reclamațiilor și observațiilor referitoare la modul de aplicare și respectare a standardelor de protecție în cadrul contractelor clasificate.

SECȚIUNEA 3: Protecția informațiilor clasificate care fac obiectul activităților contractuale

Art. 201

- (1) Clauzele și procedurile de protecție vor fi stipulate în anexa de securitate a fiecărui contract clasificat, care presupune acces la informații clasificate.
- (2) Anexa de securitate prevăzută la alin. (1) va fi întocmită de partea contractantă deținătoare de informații clasificate ce vor fi utilizate în derularea contractului clasificat.
- (3) Clauzele și procedurile de protecție vor fi supuse, periodic, inspecțiilor și verificărilor de către autoritatea desemnată de securitate competentă.

Art. 202

Partea contractantă deținătoare de informații clasificate ce vor fi utilizate în derularea unui contract este responsabilă pentru clasificarea și definirea tuturor componentelor acestuia, în conformitate cu normele în vigoare, sens în care poate solicita sprijin de la ADS, conform competențelor materiale stabilite prin lege.

Art. 203

La clasificarea contractelor se vor aplica următoarele reguli generale:

- a) în toate stadiile de planificare și execuție, contractul se clasifică pe niveluri corespunzătoare, în funcție de conținutul informațiilor;
- b) clasificările se aplică numai acelor părți ale contractului care trebuie protejate;

- c) când în derularea unui contract se folosesc informații din mai multe surse, cu niveluri de clasificare diferite, contractul va fi clasificat în funcție de nivelul cel mai înalt al informațiilor, iar măsurile de protecție vor fi stabilite în mod corespunzător;
- d) declasificarea sau trecerea la o altă clasă sau nivel de secretizare a unei informații din cadrul contractului se aprobă de conducătorul persoanei juridice care a autorizat clasificarea inițială.

Art. 204

În cazul în care apare necesitatea protejării informațiilor dintr-un contract care, anterior, nu a fost necesar a fi clasificat, contractorul are obligația declanșării procedurilor de clasificare și protejare conform reglementărilor în vigoare.

Art. 205

În cazul în care contractantul cedează unui subcontractant realizarea unei părți din contractul clasificat, se va asigura că acesta deține autorizație sau certificat de securitate industrială și este obligat să înștiințeze contractorul, iar la încheierea subcontractului să prevadă clauze și proceduri de protecție în conformitate cu prevederile prezentelor standarde.

Art. 206

- (1) În procesul de negociere a unui contract clasificat pot participa doar reprezentanți autorizați ai obiectivelor industriale care dețin autorizație de securitate industrială eliberată de către ORNISS, care va ține evidența acestora.
- (2) Autorizațiile de securitate industrială se eliberează pentru fiecare contract clasificat în parte.
- (3) În cazul în care obiectivul industrial nu deține autorizații de securitate industrială pentru participarea la negocierea aceluia contract, este obligatorie inițierea procedurii de autorizare.

Art. 207

(1) Invitațiile la licitații sau prezentări de oferte, în cazul contractelor clasificate, trebuie să conțină o clauză prin care potențialul ofertant este obligat să înapoieze documentele clasificate care i-au fost puse la dispoziție, în cazul în care nu depune oferta până la data stabilită sau nu câștigă competiția într-un termen precizat de organizator, care să nu depășească 15 zile de la comunicarea rezultatului.

(2) În situațiile menționate la alin. (1), ofertantul care a pierdut licitația are obligația să păstreze confidențialitatea informațiilor la care a avut acces

Art. 208

Contractorul păstrează evidența tuturor participanților la întâlnirile de negociere, datele de identificare ale acestora și angajamentele de confidențialitate, organizațiile pe care le reprezintă, tipul și scopul întâlnirilor, precum și informațiile la care aceștia au avut acces.

Art. 209

Contractanții care intenționează să deruleze activități industriale cu subcontractanți sunt obligați să respecte procedurile prevăzute în acest capitol.

Art. 210

Contractantul și subcontractanții sunt obligați să implementeze și să respecte toate măsurile de protecție a informațiilor clasificate puse la dispoziție sau care au fost generate pe timpul derulării contractelor.

Art. 211

Autoritățile desemnate de securitate vor verifica, potrivit competențelor, dacă obiectivul industrial îndeplinește următoarele cerințe:

- a) posedă structură/funcționar de securitate responsabilă cu protecția informațiilor clasificate care fac obiectul activităților contractuale;

- b) asigură sprijinul necesar pentru efectuarea inspecțiilor de securitate periodice, pe întreaga durată a contractului clasificat;
- c) nu permite diseminarea, fără autorizație scrisă din partea emitentului, a nici unei informații clasificate ce i-a fost încredințată în cadrul derulării unui contract clasificat;
- d) aproba accesul la informațiile vehiculate în cadrul contractului clasificat numai persoanelor care dețin certificat de securitate sau autorizație de acces, în conformitate cu principiul necesității de a cunoaște;
- e) dispune de posibilitățile necesare pentru a informa asupra oricărei compromiteri, divulgări, distrugeri, sustrageri, sabotaje sau activități subversive ori altor riscuri la adresa securității informațiilor clasificate vehiculate sau a persoanelor angajate în derularea contractului respectiv și orice schimbări privind proprietatea, controlul sau managementul obiectivului industrial cu implicații asupra statutului de securitate al acestuia;
- f) impune subcontractanților obligații de securitate similare cu cele aplicate contractantului;
- g) nu utilizează în alte scopuri decât cele specifice contractului informațiile clasificate la care are acces, fără permisiunea scrisă a emitentului;
- h) înapoiază toate informațiile clasificate ce i-au fost încredințate, precum și pe cele generate pe timpul derulării contractului, cu excepția cazului în care asemenea informații au fost distruse autorizat sau păstrarea lor a fost autorizată de către contractor pentru o perioadă de timp strict determinată,
- i) respectă procedura stabilită pentru protecția informațiilor clasificate legate de contract.

Art. 212

După adjudecarea contractului clasificat, contractantul are obligația de a informa ORNISS, în vederea inițierii procedurii de obținere a certificatului de securitate industrială.

Art. 213

Contractul clasificat va putea fi pus în executare numai în condițiile în care:

- a) ORNISS a emis certificatul de securitate industrială;
- b) au fost eliberate certificate de securitate sau autorizații de acces pentru persoanele care, în îndeplinirea sarcinilor ce le revin, necesită acces la informații secrete de stat;
- c) personalul autorizat al contractantului a fost instruit asupra reglementărilor de securitate industrială de către structura/funcționarul de securitate și a semnat fișa individuală de pregătire.

SECȚIUNEA 4: Procedura de verificare, avizare și certificare a obiectivelor industriale care negociază și derulează contracte clasificate

Art. 214

Verificarea, avizarea și eliberarea autorizației și certificatului de securitate industrială reprezintă ansamblul procedural de securitate ce se aplică numai obiectivelor industriale care au sau vor avea acces la informații clasificate în cadrul contractelor sau subcontractelor secrete de stat, încheiate cu deținătorii unor astfel de informații.

Art. 215

(1) Pentru participarea la negocieri în vederea încheierii unui contract clasificat, conducătorul obiectivului industrial adresează ORNISS o cerere pentru eliberarea autorizației de securitate industrială - anexa nr. 24, la care anexează chestionarul de securitate industrială - anexa nr. 25.

(2) După obținerea avizului de la autoritatea desemnată de securitate competentă, ORNISS eliberează autorizația de securitate industrială - anexa nr. 28.

(3) Evidența autorizațiilor de securitate industrială eliberate potrivit alin. (2) se realizează conform anexei nr. 31.

Art. 216

(1) Pentru derularea contractelor clasificate, ORNISS eliberează obiectivelor industriale, certificate de securitate industrială - anexa nr.29.

(2) Procedura de avizare a eliberării certificatului de securitate industrială se realizează pe baza cererii pentru eliberarea certificatului de securitate industrială - anexa nr. 30, chestionarului de securitate - anexele nr. 26 și 27 și a copiei anexei de securitate menționată la art. 201.

(3) ORNISS va ține evidența certificatelor de securitate industrială potrivit anexei nr. 32.

Art. 217

Activitatea de verificare în vederea eliberării autorizației și a certificatelor de securitate trebuie să asigure îndeplinirea următoarelor obiective principale:

- a) prevenirea accesului persoanelor neautorizate la informații clasificate,
- b) garantarea că informațiile clasificate sunt distribuite pe baza existenței certificatului de securitate industrială și a principiului necesității de a cunoaște;
- c) identificarea persoanelor care, prin acțiunile lor, pot pune în pericol protecția informațiilor clasificate și interzicerea accesului acestora la astfel de informații;
- d) garantarea faptului că obiectivele industriale au capacitatea de a proteja informațiile clasificate în procesul de negociere, respectiv de derulare a contractului.

Art. 218

(1) Pentru a se elibera autorizația și certificatul de securitate, obiectivul industrial trebuie să îndeplinească următoarele cerințe:

- a) să posede program de prevenire a scurgerii de informații clasificate, avizat conform reglementărilor în vigoare;
- b) să fie stabil din punct de vedere economic;
- c) să nu fi înregistrat o greșală de management cu implicații grave asupra stării de securitate a informațiilor clasificate pe care le gestionează;
- d) să fi respectat obligațiile de securitate din cadrul contractelor clasificate derulate anterior;
- e) personalul implicat în derularea contractului să dețină certificat de securitate de nivel egal cu celui al informațiilor vehiculate în cadrul contractului clasificat.

(2) Neîndeplinirea cerințelor menționate la alin. (1), precum și furnizarea intenționată a unor informații inexacte în completarea chestionarului sau în documentele prezentate în vederea certificării constituie elemente de incompatibilitate în procesul de eliberare a autorizației sau certificatului de securitate industrială.

Art. 219

Obiectivul industrial nu este considerat stabil din punct de vedere economic dacă:

- a) este în proces de lichidare;
- b) este în stare de faliment ori se află în procedura reorganizării judiciare sau a falimentului;
- c) este implicat într-un litigiu care îi afectează stabilitatea economică;
- d) nu își îndeplinește obligațiile financiare către stat;
- e) nu și-a îndeplinit la timp, în mod sistematic, obligațiile financiare către persoane fizice sau juridice.

Art. 220

(1) Un obiectiv industrial nu corespunde din punct de vedere al protecției informațiilor clasificate dacă se constată că prezintă riscuri de securitate. (2) Sunt considerate riscuri de securitate

- a) derularea unor activități ce contravin intereselor de siguranță națională sau angajamentelor pe care România și le-a asumat în cadrul acordurilor bilaterale sau multinaționale;
- b) relațiile cu persoane fizice sau juridice străine ce ar putea aduce prejudicii intereselor statului român;
- c) asociațiile, persoane fizice și juridice, care pot reprezenta factori de risc pentru interesele de stat ale României.

Art. 221

(1) Pentru eliberarea autorizației sau certificatului de securitate industrială, solicitantul va transmite la ORNISS următoarele documente:

- a) cererea de eliberare a autorizației, respectiv a certificatului de securitate industrială,
- b) chestionam! de securitate completat, introdus într-un plic separat, sigilat.

(2) Pentru eliberarea certificatului de securitate industrială, solicitantul va atașa și o copie a anexei de securitate.

Art. 222

În termen de 7 zile lucrătoare de la primirea cererii, ORNISS va solicita autorității desemnate de securitate competente să efectueze verificările de securitate.

Art. 223

Avizul de securitate eliberat de autoritatea desemnată de securitate competentă trebuie să garanteze că:

- a) agentul economic nu prezintă riscuri de securitate;
- b) sunt aplicate în mod corespunzător măsurile de securitate fizică, prevăzute de reglementările în vigoare, precum și normele privind accesul persoanelor la informații clasificate;
- c) obiectivul industrial este solvabil din punct de vedere finanțiar,
- d) obiectivul industrial nu a fost și nu este implicat sub nici o formă în activitatea unor organizații, asociații, mișcări, grupări de persoane străine sau autohtone care au adoptat sau adoptă o politică de sprijinire sau aprobare a comiterii de acte de sabotaj, subversive sau teroriste.

Art. 224

Verificările de securitate se realizează astfel:

- a) verificarea de securitate de nivel I - pentru eliberarea avizului necesar autorizației de securitate industrială;
- b) verificarea de securitate de nivel II - pentru eliberarea avizului necesar certificatului de securitate industrială de nivel secret;
- c) verificarea de securitate de nivel III - pentru eliberarea avizului necesar certificatului de securitate industrială de nivel strict secret;
- d) verificarea de securitate de nivel IV - pentru eliberarea avizului necesar certificatului de securitate industrială de nivel strict secret de importanță deosebită.

Art. 225

În cadrul verificării de securitate se desfășoară următoarele activități:

- (1) Pentru verificările de securitate de nivel I:

- a) verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială, conform anexei nr. 25;
- b) verificarea modului de aplicare a prevederilor programului de prevenire a surgerii de informații clasificate;
- c) evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociați/acționari, administratori, persoanele din comitetul director și structura de securitate - ori executivă implicată în negocierea contractului clasificat;
- d) verificarea datelor minime referitoare la bonitatea și stabilitatea economică a obiectivului industrial - domeniu și obiect de activitate, statut juridic, acționari, garanții bancare.

(2) Pentru verificările de securitate de nivel II:

- a) verificarea corectitudinii dalelor consemnate în chestionarul de securitate industrială - anexa nr. 26;
- b) evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociați/acționari, administratori, persoanele din comitetul director și structura de securitate - ori executivă implicată în derularea contractului clasificat;
- c) verificarea unor date minime referitoare la bonitatea și stabilitatea economică a obiectivului industrial - domeniu și obiect de activitate, statut juridic, acționari, garanții bancare;
- d) verificarea modului de implementare și de aplicare a normelor și măsurilor de securitate fizică, de securitate a personalului și a documentelor, prevăzute pentru nivelul secret.

(3) Pentru verificarea de securitate de nivel III:

- a) verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială - anexa nr. 27;
- b) evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociați/acționari, administratori, persoanele din comitetul director și structura de securitate - ori executivă implicată în derularea contractului clasificat, precum și a celor desemnate să participe la activitățile de negociere a acestuia;
- c) verificarea datelor referitoare la bonitatea și stabilitatea economică a agentului economic - domeniu și obiect de activitate, statut juridic, acționari, garanții bancare - incluzând și aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;
- d) verificarea existenței autorizării sistemului informatic și de comunicații propriu, pentru nivelul strict secret;
- e) verificarea modului de implementare și de aplicare a normelor și măsurilor de securitate fizică, de securitate a personalului și a documentelor, prevăzute pentru nivelul strict secret,
- f) discuții cu proprietarii, membrii consiliului director, funcționarii de securitate, angajații, în vederea clarificării datelor rezultate din chestionar, după caz.

(4) Pentru verificarea de securitate de nivel IV:

- a) verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială - anexa nr. 27;
- b) evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociați/acționari, administratori, persoanele din comitetul director și structura de securitate - ori executivă implicată în derularea contractului clasificat;
- c) verificarea informațiilor detaliate referitoare la bonitatea și stabilitatea economică a agentului economic - domeniu și obiect de activitate, statut juridic, acționari, garanții bancare - incluzând și aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;
- d) verificarea existenței autorizării sistemului informatic și de comunicații propriu, pentru nivel strict secret de importanță deosebită;

e) verificarea modului de implementare și de aplicare a normelor și măsurilor de securitate fizică, de securitate a personalului și a documentelor, prevăzute pentru nivelul strict secret de importanță deosebită;

f) discuții cu proprietarii, membrii consiliului director, funcționarii de securitate, angajații, în vederea clarificării datelor rezultate din chestionar, după caz.

Art. 226

În cazul unui obiectiv industrial la al cărui management/accionariat participă cetăteni străini, cetăteni români care au și cetătenia altui stat sau/și persoane apatride, ORNISS, împreună cu ADS competentă, va evalua măsura în care interesul străin ar putea reprezenta o amenințare la adresa protecției informațiilor secrete de stat, care vor fi încredințate aceluia obiectiv industrial.

Art. 227

În îndeplinirea sarcinilor și obiectivelor ce le revin, pe linia protecției informațiilor clasificate, ADS competente cooperează pe baza protoalelor ce vor fi încheiate între ele cu avizul ORNISS.

Art. 228

În vederea desfășurării procedurilor de avizare, obiectivul industrial are obligația de a permite accesul reprezentanților ADS în sediile, la echipamentele, operațiunile și la alte activități, respectiv de a prezenta documentele necesare și de a furniza, la cerere, alte date și informații.

Art. 229

(1) Dacă în urma verificării de securitate se constată că sunt îndeplinite cerințele de securitate necesare asigurării protecției la nivelul de clasificare corespunzător informațiilor vehiculate în cadrul contractului clasificat, ORNISS eliberează și transmite obiectivului industrial autorizația sau certificatul de securitate industrială.

(2) Dacă se constată că obiectivul industrial nu îndeplinește condițiile de securitate necesare, ORNISS nu eliberează autorizația sau certificatul de securitate industrială și informează obiectivul industrial în acest sens. ORNISS nu este obligat să prezinte motivele refuzului. Refuzul eliberării autorizației sau certificatului de securitate industrială va fi comunicat și la ADS care a efectuat verificările de securitate.

(3) Când sunt semnalate elemente care nu constituie riscuri, dar sunt relevante din punct de vedere al securității, în luarea deciziei de eliberare a autorizației sau certificatului de securitate industrială vor avea prioritate interesele de securitate.

Art. 230

În termen de 7 zile lucrătoare de la primirea avizului de securitate din partea autoritaților desemnate de securitate, ORNISS va elibera autorizația sau certificatul de securitate industrială ori, după caz, va comunica obiectivului industrial refuzul eliberării acestora.

Art. 231

Obiectivul industrial are obligația de a comunica ORNISS toate modificările survenite privind datele de securitate incluse în chestionarul completat, pe întreaga durată de valabilitate a autorizației sau certificatului de securitate industrială.

Art. 232

Termenele pentru eliberarea autorizației sau certificatului de securitate industrială sunt:

- a) pentru autorizația de securitate industrială - 60 de zile lucrătoare;
- b) pentru certificat de securitate industrială de nivel secret - 90 de zile lucrătoare;
- c) pentru certificat de securitate industrială de nivel strict secret - 120 de zile lucrătoare;
- d) pentru certificat de securitate industrială de nivel strict secret de importanță deosebită - 180 de zile lucrătoare.

Art. 233

(1) Autorizația de securitate are valabilitate până la încheierea contractului sau până la retragerea de la negocieri.

(2) Dacă în perioada menționată la alin. (1) contractul clasificat care a făcut obiectul negocierilor este adjudecat, contractantul este obligat să solicite la ORNISS eliberarea certificatului de securitate industrială.

(3) Termenul de valabilitate al certificatului de securitate industrială este determinat de perioada derulării contractului clasificat, dar nu mai mult de 3 ani, după care contractantul este obligat să solicite revalidarea acestuia.

Art. 234

În situația în care ORNISS decide retragerea autorizației sau certificatului de securitate industrială va însțiința contractantul, contractorul și autoritatea desemnată de securitate competentă.

Art. 235

Autorizația sau certificatul de securitate industrială se retrage de ORNISS în următoarele cazuri:

- a) la solicitarea obiectivului industrial;
- b) la propunerea motivată a autorității desemnate de securitate competente;
- c) la expirarea termenului de valabilitate;
- d) la încetarea contractului;
- e) la schimbarea nivelului de certificare acordat inițial.

CAPITOLUL VIII: PROTECȚIA SURSELOR GENERATOARE DE INFORMAȚII - INFOSEC

SECȚIUNEA 1: Dispoziții generale

Art. 236

Modalitățile și măsurile de protecție a informațiilor clasificate care se prezintă în format electronic sunt similare celor pe suport de hârtie.

Art. 237

Termenii specifici, folosiți în prezentul capitol, cu aplicabilitate în domeniul INFOSEC, se definesc după cum urmează:

- INFOSEC - ansamblul măsurilor și structurilor de protecție a informațiilor clasificate care sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatiche de comunicații și al altor sisteme electronice, împotriva amenințărilor și a oricărora acțiuni care pot aduce atingere confidențialității, integrității, disponibilității autenticității și nerepudierii informațiilor clasificate precum și afectarea funcționării sistemelor informatiche, indiferent dacă acestea apar accidental sau intenționat. Măsurile INFOSEC acoperă securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografică, precum și depistarea și prevenirea amenințărilor la care sunt expuse informațiile și sistemele;

- informațiile în format electronic - texte, date, imagini, sunete, înregistrate pe dispozitive de stocare sau pe suporturi magnetice, optice, electrice ori transmise sub formă de curenți, tensiuni sau câmp electromagnetic, în eter sau în rețele de comunicații;

- sistemul de prelucrare automată a datelor - SPAD - ansamblul de elemente interdependente în care se includ: echipamentele de calcul, produsele software de bază și aplicative, metodele, procedeele și, dacă este cazul, personalul, organizate astfel încât să asigure îndeplinirea funcțiilor de stocare, prelucrare automată și transmitere a informațiilor în format electronic, și

care se află sub coordonarea și controlul unei singure autorități. Un SPAD poate să cuprindă subsisteme, iar unele dintre acestea pot fi ele însăși SPAD;

- componente specifice de securitate ale unui SPAD, necesare asigurării unui nivel corespunzător de protecție pentru informațiile clasificate care urmează a fi stocate sau procesate într-un SPAD, sunt:

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

- retele de transmisii de date - RTD - ansamblul de elemente interdependente în care se includ: echipamente, programe și dispozitive de comunicație, tehnică de calcul hardware și software, metode și proceduri pentru transmisie și recepție de date și controlul rețelei, precum și, dacă este cazul, personalul aferent. Toate acestea sunt organizate astfel încât să asigure îndeplinirea funcțiilor de transmisie a informațiilor în format electronic între două sau mai multe SPAD sau să permită interconectarea cu alte RTD-uri. O RTD poate utiliza serviciile unuia sau mai multor sisteme de comunicații; mai multe RTD pot utiliza serviciile unuia și acelaiași sistem de comunicații.

Caracteristicile de securitate ale unei RTD cuprind: caracteristicile de securitate ale sistemelor SPAD individuale conectate, împreună cu toate componente și facilități asociate rețelei - facilități de comunicații ale rețelei, mecanisme și proceduri de identificare și etichetare, controlul accesului, programe și proceduri de control și revizie - necesare pentru a asigura un nivel corespunzător de protecție pentru informațiile clasificate, care sunt transmise prin intermediul RTD;

- RTD locală - rețea de transmisii de date care interconectează mai multe computere sau echipamente de rețea, situate în același perimetru;
- sistemul informatic și de comunicații - SIC ansamblu informatic prin intermediul căruia se stochează, se procesează și se transmit informații în format electronic, alcătuit din cel puțin un SPAD, izolat sau conectat la o RTD. Poate avea o configurație complexă, formată din mai multe SPAD-uri și/sau RTD-uri interconectate,
- securitatea SPAD, RTD și SIC - aplicarea măsurilor de securitate la SPAD și RTD - SIC cu scopul de a preveni sau împiedica extragerea sau modificarea informațiilor clasificate stocate, procesate, transmise prin intermediul acestora - prin interceptare, alterare, distrugere, accesare neautorizată cu mijloace electronice, precum și invalidarea de servicii sau funcții, prin mijloace specifice,
- confidențialitatea - asigurarea accesului la informații clasificate numai pe baza certificatului de securitate al persoanei, în acord cu nivelul de secretizare a informației accesate și a permisiunii rezultate din aplicarea principiului nevoii de a cunoaște;
- integritatea - interdicția modificării - prin ștergere sau adăugare - ori a distrugerii în mod neautorizat a informațiilor clasificate;
- disponibilitatea - asigurarea condițiilor necesare regăsirii și folosirii cu ușurință, ori de câte ori este nevoie, cu respectarea strictă a condițiilor de confidențialitate și integritate a informațiilor clasificate;

- autenticitatea - asigurarea posibilității de verificare a identității pe care un utilizator de SPAD sau RTD pretinde că o are;
- nerepudierea - măsură prin care se asigură faptul că, după emiterea/recepționarea unei informații într-un sistem de comunicații securizat, expeditorul/destinatarul nu poate nega, în mod fals, că a expediat/primit informații;
- risc de securitate - probabilitatea ca o amenințare sau o vulnerabilitate ale SPAD sau RTD - SIC să se materializeze în mod efectiv;
- managementul de risc - are ca scop identificarea, controlul și minimizarea riscurilor de securitate și este o activitate continuă de stabilire și menținere a unui nivel de securitate în domeniul tehnologiei informației și comunicațiilor - TIC - într-o unitate, în sensul că, pornind de la analiza de risc, identifică și evaluează amenințările și vulnerabilitățile și propune aplicarea măsurilor adecvate de contracarare, proiectate la un preț de cost corelat cu consecințele care ar decurge din divulgarea, modificarea sau ștergerea informațiilor care trebuie protejate,
- regula celor doi - obligativitatea colaborării a două persoane pentru îndeplinirea unei activități specifice;
- produs informatic de securitate - componentă de securitate care se încorporează într-un SPAD sau RTD - SIC și care servește la sporirea sau asigurarea confidențialității, integrității, disponibilității, autenticității și nerepudierii informațiilor stocate, procesate sau transmise;
- securitatea calculatoarelor - COMPUSEC - aplicarea la nivelul fiecărui calculator a facilităților de securitate hardware, software și firmware, pentru a preveni divulgarea, manevrarea, modificarea sau ștergerea neautorizată a informațiilor clasificate ori invalidarea neautorizată a unor funcții;
- securitatea comunicațiilor - COMSEC - aplicarea măsurilor de securitate în telecomunicații, cu scopul de a proteja mesajele dintr-un sistem de telecomunicații, care ar putea fi interceptate, studiate, analizate și, prin reconstituire, pot conduce la dezvăluiri de informații clasificate.

COMSEC reprezintă ansamblul de proceduri, incluzând:

- a) măsuri de securitate a transmisiilor;
 - b) măsuri de securitate împotriva radiațiilor - TEMPEST;
 - c) măsuri de acoperire criptologică;
 - d) măsuri de securitate fizică, procedurală, de personal și a documentelor;
 - e) măsuri COMPUSEC;
- TEMPEST - ansamblul măsurilor de testare și de realizare a securității împotriva surgerii de informații, prin intermediul emisiilor electomagnetic parazite;
 - evaluarea - examinarea detaliată, din punct de vedere tehnic și funcțional, a aspectelor de securitate ale SPAD și RTD - SIC sau a produselor de securitate, de către o autoritate abilitată în acest sens.

Prin procesul de evaluare se verifică:

- a) prezența facilităților/funcțiilor de securitate cerute;
- b) absența efectelor secundare compromițătoare care ar putea decurge din implementarea facilităților de securitate;
- c) funcționalitatea globală a sistemului de securitate;
- d) satisfacerea cerințelor de securitate specifice pentru un SPAD și RTD - SIC,
- e) stabilirea nivelului de încredere al SPAD sau RTD - SIC ori al produselor informatic de securitate implementate;
- f) existența performanțelor de securitate ale produselor informatic de securitate instalate în SPAD sau RTD - SIC;

- certificarea - emiterea unui document de constatare, la care se atașează unul de analiză, în care sunt prezentate modul în care a decurs evaluarea și rezultatele acesteia, în documentul de constatare se menționează măsurile în care SPAD și RTD - SIC satisfac cerințele de securitate, precum și măsura în care produsele informative de securitate răspund exigențelor referitoare la protecția informațiilor clasificate în format electronic;

- acreditarea - etapa de acordare a autorizației și aprobării unui SPAD sau RTD - SIC de a prelucra informații clasificate, în spațiul/mediul operațional propriu.

Etapa de acreditare trebuie să se desfășoare după ce s-au implementat toate procedurile de securitate și după ce s-a atins un nivel suficient de protecție a resurselor de sistem. Acreditarea se face, în principal, pe baza CSS și include următoarele:

a) notă justificativă despre obiectivul acreditării sistemului, nivel/nivelurile de clasificare a informațiilor care urmează să fie procesate și vehiculate, modul/modurile de operare protejată propuse;

b) notă justificativă despre managementul riscurilor - modul de tratare, gestionare și rezolvare a riscurilor - în care se specifică pericolele și punctele vulnerabile, precum și măsurile adecvate de contracarare a acestora;

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

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

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

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

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

- zona terminal/stație de lucru la distanță - reprezintă o zonă, separată de zona SPAD, în care se găsesc:

a) elemente de tehnică de calcul;

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

c) echipamente de comunicații;

- amenințarea - posibilitatea de compromitere accidentală sau deliberată a securității SPAD sau RTD - SIC, prin pierderea confidențialității, a integrității sau disponibilității informațiilor în format electronic sau prin afectarea funcțiilor care asigură autenticitatea și nerepudierea informațiilor;

- vulnerabilitatea - slăbiciune sau lipsă de control care ar putea permite sau facilita o manevră tehnică, procedurală sau operațională, prin care se amenință o valoare sau întă specifică.

Art. 238

Abrevierile utilizate în prezentul capitol semnifică:

a) CSTIC- componenta de securitate pentru tehnologia informației și comunicațiilor instituită în unitățile deținătoare de informații clasificate;

b) TIC - tehnologia informației și comunicațiilor;

c) CSS - cerințele de securitate specifice.

Art. 239

(1) Informațiile care se prezintă în format electronic pot fi:

- a) stocate și procesate în cadrul SPAD sau transmise prin intermediul RTD;
 - b) stocate și transportate prin intermediul suporturilor de memorie, dispozitivelor electronice - cipuri de memorie, hârtie perforată sau alte suporturi specifice.
- (2) Încărcarea informațiilor pe mediile prevăzute în alin.(I) lit.b, precum și interpretarea lor pentru a deveni inteligibile, se face cu ajutorul echipamentelor electronice specializate.

Art. 240

(1) Sistemele SPAD și RTD - SIC au dreptul să stocheze, să proceseze sau să transmită informații clasificate, numai dacă sunt autorizate potrivit prezentei hotărâri.

(2) În vederea autorizării SPAD și RTD - SIC unitățile vor întocmi, cu aprobarea organelor lor de conducere, strategia proprie de securitate, în baza căreia vor implementa sisteme proprii de securitate, care vor include utilizarea de produse specifice tehnologiei informației și comunicațiilor, personal instruit și măsuri de protecție a informației, inclusiv controlul accesului la sistemele și serviciile informatiche și de comunicații, pe baza principiului necesității de a cunoaște și al nivelului de secretizare atribuit.

(3) SPAD și RTD - SIC vor fi supuse procesului de acreditare, urmat de evaluări periodice, în vederea menținerii acreditării.

Art. 241

(1) Aplicarea reglementărilor în vigoare referitoare la protecția informațiilor clasificate în format electronic funcționează unitar la nivel național. Sistemul de emitere și implementare a măsurilor de securitate adresate protecției informațiilor clasificate care sunt stocate, procesate sau transmise de SPAD sau RTD - SIC, precum și controlul modului de implementare a măsurilor de securitate se realizează de către o structură funcțională cu atribuții de reglementare, control și autorizare, care include:

- a) o agenție pentru acordarea acreditării de funcționare în regim de securitate;
- b) o agenție care elaborează și implementează metode, mijloace și măsuri de securitate;
- c) o agenție responsabilă cu protecția criptografică.

(2) Agențile menționate la alin. (1) sunt subordonate instituției desemnate la nivel național, pentru protecția informațiilor clasificate, ORNISS.

(3) Măsurile de protecție a informațiilor clasificate în format electronic trebuie reactualizate permanent, prin depistare, documentare și gestionare a amenințărilor și vulnerabilităților la adresa informațiilor clasificate și sistemelor care le prelucreză, stochează și transmit.

Art. 242

Măsurile de securitate INFOSEC vor fi structurate după nivelul de clasificare al informațiilor pe care le protejează și în conformitate cu conținutul acestora.

Art. 243

Conducătorul unității deținătoare de informații clasificate răspunde de securitatea propriilor informații care sunt stocate, procesate sau transmise în SPAD sau RTD - SIC.

Art. 244

(1) În fiecare unitate care administrează SPAD și RTD -SIC în care se stochează, se procesează sau se transmit informații clasificate, se va institui o componentă de securitate pentru tehnologia informației și a comunicațiilor - CSTIC, în subordinea structurii/funcționarului de securitate.

(2) în funcție de volumul de activitate și dacă cerințele de securitate permit, atribuțiile CSTIC pot fi îndeplinite numai de către funcționarul de securitate TIC sau pot fi preluate, în totalitate, de către structura/funcționarul de securitate din unitate.

(3) CSTIC îndeplinește atribuții privind:

- a) implementarea metodelor, mijloacelor și măsurilor necesare protecției informațiilor în format electronic;
- b) exploatarea operațională a SPAD și RTD - SIC în condiții de securitate;
- c) coordonarea cooperării dintre unitatea deținătoare a SPAD sau RTD - SIC și autoritatea care asigură acreditarea;
- d) implementarea măsurilor de securitate și protecția criptografică ale SPAD sau RTD - SIC.

(4) CSTIC reprezintă punctul de contact al agenților competente cu unitățile care dețin în administrare SPAD sau RTD-SIC și, după caz, poate fi investită, temporar, de către aceste agenții, cu unele dintre atribuțiile lor.

(5) Propunerile pe linie de securitate avansate de către CSTIC devin operaționale numai după ce au fost aprobată de către conducerea unității care deține în administrare respectivul SPAD sau RTD - SIC.

Art. 245

CSTIC se institue la nivelul fiecărei SPAD și RTD - SIC și reprezintă persoana sau compartimentul cu responsabilitatea delegată de către agenția de securitate pentru informatică și comunicații de a implementa metodele, mijloacele și măsurile de securitate și de a exploata SPAD și RTD - SIC în condiții de securitate.

Art. 246

CSTIC este condusă de către funcționarul de securitate TIC și are în compunere administratorii de securitate și, după caz, și alți specialiști din SPAD sau RTD - SIC. Toată structura CSTIC face parte din personalul unității care administrează SPAD sau RTD - SIC.

Art. 247

Exercitarea atribuțiilor CSTIC trebuie să cuprindă întregul ciclu de viață al SPAD sau RTD -SIC, începând cu proiectarea, continuând cu elaborarea specificațiilor, testarea instalării, acreditarea, testarea periodică în vederea reacreditării, exploatarea operațională, modificarea și încheind cu scoaterea din uz. În anumite situații, rolul CSTIC poate fi preluat de către alte componente ale unității, în decursul ciclului de viață.

Art. 248

CSTIC mijlocește cooperarea dintre conducerea unității căreia îi aparține SPAD sau RTD - SIC și agenția pentru acreditare de securitate, atunci când unitatea:

- a) planifică dezvoltarea sau achiziția de SPAD sau RTD;
- b) propune schimbări ale unei configurații de sistem existente;
- c) propune conectarea unui SPAD sau a unei RTD - SIC cu un alt SPAD sau RTD - SIC;
- d) propune schimbări ale modului de operare de securitate ale SPAD sau RTD - SIC;
- e) propune schimbări în programele existente sau utilizarea de noi programe, pentru optimizarea securității SPAD sau RTD - SIC;
- f) inițiază proceduri de modificare a nivelului de clasificare a SPAD și RTD - SIC care au fost deja acreditate;
- g) planifică sau propune întreprinderea oricărei alte activități referitoare la îmbunătățirea securității SPAD sau RTD - SIC deja acreditate.

Art. 249

CSTIC, cu aprobarea autorității de acreditare de securitate, stabilește standardele și procedurile de securitate care trebuie respectate de către furnizorii de echipamente, pe parcursul dezvoltării, instalării și testării SPAD și RTD - SIC și răspunde pentru justificarea, selecția, implementarea și controlul componentelor de securitate, care constituie parte a SPAD și RTD - SIC.

Art. 250

CSTIC stabilește, pentru structurile de securitate și management ale SPAD și RTD - SIC, încă de la înființare, responsabilitățile pe care le vor exercita pe tot ciclul de viață al SPAD și RTD - SIC respective.

Art. 251

Activitatea INFOSEC din SPAD și RTD - SIC, desfășurată de către CSTIC, trebuie condusă și coordonată de persoane care dețin certificat de securitate corespunzător, cu pregătire de specialitate în domeniul sistemelor TIC precum și al securității acestora, obținută în instituții de învățământ acreditate INFOSEC, sau care au lucrat în domeniu cel puțin 5 ani.

Art. 252

Protecția SPAD și RTD - SIC din compunerea sistemelor de armament și de detecție va fi definită în contextul general al sistemelor din care acestea fac parte și va fi realizată prin aplicarea prevederilor prezenterelor standarde.

SECȚIUNEA 2: Structuri organizatorice cu atribuții specifice în domeniul INFOSEC

A. Agenția de acreditare de securitate

Art. 253

Agenția de acreditare de securitate este subordonată instituției desemnate la nivel național pentru protecția informațiilor clasificate, are reprezentanți delegați din cadrul ADS implicate, în funcție de SPAD și RTD - SIC care trebuie acreditate, și îndeplinește următoarele atribuții principale:

- a) asigură, la nivel național, acreditarea de securitate și reacreditarea SPAD și RTD - SIC care stochează, procesează sau transmit informații clasificate, în funcție de nivelul de clasificare a acestora;
- b) asigură evaluarea și certificarea sistemelor SPAD și RTD - SIC sau a unor elemente componente ale acestora;
- c) stabilește criteriile de acreditare de securitate pentru SPAD și RTD - SIC.

Art. 254

Agenția de acreditare de securitate își exercită atribuțiile în domeniul INFOSEC în numele instituției desemnate la nivel național pentru protecția informațiilor clasificate și are responsabilitatea de a impune standarde de securitate în acest domeniu.

B. Agenția de securitate pentru informatică și comunicații

Art. 255

Agenția de securitate pentru informatică și comunicații este structura subordonată instituției desemnate la nivel național pentru protecția informațiilor electronice clasificate, având reprezentanți delegați din cadrul ADS implicate care acționează la nivel național.

Art. 256

Agenția este responsabilă de conceperea și implementarea mijloacelor, metodelor și măsurilor de protecție a informațiilor clasificate care sunt stocate, procesate sau transmise prin intermediul SPAD și RTD - SIC și are, în principal, următoarele atribuții:

- a) coordonează activitățile de protecție a informațiilor clasificate care sunt stocate, procesate sau transmise prin intermediul SPAD și RTD - SIC;
- b) elaborează și promovează reglementări și standarde specifice;
- c) analizează cauzele incidentelor de securitate și gestionează baza de date privind amenințările și vulnerabilitățile din sistemele de comunicație și informatică, necesare pentru elaborarea managementului de risc;
- d) semnalează agenției de acreditare de securitate incidentele de securitate în domeniu;
- e) integrează măsurile privind protecția fizică, de personal, a documentelor administrative, COMPUSEC, COMSEC, TEMPEST și criptografică,
- f) execută inspecții periodice asupra SPAD și RTD - SIC în vederea reacreditării;
- g) supune certificării și autorizării sistemele de securitate specifice SPAD și RTD - SIC.

Art. 257

Pentru îndeplinirea atribuțiilor sale, agenția de securitate pentru informatică și comunicații cooperează cu agenția de acreditare de securitate, cu agenția de protecție criptografică și cu alte structuri cu atribuții în domeniu.

C. Agenția de protecție criptografică

Art. 258

Agenția de protecție criptografică se organizează la nivel național, este subordonată instituției desemnate la nivel național pentru protecția informațiilor clasificate și are următoarele atribuții principale:

- a) asigură managementul materialelor și echipamentelor criptografice;
- b) realizează distribuirea materialelor și echipamentelor criptografice;
- c) raportează instituției desemnate la nivel național pentru protecția informațiilor clasificate incidentele de securitate cu care s-a confruntat;
- d) cooperează cu agenția de acreditare de securitate, cu agenția de concepere și implementare a metodelor, mijloacelor și măsurilor de securitate și cu alte structuri cu atribuții în domeniu.

SECȚIUNEA 3: Măsuri, cerințe și moduri de operare

A. Măsuri și cerințe specifice INFOSEC

Art. 259

- (1) Măsurile de protecție a informațiilor clasificate în format electronic se aplică sistemelor SPAD și RTD - SIC care stochează, procesează sau transmit asemenea informații.
- (2) Unitățile deținătoare de informații clasificate au obligația de a stabili și implementa un ansamblu de măsuri de securitate a sistemelor SPAD și RTD - SIC - fizice, de personal, administrative, de tip TEMPEST și criptografic.

Art. 260

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

B. Cerințe de securitate specifice SPAD și RTD - SIC

Art. 261

(1) Cerințele de securitate specifice - CSS se constituie într-un document încheiat între agenția de acreditare de securitate și CSTIC, ce va cuprinde principii și măsuri de securitate care trebuie să stea la baza procesului de certificare și acreditare a SPAD sau RTD - SIC.

(2) CSS se elaborează pentru fiecare SPAD și RTD - SIC care stochează, procesează sau transmite informații clasificate, sunt stabilite de către CSTIC și aprobată de către agenția de acreditare de securitate.

Art. 262

CSS vor fi formulate încă din faza de proiectare a SPAD sau RTD - SIC și vor fi dezvoltate pe tot ciclul de viață al sistemului.

Art. 263

CSS au la bază standardele naționale de protecție, parametrii esențiali ai mediului operațional, nivelul minim de autorizare a personalului, nivelul de clasificare a informațiilor gestionate și modul de operare a sistemului care urmează să fie acreditat.

C. Moduri de operare

Art. 264

SPAD și RTD - SIC care stochează, procesează sau transmit informații clasificate vor fi certificate și acreditate să opereze, pe anumite perioade de timp, în unul din următoarele moduri de operare:

- a) dedicat;
- b) de nivel înalt;
- c) multi-nivel.

Art. 265

(1) în modul de operare dedicat, toate persoanele cu drept de acces la SPAD sau la RTD trebuie să aibă certificat de securitate pentru cel mai înalt nivel de clasificare a informațiilor stocate, procesate sau transmise prin aceste sisteme. Necesitatea de a cunoaște pentru aceste persoane se stabilește cu privire la toate informațiile stocate, procesate sau transmise în cadrul SPAD sau RTD - SIC.

(2) în acest mod de operare, principiul necesității de a cunoaște nu impune o separare a informațiilor în cadrul SPAD sau RTD, ca mijloc de securitate a SIC. Celealte măsuri de protecție prevăzute vor asigura îndeplinirea cerințelor impuse de cel mai înalt nivel de clasificare a informațiilor gestionate și de toate categoriile de informații cu destinație specială stocate, procesate sau transmise în cadrul SPAD sau RTD.

Art. 266

(1) în modul de operare de nivel înalt, toate persoanele cu drept de acces la SPAD sau la RTD SIC trebuie să aibă certificat de securitate pentru cel mai înalt nivel de clasificare a informațiilor stocate, procesate sau transmise în cadrul SPAD sau RTD - SIC, iar accesul la informații se va face diferențiat, conform principiului necesității de a cunoaște.

(2) Pentru a asigura accesul diferențiat la informații, conform principiului necesității de a cunoaște, se instituie facilități de securitate care să asigure un acces selectiv la informații în cadrul SPAD sau RTD - SIC.

(3) Celelalte măsuri de protecție vor satisface cerințele pentru cel mai înalt nivel de clasificare și pentru toate categoriile de informații cu destinație specială stocate, procesate, transmise în cadrul SPAD sau RTD - SIC.

(4) Toate informațiile stocate, procesate sau vehiculate în cadrul unui SPAD sau RTD - SIC în acest mod de operare vor fi protejate ca informații cu destinație specială, având cel mai înalt nivel de clasificare care a fost constatat în mulțimea informațiilor stocate, procesate sau vehiculate prin sisteme.

Art. 267

(1) În modul de operare multi-nivel, accesul la informațiile clasificate se face diferențiat, potrivit principiului necesității de a cunoaște, conform următoarelor reguli:

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

(2) Aplicarea regulilor prevăzute la alin. (1) impune instituirea, în compensație, a unor facilități de securitate care să asigure un mod selectiv, individual, de acces la informațiile clasificate din cadrul SPAD sau RTD -SIC.

D. Administratorii de securitate

Art. 268

(1) Securitatea SPAD a rețelei și a obiectivului SIC se asigură prin funcțiile de administrator de securitate.

(2) Administratorii de securitate sunt:

- a) administratorul de securitate al SPAD;
- b) administratorul de securitate al rețelei;
- c) administratorul de securitate al obiectivului SIC.

(3) Funcțiile de administratori de securitate trebuie să asigure îndeplinirea atribuțiilor CSTIC. Dacă este cazul, aceste funcții pot fi cumulate de către un singur specialist.

Art. 269

(1) CSTIC desemnează un administrator de securitate al SPAD responsabil cu supervizarea dezvoltării, implementării și administrării măsurilor de securitate dintr-un SPAD, inclusiv participarea la elaborarea procedurilor operaționale de securitate.

(2) La recomandarea autorității de acreditare de securitate, CSTIC poate desemna structuri de administrare ale SPAD care îndeplinesc aceleași atribuții.

Art. 270

Administratorul de securitate al rețelei este desemnat de CSTIC pentru un SIC de mari dimensiuni sau în cazul interconectării mai multor SPAD și îndeplinește atribuții privind managementul securității comunicațiilor.

Art. 271

(1) Administratorul de securitate al obiectivului SIC este desemnat de CSTIC sau de autoritatea de securitate competentă și răspunde de asigurarea implementării și menținerea măsurilor de securitate aplicabile obiectivului SIC respectiv.

(2) Responsabilitățile unui administrator de securitate al obiectivului SIC pot fi îndeplinite de către structura/funcționarul de securitate al unității, ca parte a îndatoririlor sale profesionale.

(3) Obiectivul SIC reprezintă un amplasament specific sau un grup de amplasamente în care funcționează un SPAD și/sau RTD. Responsabilitățile și măsurile de securitate pentru fiecare zonă de amplasare a unui terminal/stație de lucru care funcționează la distanță trebuie explicit determinate.

E. Utilizatorii și vizitatorii

Art. 272

(1) Toți utilizatorii de SPAD sau RTD - SIC poartă responsabilitatea în ce privește securitatea acestor sisteme - raportate, în principal, la drepturile acordate și sunt îndrumați de către administratorii de securitate

(2) Utilizatorii vor fi autorizați pentru clasa și nivelul de secretizare a informațiilor clasificate stocate, procesate sau transmise în SPAD sau RTD - SIC. La acordarea accesului la informații, individual, se va urmări respectarea principiului necesității de a cunoaște.

(3) Informarea și conștientizarea utilizatorilor asupra îndatoririlor lor de securitate trebuie să asigure o eficacitate sporită a sistemului de securitate.

Art. 273

Vizitatorii trebuie să aibă autorizare de securitate de nivel corespunzător și să îndeplinească principiul necesității de a cunoaște, în situația în care accesul unui vizitator fără autorizare de securitate este considerat necesar, vor fi luate măsuri de securitate suplimentare pentru ca acesta să nu poată avea acces la informațiile clasificate.

SECȚIUNEA 4: Componentele EVFOSEC

A. Securitatea personalului

Art. 274

(1) Utilizatorii SPAD și RTD - SIC sunt autorizați și li se permite accesul la informații clasificate pe baza principiului necesității de a cunoaște și în funcție de nivelul de clasificare a informațiilor stocate, procesate sau transmise prin aceste sisteme.

(2) Unitățile deținătoare de informații clasificate în format electronic au obligația de a institui măsuri speciale pentru instruirea și supravegherea personalului, inclusiv a personalului de proiectare de sistem care are acces la SPAD și RTD, în vederea prevenirii și înălțării vulnerabilităților față de accesarea neautorizată.

Art. 275

În proiectarea SPAD și RTD - SIC trebuie să se aibă în vedere ca atribuirea sarcinilor și răspunderilor personalului să se facă în aşa fel încât să nu existe o persoană care să aibă cunoștință sau acces la toate programele și cheile de securitate - parole, mijloace de identificare personală.

Art. 276

Procedurile de lucru ale personalului din SPAD și RTD - SIC trebuie să asigure separarea între operațiunile de programare și cele de exploatare a sistemului sau rețelei. Este interzis, cu

excepția unor situații speciale, ca personalul să facă atât programarea, cât și operarea sistemelor sau rețelelor și trebuie instituite proceduri speciale pentru depistarea acestor situații.

Art. 277

Pentru orice fel de modificare aplicată unui sistem SPAD sau RTD - SIC este obligatorie colaborarea a cel puțin două persoane - regula celor doi. Procedurile de securitate vor menționa explicit situațiile în care regula celor doi trebuie aplicată.

Art. 278

Pentru a asigura implementarea corectă a măsurilor de securitate, personalul SPAD și RTD -SIC și personalul care răspunde de securitatea acestora trebuie să fie instruit și informat astfel încât să își cunoască reciproc atribuțiile.

B. Securitatea fizică

Art. 279

Zonele în care sunt amplasate SPAD și/sau RTD - SIC și cele cu terminale la distanță, în care sunt prezentate, stocate, procesate sau transmise informații clasificate ori în care este posibil accesul potențial la astfel de informații, se declară zone de securitate clasa I sau clasa II ale obiectivului și se supun măsurilor de protecție fizică stabilite prin prezentele standarde.

Art. 280

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

- a) intrarea personalului și a materialelor, precum și plecarea în/din aceste zone sunt controlate prin mijloace bine stabilite;
- b) zonele și locurile în care securitatea SPAD sau RTD - SIC sau a terminalelor la distanță poate fi modificată nu trebuie să fie niciodată ocupate de un singur angajat autorizat;
- c) persoanelor care solicită acces temporar sau cu intermitențe în aceste zone trebuie să li se autorizeze accesul, ca vizitatori, de către responsabilul pe probleme de securitate al zonei, desemnat de către administratorul de securitate al obiectivului SIC. Vizitorii vor fi însotiti permanent, pentru a avea garanția că nu pot avea acces la informații clasificate și nici la echipamentele utilizate.

Art. 281

În funcție de riscul de securitate și de nivelul de secretizare al informațiilor stocate, procesate și transmise, se impune cerința de aplicare a regulii de lucru cu două persoane și în alte zone, ce vor fi stabilite în stadiul inițial al proiectului și prezentate în cadrul CSS.

Art. 282

Când un SPAD este exploatat în mod autonom, deconectat în mod permanent de alte SPAD, ținând cont de condițiile specifice, de alte măsuri de securitate, tehnice sau procedurale și de rolul pe care îl are respectivul SPAD în funcționarea de ansamblu a sistemului, agenția de acreditare de securitate trebuie să stabilească măsuri specifice de protecție, adaptate la structura acestui SPAD, conform nivelului de clasificare a informațiilor gestionate.

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

Art. 283

Toate informațiile și materialele care privesc accesul la un SPAD sau RTD - SIC sunt controlate și protejate prin reglementări corespunzătoare nivelului de clasificare cel mai înalt și specificului informațiilor la care respectivul SPAD sau RTD - SIC permite accesul.

Art. 284

Când nu mai sunt utilizate, informațiile și materialele de control specificate la articolul precedent trebuie să fie distruse conform prevederilor prezentelor standarde.

D. Securitatea informațiilor clasificate în format electronic

Art. 285

Informațiile clasificate în format electronic trebuie să fie controlate conform regulilor INFOSEC, înainte de a fi transmise din zonele SPAD și RTD - SIC sau din cele cu terminale la distanță.

Art. 286

Modul în care este prezentată informația în clar, chiar dacă se utilizează codul prescurtat de transmisie sau reprezentarea binară ori alte forme de transmitere la distanță, nu trebuie să influențeze nivelul de clasificare acordat informațiilor respective.

Art. 287

Când informațiile sunt transferate între diverse SPAD sau RTD - SIC, ele trebuie să fie protejate atât în timpul transferului, cât și la nivelul sistemelor informatic ale beneficiarului, corespunzător cu nivelul de clasificare al informațiilor transmise.

Art. 288

Toate mediile de stocare a informațiilor se păstrează într-o modalitate care să corespundă celui mai înalt nivel de clasificare a informațiilor stocate sau suportilor, fiind protejate permanent.

Art. 289

Copierea informațiilor clasificate situate pe medii de stocare specifice TIC se execută în conformitate cu prevederile din procedurile operaționale de securitate.

Art. 290

Mediile refolosibile de stocare a informațiilor utilizate pentru înregistrarea informațiilor clasificate își mențin cea mai înaltă clasificare pentru care au fost utilizate anterior, până când respectivelor informații li se reduce nivelul de clasificare sau sunt declasificate, moment în care mediile susmenționate se reclasifică în mod corespunzător sau sunt distruse în conformitate cu prevederile procedurilor operaționale de securitate.

E. Controlul și evidența informațiilor în format electronic

Art. 291

(1) Evidența automată a accesului la informațiile clasificate în format electronic se ține în registrele de acces și trebuie realizată necondiționat prin software.

(2) Registrele de acces se păstrează pe o perioadă stabilită de comun acord între agenția de acreditare de securitate și CSTIC.

(3) Perioada minimă de păstrare a registrelor de acces la informațiile strict secrete de importanță deosebită este de 10 ani, iar a registrelor de acces la informațiile strict secrete și secrete, de cel puțin 3 ani.

Art. 292

(1) Mediile de stocare care conțin informații clasificate utilizate în interiorul unei zone SPAD pot fi manipulate ca unic material clasificat, cu condiția ca materialul să fie identificat, marcat cu nivelul său de clasificare și controlat în interiorul zonei SPAD, până în momentul în care este distrus, redus la o copie de arhivă sau pus într-un dosar permanent.

(2) Evidențele acestora vor fi menținute în cadrul zonei SPAD până când sunt supuse controlului sau distruse, conform prezentelor standarde.

Art. 293

În cazul în care un mediu de stocare este generat într-un SPAD sau RTD - SIC, iar apoi este transmis într-o zonă cu terminal/stație de lucru la distanță, se stabilesc proceduri adecvate de securitate, aprobate de către agenția de acreditare de securitate. Procedurile trebuie să cuprindă și instrucțiuni specifice privind evidența informațiilor în format electronic.

F. Manipularea și controlul mediilor de stocare a informațiilor clasificate în format electronic

Art. 294

(1) Toate mediile de stocare secrete de stat se identifică și se controlează în mod corespunzător nivelului de secretizare.

(2) Pentru informațiile neclasificate sau secrete de serviciu se aplică regulamente de securitate interne.

(3) Identificarea și controalele trebuie să asigure următoarele cerințe:

a) Pentru nivelul secret:

- un mijloc de identificare - număr de serie și marcajul nivelului de clasificare - pentru fiecare astfel de mediu, în mod separat;

- proceduri bine definite pentru emiterea, primirea, retragerea, distrugerea sau păstrarea mediilor de stocare;

- evidențele manuale sau tipărite la imprimantă, indicând conținutul și nivelul de secretizare a informațiilor înregistrate pe mediile de stocare.

b) Pentru nivelul strict secret și strict secret de importanță deosebită, informațiile detaliate asupra mediului de stocare, inclusiv conținutul și nivelul de clasificare, se țin într-un registru adecvat.

Art. 295

Controlul punctual și de ansamblu al mediilor de stocare, pentru a asigura compatibilitatea cu procedurile de identificare și control în vigoare, trebuie să asigure îndeplinirea următoarelor cerințe:

a) pentru nivelul secret - controalele punctuale ale prezenței fizice și conținutului mediilor de stocare se efectuează periodic, verificându-se dacă acele medii de stocare nu conțin informații cu un nivel de clasificare superior;

b) pentru nivelul strict secret - toate mediile de stocare se inventariază periodic, controlând punctual prezența lor fizică și conținutul, pentru a verifica dacă pe acele medii nu sunt stocate informații cu un nivel de clasificare superior;

c) pentru nivelul strict secret de importanță deosebită, toate mediile se verifică periodic, cel puțin anual și se controlează punctual, în legătură cu prezența fizică și conținutul lor.

G. Declasificarea și distrugerea mediilor de stocare a informațiilor în format electronic

Art. 296

Informațiile clasificate înregistrate pe medii de stocare reutilizabile se șterg doar în conformitate cu procedurile operaționale de securitate.

Art. 297

(1) Când un mediu de stocare urmează să iasă din uz, trebuie să fie declasificat suprimându-se orice marcaje de clasificare, ulterior putând fi utilizat ca mediu de stocare nesecret. Dacă acesta nu poate fi declasificat, trebuie distrus printr-o procedură aprobată.

(2) Sunt interzise declasificarea și refolosirea mediilor de stocare care conțin informații strict secrete de importanță deosebită, acestea putând fi numai distruse, în conformitate cu procedurile operaționale de securitate.

Art. 298

Informațiile clasificate în format electronic stocate pe un mediu de unică folosință - cartele, benzi perforate - trebuie distruse conform prevederilor procedurilor operaționale de securitate.

SECȚIUNEA 5: Reguli generale de securitate TIC

A. Securitatea comunicațiilor

Art. 299

Toate mijloacele folosite pentru transmiterea electromagnetică a informațiilor clasificate se supun instrucțiunilor de securitate a comunicațiilor emise de către instituția desemnată la nivel național pentru protecția informațiilor clasificate.

Art. 300

Într-un SPAD - SIC trebuie să se dispună mijloace de interzicere a accesului la informațiile clasificate de la toate terminalele/stațiile de lucru la distanță, atunci când se solicită acest lucru, prin deconectare fizică sau prin proceduri software speciale, aprobate de către autoritatea de acreditare de securitate.

B. Securitatea la instalare și față de emisiile electromagneticice

Art. 301

Instalarea inițială a SPAD sau RTD - SIC sau orice modificare majoră adusă acestora vor fi executate de persoane autorizate, în condițiile prezentelor standarde. Lucrările vor fi permanent supravegheate de personal tehnic calificat, care are acces la informații de cel mai înalt nivel de clasificare pe care respectivul SPAD sau RTD - SIC le va stoca, procesa sau transmite.

Art. 302

Toate echipamentele SPAD și RTD-SIC vor fi instalate în conformitate cu reglementările specifice în vigoare, emise de către instituția desemnată la nivel național pentru protecția informațiilor clasificate, cu directivele și standardele tehnice corespunzătoare.

Art. 303

Sistemele SPAD și RTD-SIC care stochează, procesează sau transmit informații secrete de stat vor fi protejate corespunzător față de vulnerabilitățile de securitate cauzate de radiațiile compromișătoare -TEMPEST. "

C. Securitatea în timpul procesării informațiilor clasificate

Art. 304

Procesarea informațiilor se realizează în conformitate cu procedurile operaționale de securitate, prevăzute în prezentele standarde.

Art. 305

Transmiterea informațiilor secrete de stat către instalații automate - a căror funcționare nu necesită prezența unui operator uman - este interzisă, cu excepția cazului când se aplică reglementări speciale aprobate de către autoritatea de acreditare de securitate, iar acestea au fost specificate în procedurile operaționale de securitate.

Art. 306

În SPAD sau RTD-SIC care au utilizatori - existenți sau potențiali - fără certificate de securitate emise conform prezentelor standarde nu se pot stoca, procesa sau transmite informații strict secrete de importanță deosebită.

D. Procedurile operaționale de securitate

Art. 307

Procedurile operaționale de securitate reprezintă descrierea implementării strategiei de securitate ce urmează să fie adoptată, a procedurilor operaționale de urmat și a responsabilităților personalului.

Art. 308

Procedurile operaționale de securitate sunt elaborate de către agenția de concepere și implementare a metodelor, mijloacelor și măsurilor de securitate, în colaborare cu CSTIC, precum și cu agenția de acreditare de securitate, care are atribuții de coordonare, și alte autorități cu atribuții în domeniul. Agenția de acreditare de securitate va aproba procedurile de operare înainte de a autoriza stocarea, procesarea sau transmiterea informațiilor secrete de stat prin SPAD - RTD - SIC.

E. Protecția produselor software și managementul configurației

Art. 309

CSTIC are obligația să efectueze controale periodice, prin care să stabilească dacă toate produsele software originale - sisteme de operare generale, subsisteme și pachete soft - aflate în folosință, sunt protejate în condiții conforme cu nivelul de clasificare al informațiilor pe care acestea trebuie să le proceseze. Protecția programelor - software de aplicație se stabilește pe baza evaluării nivelului de secretizare a acestora, ținând cont de nivelul de clasificare a informațiilor pe care urmează să le proceseze.

Art. 310

- (1) Este interzisă utilizarea de software neautorizat de către agenția de acreditare de securitate.
- (2) Conservarea exemplarelor originale, a copiilor - backup sau off-site, precum și salvările periodice ale datelor obținute din procesare vor fi executate în conformitate cu prevederile procedurilor operaționale de securitate.

Art. 311

- (1) Versiunile software care sunt în uz trebuie să fie verificate la intervale regulate, pentru a garanta integritatea și funcționarea lor corectă.
- (2) Versiunile noi sau modificate ale software-ului nu vor fi folosite pentru procesarea informațiilor secrete de stat, până când procedurile de securitate ale acestora nu sunt testate și aprobată conform CSS.
- (3) Un software care îmbunătățește posibilitățile sistemului și care nu are nici o procedură de securitate nu poate fi folosit înainte de a fi verificat de către CSTIC.

F. Verificări pentru depistarea virușilor de calculator și a software-ului nociv

Art. 312

Verificarea prezenței virușilor și software-ului nociv se face în conformitate cu cerințele impuse de către agenția de acreditare de securitate.

Art. 313

(1) Versiunile de software noi sau modificate - sisteme de operare, subsisteme, pachete de software și software de aplicație - stocate pe diferite medii care se introduc într-o unitate, trebuie verificate obligatoriu pe sisteme de calcul izolate, în vederea depistării software-ului nociv sau a virușilor de calculator, înainte de a fi folosite în SPAD sau RTD - SIC. Periodic se va proceda la verificarea software-ului instalat.

(2) Verificările trebuie făcute mai frecvent dacă SPAD sau RTD - SIC sunt conectate la alt SPAD sau RTD - SIC sau la o rețea publică de comunicații.

G. Întreținerea tehnică a SPAD sau RTD - SIC

Art. 314

(1) În contractele de întreținere a SPAD și RTD - SIC care stochează, procesează sau transmit informații secrete de stat, se vor specifica cerințele care trebuie îndeplinite pentru ca personalul de întreținere și aparatura specifică a acestuia să poată fi introduse în zona de operare a sistemelor respective.

(2) Personalul de întreținere trebuie să dețină certificate de securitate de nivel corespunzător nivelului de secretizare a informațiilor la care au acces.

Art. 315

Scoaterea echipamentelor sau a componentelor hardware din zona SPAD sau RTD - SIC se execută în conformitate cu prevederile procedurilor operaționale de securitate.

Art. 316

Cerințele menționate la art. 314 trebuie stipulate în CSS, iar procedurile de desfășurare a activității respective trebuie stabilite în procedurile operaționale de securitate. Nu se acceptă tipurile de întreținere care constau în aplicarea unor proceduri de diagnosticare ce implică accesul de la distanță la sistem, decât dacă activitatea respectivă se desfășoară sub control strict și numai cu aprobarea agenției de acreditare de securitate.

H. Achiziții

Art. 317

Sistemele SPAD sau RTD - SIC, precum și componentele lor hardware și software sunt achiziționate de la furnizori interni sau externi selectați dintre cei agreeați de către agenția de acreditare de securitate.

Art. 318

Componentele sistemelor de securitate implementate în SPAD sau RTD - SIC trebuie acreditate pe baza unei documentații tehnice amănunțite privind proiectarea, realizarea și modul de distribuire al acestora.

Art. 319

SPAD sau RTD - SIC care stochează, procesează sau transmit informații secrete de stat sau componentele lor de bază - sisteme de operare de scop general, produse de limitare a funcționării pentru realizarea securității și produse pentru comunicare în rețea - se pot achiziționa numai dacă au fost evaluate și certificate de către agenția de acreditare de securitate.

Art. 320

Pentru SPAD și RTD - SIC care stochează, procesează sau transmit informații secrete de serviciu, sistemele și componentele lor de bază vor respecta, pe cât posibil, criteriile prevăzute de prezentele standarde.

Art. 321

La închirierea unor componente hardware sau software, în special a unor medii de stocare, se va ține cont că astfel de echipamente, odată utilizate în SPAD sau RTD - SIC ce procesează, stochează sau transmit informații clasificate, vor fi supuse măsurilor de protecție reglementate prin prezentele standarde. O dată clasificate, componentele respective nu vor putea fi scoase din zonele SPAD sau RTD - SIC decât după declasificare.

I. Acreditarea SPAD și RTD - SIC

Art. 322

(1) Toate SPAD și RTD - SIC, înainte de a fi utilizate pentru stocarea, procesarea sau transmiterea informațiilor clasificate, trebuie acreditate de către agenția de acreditare de securitate, pe baza datelor furnizate de către CSS, procedurilor operaționale de securitate și altor documentații relevante.

(2) Subsistemele SPAD și RTD - SIC și stațiile de lucru cu acces la distanță sau terminalele vor fi acreditate ca parte integrantă a sistemelor SPAD și RTD - SIC la care sunt conectate, în cazul în care un sistem SPAD sau RTD - SIC deservește atât NATO, cât și organizațiile/structurile interne ale țării, acreditarea se va face de către autoritatea națională de securitate, cu consultarea ADS și a agenților INFOSEC, potrivit competențelor.

J. Evaluarea și certificarea

Art. 323

În situațiile ce privesc modul de operare de securitate multi-nivel, înainte de acreditarea propriu-zisă a SPAD sau RTD - SIC, hardware-ul, firmware-ul și software-ul vor fi evaluate și certificate de către agenția de acreditare de securitate, în acest sens, instituția desemnată la nivel național pentru protecția informațiilor clasificate va stabili criterii diferențiate pentru fiecare nivel de secretizare a informațiilor vehiculate de SPAD sau RTD - SIC.

Art. 324

Cerințele de evaluare și certificare se includ în planificarea sistemului SPAD și RTD - SIC și sunt stipulate explicit în CSS, imediat după ce modul de operare de securitate a fost stabilit.

Art. 325

Următoarele situații impun evaluarea și certificarea de securitate în modul de operare de securitate multi-nivel:

- a) pentru SPAD sau RTD - SIC care stochează, procesează sau transmite informații clasificate strict secret de importanță deosebită;
- b) pentru SPAD sau RTD - SIC care stochează, procesează sau transmite informații clasificate strict secret, în cazurile în care:
 - SPAD sau RTD - SIC este interconectat cu un alt SPAD sau RTD - SIC - de exemplu, aparținând altui CSTIC;
 - SPAD sau RTD - SIC are un număr de utilizatori posibili care nu poate fi definit exact.

Art. 326

Procesele de evaluare și certificare trebuie să se desfășoare, conform principiilor și instrucțiunilor aprobată, de către echipe de expertizare cu pregătire tehnică adecvată și autorizate corespunzător. Aceste echipe vor fi compuse din experți selecționați de către agenția de acreditare de securitate.

Art. 327

(1) În procesele de evaluare și certificare se va stabili în ce măsură un SPAD sau RTD - SIC îndeplinește condițiile de securitate specificate prin CSS, avându-se în vedere că, după încheierea procesului de evaluare și certificare, anumite secțiuni - paragrafe sau capitole - din CSS trebuie să fie modificate sau actualizate.

(2) Procesele de evaluare și certificare trebuie să înceapă din stadiul de definire a SPAD sau RTD - SIC și continuă pe parcursul fazelor de dezvoltare.

K. Verificări de rutină pentru menținerea acreditării

Art. 328

Pentru toate SPAD și RTD - SIC care stochează, procesează sau transmit informații secrete de stat, CSTIC stabilește proceduri de control prin care să se poată stabili dacă schimbările intervenite în SIC sunt de natură a le compromite securitatea.

Art. 329

(1) Modificările care implică reacreditarea sau pentru care se solicită aprobarea anterioară a agenției de acreditare de securitate trebuie să fie identificate cu claritate și expuse în CSS.

(2) După orice modificare, reparare sau eroare care ar fi putut afecta dispozitivele de securitate ale SPAD sau RTD - SIC, CSTIC trebuie să efectueze o verificare privind funcționarea corectă a dispozitivelor de securitate.

(3) Menținerea acreditării SPAD sau RTD - SIC trebuie să depindă de satisfacerea criteriilor de verificare.

Art. 330

(1) Toate SPAD și RTD - SIC care stochează, procesează sau transmit informații secrete de stat sunt inspectate și reexamineate periodic de către agenția de acreditare de securitate.

(2) Pentru SPAD sau RTD - SIC care stochează, procesează sau transmit informații strict secrete de importanță deosebită, inspecția se va face cel puțin o dată 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 informației, ce operează autonom sau ca parte a unei rețele, precum și calculatoarele portabile cu discuri fixe sunt considerate medii de stocare a informațiilor, în același sens ca și celealte medii amovibile de stocare a informațiilor.

(2) În măsura în care acestea stochează informații clasificate trebuie supuse prezentelor standarde.

Art. 332

Echipamentelor prevăzute la art. 331 trebuie să li se acorde nivelul de protecție pentru acces, manipulare, stocare și transport, corespunzător cu cel mai înalt nivel de clasificare a informațiilor care au fost vreodată stocate sau procesate pe ele, până la trecerea la un alt nivel de clasificare sau declasificarea lor, în conformitate cu procedurile legale.

M. Utilizarea echipamentelor de calcul proprietate privată

Art. 333

(1) Este interzisă utilizarea mediilor de stocare amovibile, a software-ului și a hardware-ului, aflate în proprietate privată, pentru stocarea, procesarea și transmiterea informațiilor secrete de stat.

(2) Pentru informațiile secrete de serviciu sau neclasificate, se aplică reglementările interne ale unității.

Art. 334

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

N. Utilizarea echipamentelor contractorilor sau a celor puse la dispoziție de alte instituții

Art. 335

Utilizarea într-un obiectiv a echipamentelor și a software-ului contractanților, pentru stocarea, procesarea sau transmiterea informațiilor clasificate este permisă numai cu avizul CSTIC și aprobarea șefului unității.

Art. 336

Utilizarea într-un obiectiv a echipamentelor și software-ului puse la dispoziție de către alte instituții poate fi permisă, în acest caz echipamentele sunt evidențiate în inventarul unității, în ambele situații, trebuie obținut avizul CSTIC.

O. Marcarea informațiilor cu destinație specială

Art. 337

Marcarea informațiilor cu destinație specială se aplică, în mod obișnuit, informațiilor clasificate care necesită o distribuție limitată și manipulare specială, suplimentar față de caracterul atribuit prin clasificarea de securitate.

CAPITOLUL IX: CONTRAVENTII ȘI SANCTIUNI LA NORMELE PRIVIND PROTECȚIA INFORMAȚIILOR CLASIFICATE

Art. 338

(1) Constitue contravenții la normele privind protecția informațiilor clasificate următoarele fapte:

- a) detinerea fără drept, sustragerea, divulgarea, alterarea sau distrugerea neautorizată a informațiilor secrete de stat;
- b) neîndeplinirea măsurilor prevăzute în art. 18, 25-28, 29, 96-139 și 140-181;
- c) neîndeplinirea obligațiilor prevăzute la art. 31, 41-43, 213, 214;
- d) nerespectarea normelor prevăzute în art. 140-142, 145, 159, 160, 162, 163, 179-181, 183 alin. (1) și 185-190;
- e) neîndeplinirea sau îndeplinirea defectuoasă a obligațiilor prevăzute în art. 240 alin. (2) și (3), art. 243 și art. 248, precum și nerespectarea regulilor prevăzute în art. 274-336.

(2) Contravențiile prevăzute la alin. (1) se sanctionează astfel:

- a) contravențiile prevăzute la alin. (1) lit. a) se sanctionează cu amendă de la 500.000 lei la 50.000.000 lei în cazul faptelor de detinere fără drept sau de alterare a informațiilor clasificate

și cu amendă de la 10.000.000 lei la 100.000.000 lei, în cazul faptelor de sustragere, divulgare sau distrugere neautorizată a informațiilor clasificate;

b) faptele prevăzute în alin. (1) lit. b) și c) se sancționează cu avertisment sau cu amendă de la 500.000 lei la 25.000.000 lei;

c) faptele prevăzute în alin. (1) lit. d) se sancționează cu avertisment sau cu amendă de la 1.000.000 lei la 50.000.000 lei;

d) faptele prevăzute în alin. 1 lit. e) se sancționează cu amendă de la 5.000.000 lei la 50.000.000 lei.

(3) Persoanele sau autoritățile care constată contravențiile pot aplica, după caz, și sancțiunea complementară, constând în confiscarea, în condițiile legii, a bunurilor destinate, folosite sau rezultate din contravenții.

(4) Dispozițiile reglementărilor generale referitoare la regimul juridic al contravențiilor se aplică în mod corespunzător.

Art. 339

(1) Contravențiile și sancțiunile prevăzute la art. 338 se constată și se aplică, în limitele competențelor ce le revin, de către persoane anume desemnate din Serviciul Român de Informații, Ministerul Apărării Naționale, Ministerul de Interne, Ministerul Justiției, Serviciul de Informații Externe, Serviciul de Protecție și Pază și Serviciul de Telecomunicații Speciale.

(2) Pot să constate contravențiile și să aplice sancțiunile prevăzute la art. 338, în limitele competențelor stabilite:

a) persoane anume desemnate din ORNISS;

b) conducătorii autorităților sau instituțiilor publice, agenților economici cu capital parțial sau integral de stat și ai altor persoane juridice de drept public;

c) autoritățile sau persoanele prevăzute de reglementările generale referitoare la regimul juridic al contravențiilor.

(3) Plângerile împotriva proceselor-verbale de constatare a contravențiilor și de aplicare a sancțiunilor se soluționează potrivit reglementărilor generale privind regimul juridic al contravențiilor.

CAPITOLUL X: DISPOZIȚII FINALE

Art. 340

Nomenclatura funcțiilor, condițiile de studii și vechime, precum și salarizarea personalului cu atribuții privind evidența, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea și distrugerea informațiilor clasificate se stabilesc potrivit actelor normative în vigoare.

Art. 341

Conducătorii unităților care gestionează informații clasificate vor lua măsuri ca dispozițiile prezentelor standarde să fie aduse la cunoștința tuturor salariaților și vor întreprinde măsuri pentru:

a) crearea structurilor interne specializate cu atribuții în aplicarea prezentelor standarde;

b) nominalizarea personalului cu atribuții și funcții privind gestionarea informațiilor clasificate;

c) inițierea demersurilor prevăzute de lege și de prezentele standarde, pentru obținerea abilităților privind accesul la informații clasificate.

Art. 342

La solicitarea persoanelor juridice din sfera de competență a Serviciului Român de Informații, R.A. Rasirom va evalua conformitatea și va prezenta ORNISS propuneri de eliberare a certificatelor de acreditare a calității pentru sistemele și echipamentele de protecție fizică a informațiilor clasificate.

Art. 343

(1) Prezentele standarde se interpretează și se aplică în concordanță cu Normele privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România, aprobate prin Hotărârea Guvernului nr. **353 din 15 aprilie 2002**.

(2) În eventualitatea unor neconcordanțe între cele două reglementări menționate la alin (1), au prioritate Normele privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România, aprobate prin Hotărârea Guvernului nr. **353 din 15 aprilie 2002**.

Art. 344

Dispozițiile prezenterelor standarde referitoare la contravențiile și sancțiunile la normele privind protecția informațiilor clasificate se aplică după 60 de zile de la publicarea prezentei hotărâri.

Art. 345

Anexele nr. 1-32 fac parte integrantă din prezentele standarde naționale de protecție a informațiilor clasificate.

ANEXA Nr. 1

FIȘA DE CONSULTARE
a documentului "Strict secret de importanță deosebită" nr. _____ din
privind _____

Nr. crt .	Numele, prenumele și funcția celor care au luat cunoștință de conținutul documentului	Numărul și seria certificătului de securitate	Data și ora primirii documentului	Semnătura celui care a primit documentul	Cine a aprobat consulta-rea documentului (numele , prenumele, funcția)	Data și ora restituiri documentului	Numele, prenumele și semnatură a celui care a primit documentul (în urma restituirii)	Obs.

ANEXA Nr. 2

ROMÂNIA

UNITATEA _____

Compartimentul _____

Nr. _____ din _____

FIŞĂ DE PREGĂTIRE INDIVIDUALĂ

NUME:

PRENUME:

FUNCȚIA:

COMPARTIMENTUL:

Nr. crt.	Tema pregătirii	Forma de pregătire	Locul	Perioada	Semnătura titularului de fișă	Observații

ANEXA Nr. 3

ANGAJAMENT DE CONFIDENTIALITATE*

Subsemnatul _____ născut în localitatea _____ la data de _____, fiul (fiica) lui _____ și a _____ angajat al _____ în funcția de _____, cu domiciliul în localitatea _____, strada _____, nr. _____, bl. ___, sc. ___, et. ___, ap. ___, județul/sectorul _____, posesor al certificatului/autorizației seria _____, nr. _____, declar că am luat cunoștință de dispozițiile legale cu privire la protecția informațiilor clasificate și mă angajez să păstrez cu strictețe secretul de stat și de serviciu, să respect întocmai normele legale cu privire la evidența, manipularea și păstrarea informațiilor, datelor și documentelor secrete de stat și de serviciu ce mi-au fost încredințate, inclusiv după închiderea activităților care presupun accesul la aceste informații.

Sunt conștient că în cazul în care voi încălca prevederile normative privind protecția informațiilor clasificate voi răspunde, potrivit legii, administrativ, disciplinar, material, civil ori penal, în raport cu gravitatea faptei.

Data

Semnătura

DAT ÎN PREZENȚA

(numele și prenumele funcționarului de securitate)

Semnătura

* Pentru persoanele care au acces la informații secrete de stat și de serviciu.

ANEXA Nr. 4

ROMÂNIA

(UNITATEA) _____

Compartimentul _____

REGISTRUL DE EVIDENȚĂ al informațiilor strict secrete de importanță deosebită

INTRARE

Nr. de înre- gis- trare	Data înregistrării			Nr. și data docu- mentulu i la expedit or	De la cine pro-vine docu- mentul	Con- ținutul pe scurt al docu- mentului	Nr. ex.	Nr. file/ ex.	Nr. ane -xe	Nr. file ane -xe	Cui i s-a repar- tizat docu- ment ul
	anul	luna	ziua								

IEȘIRE

Data expedierii			Destinatar	Nr. ex.	Nr. file	Nr. anex e	Nr. file anex e	Nr. borderoul ui de expediere	Nr. dosarului și fila unde a fost clasat documentul sau nr. procesului- verbal de distrugere	Obser- vații
anul	luna	ziua								

ANEXA Nr. 5

ROMÂNIA

(UNITATEA) _____

Compartimentul _____

REGISTRUL DE EVIDENȚĂ al informațiilor strict secrete și secrete

INTRARE

Nr.	Data înregistrării	Nr. și	De la	Nr.	Nr.	Nivelul	Con-	Nr.	Nr.	Cui i

de înregistrare	anul	luna	ziua	data documentului la expeditor	cine provine documentul	ex.	file / ex.	de secretezare	ținutul pe scurt al documentului	anexe	file anexe	s-a repara-tizat documentul

IEȘIRE

Data expedierii			Nivelul de secretezare	Destina-tar	Nr. ex.	Nr. file / ex.	Nr. anexe	Nr. file anexe	Nr. borderoului de expediere	Nr. dosarului și fila unde a fost clasat documentul (nr. procesului-verbal de distrugere)	Obser-vări
anul	luna	ziua									

ANEXA Nr. 6

ROMÂNIA

(UNITATEA) _____

Compartimentul _____

REGISTRUL DE EVIDENȚĂ al informațiilor secrete de serviciu

INTRARE

Nr. de înregistrare	Data înregistrării			Nr. și data documentului la expeditor	De la cine provine documentul	Conținutul pe scurt al documentului	Nr. ex.	Nr. file / ex.	Nr. anexe	Nr. file anexe	Cui i s-a repartizat documentul
	anul	luna	ziua								

IEȘIRE

Data expedierii	Destinatar	Nr. dosarului	Observații						
-----------------	------------	-----	-----	-----	-----	-----	-----	---------------	------------

anul	luna	ziua		ex .	file	anex e	file anex e	borderoul ui de expediere	și fila unde a fost clasat documentul (nr. procesului-verbal de distrugere)	

ANEXA Nr. 7

REGISTRU UNIC de evidență a registrelor, condicilor, borderourilor și a caietelor pentru însemnări clasificate

Nr. crt. / serie	Nr. file	Denumirea materialelor distribuite	Numele, prenumele celui care a primit materialul	Seria și numărul certificatului de securitate	Data distribuirii			Semnătura celui care a primit materialul	Nr. dosarului unde a fost clasat sau nr. procesului-verbal de distrugere	Obs.
					Ziua	Luna	Anul			

ANEXA Nr. 8

ROMÂNIA
(UNITATEA) _____
Compartimentul _____

CONDICA DE PREDARE - PRIMIRE a documentelor clasificate

Nr.	Compunerea documentului	Numele,	Data	Semnă-	Semnă-	Obs.
-----	-------------------------	---------	------	--------	--------	------

crt .	Nr. de înregistrare	Denumire document	Clasa (nivelul de secretizare)	Ex. nr.	Nr. de dosare, mape sau file	prenumele, seria și nr. certificatului de securitate ale persoanei căreia i-a fost predat documentul I		tura de primire	tura de restituire	

ANEXA Nr. 9

ROMÂNIA

(UNITATEA) _____

Compartimentul _____

REGISTRUL de evidență a informațiilor clasificate multiple

INTRARE

Nr. de înregistrare	Compartimentul care a solicitat copierea	Numele și prenumele celui care a predat documentul I	Numărul de înregistrare al documentului original și al cererii de copiere	Data și semnătura de primire a documentului pentru copiat	Nivelul de secretizare al documentului copiat	Nr. file	Nr. anexe

IEȘIRE

Documentul copiat		Forma de copiere	Data, numele și prenumele persoanei care a primit originalul și copile	Observații
Nr. exemplare	Total file copiate			

ANEXA Nr. 10

ANTET
(instituția/ agentul economic)
Nr. _____ din _____

CLASIFICAREA
(după completare, în funcție de nivelul maxim de clasificare a informațiilor pe care le cuprinde)

APROB

(funcția, numele și prenumele conducătorului instituției/agentului economic, semnătura și stampila)

**PROGRAMUL DE PREVENIRE A SCURGERII DE INFORMAȚII CLASIFICATE
DEȚINUTE DE**
(unitatea care îl întocmește)**CAPITOLUL I: BAZA LEGALĂ**

Se va menționa cadrul normativ care a stat la baza întocmirii programului.

CAPITOLUL II**1. GENERALITĂȚI**

Se va face o scurta prezentare a instituției/agentului economic, sucursalelor și filialelor. Vor fi prezentate elementele de concretizare a identității, statutului juridic, obiectul de activitate.

2. OBIECTIVE

Vor fi prezentate obiectivele urmărite prin măsurile prezentate în program.

Vor fi vizate următoarele obiective minimale:

- apărarea informațiilor clasificate împotriva acțiunilor de compromitere, sabotaj, sustragere, distrugere neautorizată sau alterare;
- prevenirea accesului neautorizat la astfel de informații, a cunoașterii și diseminării lor ilegale;
- înlăturarea riscurilor și vulnerabilităților ce pot pune în pericol protecția informațiilor clasificate;
- asigurarea cadrului procedural necesar protecției informațiilor clasificate.

3. PRINCIPII

Se precizează principiile care stau la baza măsurilor de prevenire a scurgerii de informații.

Măsurile de prevenire a scurgerii de informații se bazează pe:

- autorizarea accesului la informațiile clasificate absolut necesare îndeplinirii atribuțiilor de serviciu (principiul "nevoii de a cunoaște");
- asigurarea aplicării măsurilor de protecție, în mod diferențiat, pe zone de securitate și în funcție de nivelurile de acces la informații clasificate;
- accesul la informații clasificate este permis numai în baza verificărilor și abilitărilor legale;
- aplicarea, în mod obligatoriu și unitar, a măsurilor de protecție atât în locurile în care se depozitează informațiile clasificate și în cazul sistemelor informatice care stochează, prelucrează sau transmit informații de acest fel, cât și al persoanelor care au acces la acestea și utilizatorilor rețelelor respective;
- răspunderea personală privind aplicarea măsurilor de protecție stipulate prin programul de prevenire a scurgerii de informații clasificate.

CAPITOLUL III

1. ELEMENTE GENERALE PRIVIND INFORMAȚIILE CLASIFICATE DEȚINUTE DE INSTITUȚIA/AGENTUL ECONOMIC

Se vor face precizări privind clasele și nivelurile de secretizare a informațiilor clasificate deținute de instituția/agentul economic (în cazul celor primite de la alți emitenți se va menționa baza juridică a deținerii, respectiv tipul contractului și dacă s-au asumat obligații de protejare a secretului prin încheierea de acorduri între părți).

2. LISTA INFORMAȚIILOR CLASIFICATE, APROBATE PRIN HOTĂRÂRE A GUVERNULUI (DOCUMENTE, DATE, OBIECTE SAU ACTIVITĂȚI, INDIFERENT DE SUPORT SAU FORMĂ), PE CLASE ȘI NIVELURI DE SECRETIZARE, DEȚINUTE DE UNITATEA ÎN CAUZĂ

Instituțiile/agenții economici vor întocmi lista cuprinzând categoriile informațiilor clasificate, pe care le dețin, pe clase și niveluri de secretizare.

Lista va fi actualizată ori de câte ori situația o impune (clasificarea sau declasificarea unor informații).

3. LOCURI UNDE SE CONCENTREAZĂ, DE REGULĂ ORI TEMPORAR, DATE, INFORMAȚII, DOCUMENTE CLASIFICATE SAU SE DESFĂȘOARĂ ASTFEL DE ACTIVITĂȚI (CONFORM ANEXEI NT. 10/A)

Vor fi menționate:

- spațiile destinate păstrării documentelor clasificate;
- spațiul destinat sistemului/rețelelor informatiche de procesare automată a datelor care preia, prelucrează, stochează și transmite date și informații clasificate;
- alte locuri unde se gestionează sau se manipulează asemenea date, informații și documente clasificate sau se desfășoară astfel de activități.

CAPITOLUL IV

1. LISTA FUNCȚIILOR CARE NECESITĂ ACCES LA INFORMAȚII CLASIFICATE

Vor fi precizate funcțiile care necesită accesarea informațiilor clasificate, pe clase și niveluri de secretizare, cu respectarea strictă a principiului "nevoii de a cunoaște".

2. PREZENTAREA PERSOANEI/STRUCTURII DESEMNAME SĂ ÎNDEPLINEASCĂ ATRIBUȚII PE LINIA PROTECȚIEI ACTIVITĂȚILOR, DATELOR, INFORMAȚIILOR ȘI DOCUMENTELOR CLASIFICATE

2.1. Pentru fiecare persoană în parte se vor preciza:

- numele și prenumele;
- datele de identificare (prenumele părinților, nume anterioare, data și locul nașterii, profesia și locul de muncă, domiciliul, telefonul);

2.2. Atribuțiile și competențele privind asigurarea protecției informațiilor clasificate.

Nominalizarea se va face de către conducătorul instituției/agentului economic respectiv, situația fiind prezentată pe niveluri de acces, care va fi acordat numai în urma obținerii abilitării.

3. PREZENTAREA PERSOANELOR CARE AU SAU URMEAZĂ SĂ AIBĂ ACCES LA INFORMAȚII CLASIFICATE, PE NIVELURI DE SECRETIZARE

Va fi întocmită lista cu persoanele care au sau urmează să aibă acces la informații clasificate, nominalizate de către conducătorul instituției/agentului economic (inclusiv cele care lucrează în sistemul informatic și de telecomunicații, destinat preluării, prelucrării, stocării și transmiterii de informații clasificate) *

Va fi întocmită, de asemenea, lista cu persoanele cărora li se acordă acces temporar la informații clasificate din cadrul sau din afara instituției/agentului economic (inclusiv cele aparținând firmelor prestatoare de servicii pentru întreținerea sau instalarea programelor, care vor fi avizate corespunzător nivelului maxim de secretizare a informațiilor din sistemele informatiche și de telecomunicații) **

Accesul la informații clasificate va fi permis numai după obținerea abilitării.

Pentru fiecare persoană nominalizată vor fi precizate:

- numele, prenumele și datele de identificare (prenumele părinților, nume anterioare, data și locul nașterii, profesia și locul de muncă, domiciliu, telefonul);
- informațiile clasificate care îi sunt absolut necesare îndeplinirii atribuțiilor de serviciu, cu precizarea clasei și nivelului de secretizare a acestuia.

* Numărul persoanelor nominalizate în lista respectivă va fi cel mult egal cu cel al funcțiilor ce necesită acces la informațiile clasificate.

** Listele respective vor fi actualizate, cu îndeplinirea procedurilor legale de avizare, în raport de necesități (extinderea sau limitarea accesului unor persoane la informații clasificate, în funcție de modificarea atribuțiilor de serviciu).

CAPITOLUL V

1. MĂSURI DE PROTECȚIE FIZICĂ A CLĂDIRILOR, SPAȚIILOR/LOCURILOR UNDE SE PĂSTREAZĂ SAU SE CONCENTREAZĂ INFORMAȚII CLASIFICATE ORI SE DESFĂȘOARĂ ASTFEL DE ACTIVITĂȚI (CONFORM ANEXEI Nr. 10/B)

Vor fi stipulate măsuri vizând:

- securitatea clădirilor;
- controlul intrărilor și ieșirilor;
- paza;
- containerele și încăperile de securitate;
- încuietorile;
- controlul cheilor și combinațiilor;
- dispozitivele de detectare a intrușilor;
- protecția fizică a copiatoarelor și dispozitivelor telefax;
- planurile de urgență.

2. MĂSURI PROCEDURALE DE PROTECȚIE A DATELOR, INFORMAȚIILOR, DOCUMENTELOR ORI A ACTIVITĂȚILOR CLASIFICATE

Vor fi prezentate:

- reguli de evidență, procesare, manipulare, accesare, multiplicare, transmitere, păstrare și stocare a datelor, informațiilor și documentelor clasificate indiferent de suport (aprobate de conducerea instituției/agentului economic);
- reguli de acces pentru personalul propriu;
- reguli de acces pentru personalul/persoanele din afara instituției/agentului economic, inclusiv pentru străini sau reprezentanți mass-media.

CAPITOLUL VI: PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ȘI DE TELECOMUNICAȚII DESTINAT PRELUĂRII, PRELUCRĂRII, STOCĂRII ȘI TRANSMITERII DE DATE ȘI INFORMAȚII CLASIFICATE

Vor fi prezentate echipamentele de comunicații și birotică (telefoane, fax, telex, copiatoare) prin care vor fi transmise/prelucrate informații clasificate.

Vor fi prezentate, de asemenea, echipamentul informatic existent, calculatoarele conectate la Internet, sistemele de protecție utilizate și firma prestatoare de servicii pentru întreținerea sau instalarea programelor (conform anexei nr./ O/C).

În situația în care unele dintre aceste echipamente nu sunt protejate corespunzător, se va face precizarea că folosirea acestora pentru prelucrarea informațiilor clasificate este interzisă.

CAPITOLUL VII: MĂSURI DE PROTECȚIE ÎMPOTRIVA. OBSERVĂRII ȘI ASCULTĂRII *

* Zonele în care se elaborează și/sau se discută informații clasificate secret de stat trebuie protejate împotriva observării și ascultării pasive și/sau active. Responsabilitatea înălțurării riscurilor privind observarea și ascultarea revine instituției/agentului economic, care elaborează sau, după caz, gestionează informații clasificate (conform anexei nr. 10/D).

CAPITOLUL VIII

1. CONTROALE, ACTIVITĂȚI DE ANALIZĂ ȘI EVALUARE A MODULUI ÎN CARE SE RESPECTĂ PREVEDERILE LEGALE REFERITOARE LA PROTECȚIA INFORMAȚIILOR CLASIFICATE

Vor fi prezentate tematica și periodicitatea controalelor (inopinate, periodice), cine le execută, documentele ce se întocmesc și sancțiunile ce se vor aplica în cazurile de încălcare a reglementărilor privind protecția informațiilor clasificate.

Se va întocmi planificarea, activităților de evaluare și analiză a stării de protecție a informațiilor clasificate și se va prevedea ca anual, după încheierea operațiunii de inventariere a suportilor de informații clasificate să se analizeze și să se evaluateze modul în care au fost respectate prevederile programului, prevăzându-se și măsurile care se impun și termenele de remediere a unor nereguli constatate.

2. SOLUȚIONAREA CAZURIOR DE ÎNCĂLCARE A REGLEMENTĂRILOR PRIVIND PROTECȚIA INFORMAȚIILOR CLASIFICATE (CONFORM ANEXEI Nr. 10/E)

Se vor face referiri la:

- măsurile ce vor fi luate în cazul constatării încălcării reglementărilor privind protecția informațiilor clasificate;
- evidența încălcărilor reglementărilor de securitate;
- comunicarea compromiterilor;
- scoaterea din evidență a documentelor clasificate pierdute sau distruse.

CAPITOLUL IX: MĂSURI DE INSTRUIRE ȘI EDUCAȚIE PROTECTIVĂ A PERSOANELOR CARE AU ATRIBUȚII PE LINIA PROTECȚIEI INFORMAȚIILOR CLASIFICATE ȘI A CELOR CARE AU ACCES LA ASTFEL DE INFORMAȚII (CONFORM ANEXEI Nr. 10/F) *

Se vor preciza:

- situații care impun asemenea măsuri;
- responsabilități;

- mijloace și metode de instruire și pregătire contrainformativă.

* Planul specific de pregătire a personalului este elaborat la începutul fiecărui an. În conținutul acestuia vor fi menționate responsabilitățile, termenele, mijloacele și metodele de instruire și educație protectivă. Funcționarul sau structura de securitate va ține evidență instruirilor/activităților de educație protectivă și va asigura pregătirea tuturor persoanelor avizate pentru acces la informații clasificate, care nu au participat la instruirile organizate.

Întocmit

(numele, prenumele și semnătura funcționarului de securitate)

Răspunderea pentru întocmirea, avizarea și aplicarea programului de prevenire a scurgerii de informații clasificate revine conducătorului unității deținătoare.

Programul de prevenire a scurgerii de informații clasificate se actualizează, anual sau ori de câte ori se impune (identificarea unor noi riscuri și vulnerabilități, apariția unor noi situații sau acte normative), modificările efectuate aducându-se de fiecare dată la cunoștință instituției abilitate, unde se transmite sub formă de completare pentru a fi avizat.

Se întocmește în 2 exemplare (un exemplar la beneficiar și unul la instituția abilitată).

ANEXA Nr. 10/A

LOCURI UNDE SE CONCENTREAZĂ, DE REGULĂ ORI TEMPORAR, DATE, INFORMAȚII ȘI DOCUMENTE CLASIFICATE SAU SE DESFĂȘOARĂ ASTFEL DE ACTIVITĂȚI

De la caz la caz, pentru fiecare zonă administrativă, zonă de securitate sau incintă în care se desfășoară activități, se lucrează cu/se gestionează informații clasificate vor fi menționate măsurile de securitate protectivă existente și garanțiile pe care le prezintă în protecția informațiilor și activităților clasificate. De asemenea, se vor menționa sarcinile și atribuțiile ce trebuie îndeplinite conform Regulamentului de organizare și funcționare internă.

Măsurile de protecție fizică a încăperilor și locurilor unde se păstrează sau se manipulează informații clasificate sau se desfășoară astfel de activități se vor organiza și implementa în funcție de zonele de securitate. Accesul în zonele de securitate și încăperile în care se derulează activități ori se lucrează cu informații clasificate va fi permis exclusiv persoanelor abilitate, potrivit nivelurilor de clasificare, cu respectarea principiului "nevoii de a cunoaște".

Zonele în care sunt manipulate sau stocate informații clasificate trebuie organizate și administrate în aşa fel încât să corespundă uneia dintre următoarele categorii:

a) Zona de securitate clasa I, care presupune că orice persoană aflată în interiorul acesteia are acces la informații secrete de stat, de nivelul "strict secret" și "strict secret de importanță deosebită". O asemenea zonă, necesită:

- un perimetru clar definit și protejat, în care toate intrările și ieșirile sunt supravegheate;
- controlul sistemului de intrare, care să permită numai accesul persoanelor verificate corespunzător și autorizate în mod special;
- indicarea clasei și nivelului de securitate a informațiilor existente în zonă;

b) Zona de securitate clasa a II-a, care presupune că gestionarea informațiilor de nivel secret se realizează prin aplicarea unor măsuri specifice de protecție împotriva accesului persoanelor neautorizate.

O asemenea zonă necesită:

- perimetru clar definit și protejat, în care toate intrările și ieșirile sunt supravegheate;
- controlul sistemului de intrare, pentru a permite accesul neînsotit numai persoanelor verificate și autorizate să pătrundă în această zonă. Pentru toate celelalte persoane trebuie să existe

reguli de însotire, supraveghere și prevenire a accesului neautorizat la informații clasificate sau în sectoare în care sunt manipulate și stocate astfel de informații.

Incintele în care nu se lucrează zilnic 24 de ore vor fi inspectate după orele de program, pentru a verifica dacă informațiile clasificate sunt asigurate în mod corespunzător.

c) Zona administrativă

În jurul zonelor de securitate clasa I sau clasa a II-a poate fi stabilită o zonă administrativă cu perimetru vizibil definit, în interiorul căreia să existe posibilitatea de control al personalului și vehiculelor, în zona administrativă sunt permise manipularea și păstrarea numai a informațiilor secrete de serviciu.

ANEXA Nr. 10/B

MĂSURI DE PROTECȚIE FIZICĂ A CLĂDIRILOR, SPAȚIILOR/LOCURILOR UNDE SE PĂSTREAZĂ SAU SE CONCENTREAZĂ DATE, INFORMAȚII ȘI DOCUMENTE CLASIFICATE ORI SE DESFĂȘOARĂ ASTFEL DE ACTIVITĂȚI

Securitatea clădirilor

Clădirile, spațiile/locurile în care se află informații clasificate trebuie protejate împotriva accesului neautorizat.

Măsurile de protecție (grilaje la ferestre, încuietori la uși, pază la intrări, sisteme automate pentru controlul accesului, controale și patrule de securitate, sisteme de alarmă sau pentru detectarea intrușilor etc.) vor fi dimensionate în raport cu:

- a) clasa de securitate a informațiilor, suportul, volumul și modul de depozitare a acestora în clădire;
- b) calitatea containerelor în care sunt depozitate informațiile clasificate;
- c) locul de dispunere a spațiilor/locurilor unde se păstrează sau se concentrează date, informații și documente clasificate ori se desfășoară astfel de activități;
- d) caracteristicile clădirii.

Controlul intrărilor și ieșirilor

Intrările în zonele de securitate clasa I și clasa a II-a vor fi controlate prin permis de intrare sau prin un sistem special de recunoaștere personală aplicat personalului permanent, în mod obligatoriu se va institui un sistem de control al vizitatorilor pentru prevenirea accesului neautorizat la informațiile clasificate.

Se recomandă ca permisul de intrare să nu arate, în clar, identitatea organizației emitente sau locul în care detinătorul are acces. Controlul intrărilor și ieșirilor poate fi însotit de un sistem de identificare automată, care trebuie considerat suplimentar, fără a presupune o înlocuire totală a paizei.

Dacă se apreciază necesar, la intrarea sau la ieșirea din zonele de securitate clasa I sau clasa a II-a, se vor efectua controale pentru depistarea și/sau prevenirea tranzitării fără drept a informațiilor și materialelor clasificate.

Paza

Folosirea paznicilor pentru asigurarea zonelor de securitate și a informațiilor clasificate se va face numai după ce au fost verificate, li s-a acordat abilitarea de securitate corespunzătoare zonei și li s-a efectuat pregătirea de specialitate. Vor fi precizate inclusiv măsuri de control și supraveghere corespunzătoare a paznicilor.

Patrulările în zonele de securitate clasa I și clasa a II-a se vor realiza în afara orelor de program și în zilele nelucrătoare, la intervale care vor fi stabilite în funcție de amenințarea locală, pentru a exista garanția că informațiile clasificate sunt protejate în mod corespunzător.

Pentru eficientizarea sistemelor de pază, în special în zonele de securitate unde, în interesul securității, paznicii nu pot avea intrare directă, trebuie asigurate măsuri menite să prevină accesul neautorizat și să detecteze eventualele încercări de pătrundere fără drept în aceste perimetre, prin folosirea unor modalități adecvate (televiziune cu circuit închis, sisteme de alarmă sau pentru inspectare vizuală). De la caz la caz, astfel de modalități pot fi folosite și ca substitutie ale patrulelor.

Containere și încăperi de securitate

Containerele folosite pentru păstrarea informațiilor clasificate se împart în trei clase:

- clasa A: containere aprobate la nivel național pentru depozitarea informațiilor strict secrete de importanță deosebită în zone de securitate clasa I sau clasa a II-a;
- clasa B: containere aprobate la nivel național pentru păstrarea informațiilor strict secrete și secrete în zone de securitate clasa I sau clasa a II-a;
- clasa C: mobilier de birou adecvat numai pentru păstrarea informațiilor secrete de serviciu.

Încăperile de securitate sunt construite (amenajate) în zone de securitate clasa I sau clasa a II-a, unde informațiile clasificate secret de stat sunt păstrate pe rafturi deschise sau sunt expuse pe hărți, diagrame etc. Pereții, podelele, plafonanele, ușile și încuietorile acestor încăperi vor oferi o protecție echivalentă clasei containerului de securitate aprobat pentru păstrarea informațiilor clasificate respective.

Încuietori

Încuietorile folosite la containerele și încăperile de securitate în care sunt păstrate informații clasificate se împart în trei grupe astfel:

- grupa A: încuietori aprobate la nivel național pentru containerele din clasa A;
- grupa B: încuietori aprobate la nivel național pentru containerele din clasa B;
- grupa C: încuietori indicate numai pentru mobilierul de birou adecvat numai pentru păstrarea informațiilor secrete de serviciu (pentru clasa C).

Controlul cheilor și combinațiilor

Cheile containerelor și încăperilor de securitate nu trebuie scoase din clădirea sau zona de securitate în care se află documentele clasificate.

Combinațiile încuietorilor (containerelor de securitate) vor fi cunoscute numai de persoanele abilitate.

Pentru cazurile de urgență, un rând de chei suplimentare (o evidență scrisă a fiecărei combinații) vor fi păstrate în plicuri mate sigilate într-un compartiment stabilit de conducerea instituției/agentului economic, sub control corespunzător, în containere separate. Evidența fiecărei combinații trebuie păstrată în plic separat. Cheilor și plicurilor trebuie să li se asigure protecție la nivelul de securitate a informațiilor clasificate la care acestea permit accesul.

Cunoașterea combinațiilor încuietorilor de la containerele de securitate va fi restrânsă la un număr minim de persoane. Cheile și combinațiile vor fi schimbată:

- a) ori de câte ori are loc o schimbare de personal;
- b) de fiecare dată când se constată că a avut loc un compromis de natură să le facă vulnerabile;
- c) la intervale regulate, de preferință o dată la șase luni (fără a se depăși 12 luni).

Dispozitive de detectare a intrușilor

Când se folosesc sisteme de alarmă, televiziune cu circuit închis sau alte dispozitive destinate supravegherii zonelor de securitate sau protecției informațiilor clasificate, sursa de alimentare trebuie să aibă atât conectare permanentă, cât și de rezervă (eventual, o baterie reîncărcabilă). Orice defectare sau intervenție neautorizată asupra acestor sisteme trebuie să declanșeze o

alarmă sau un alt sistem de avertizare pentru personalul care monitorizează instalația respectivă.

Protecția fizică a copiatoarelor și dispozitivelor telefax

Copiatoarele și dispozitivele telefax trebuie protejate fizic, în măsura în care este necesar să se garanteze folosirea lor numai de către persoanele autorizate.

Planuri de urgență

Fiecare autoritate și instituție/agent economic vor pregăti planuri pentru protejarea informațiilor clasificate în cazuri de urgență, care să prevadă inclusiv evacuarea și distrugerea acestora atunci când este cazul.

Protecția, evacuarea și/sau distrugerea materialelor strict secrete și secrete, în cazuri de urgență, nu trebuie să afecteze protecția, evacuarea și/sau distrugerea materialelor strict secrete de importanță deosebită, sau a materialelor codificate, care vor avea totdeauna prioritate față de alte documente clasificate.

ANEXA Nr. 10/C

PROTECȚIA SISTEMELOR/SUBSISTEMELOR INFORMATICE DESTINATE PRELUĂRII, PRELUCRĂRII, STOCĂRII ȘI TRANSMITERII DE DATE ȘI INFORMAȚII CLASIFICATE ȘI A ÎNCĂPERILOR ÎN CARE ACESTEA SE AFLĂ AMPLASATE

- Administratorul și utilizatorii sistemului destinat preluării, prelucrării, stocării și transmisiei de date și informații clasificate sunt numiți de șeful instituției/agentului economic
- Administratorul, utilizatorii și persoanele care au acces la date și informații cu caracter secret de stat, procesate prin sisteme de prelucrare automată a datelor sunt supuse procedurilor de selecționare, verificare și avizare, potrivit nivelurilor de acces.
- Încăperile unde sunt amplasate sisteme/subsisteme informative destinate preluării, prelucrării, stocării și transmisiei de date și informații cu caracter secret de stat vor fi asigurate cu sisteme de supraveghere și control-acces potrivit standardelor în vigoare, corespunzător nivelurilor de clasificare a informațiilor.
- Sistemul/subsistemul informatic destinat preluării, prelucrării, stocării și transmisiei de date și informații secrete de stat va fi prevăzut cu sistem de securizare prin metode, mijloace și echipamente pentru asigurarea integrității, confidențialității și disponibilității acestora.
- Utilizarea sistemelor informative care preiau, prelucrează, stochează și transmit date cu caracter secret de stat se face pe bază de parole și coduri și chei de criptare care se păstrează în plicuri sigilate la dispoziția șefului unității.
- Accesul în sistemul/subsistemul informatic destinat preluării, prelucrării, stocării și transmiterii de date și informații clasificate se atribuie, individual și diferențiat, în conformitate cu atribuțiile de serviciu ale fiecărui utilizator pentru pornirea, utilizarea și oprirea sistemului de calcul, introducerea, citirea, modificarea, ștergerea sau transferul de date în/din bazele de date ale sistemului informatic gestionarea și manipularea cheilor de criptare/decriptare.
- Consultarea, introducerea, modificarea sau ștergerea informațiilor din baza de date se execută numai cu aprobația șefului instituției/agentului economic, asigurându-se o evidență strictă, în scopul realizării eventualei examinări ulterioare a activității, a interacțiunii utilizatorilor cu sistemele de calcul, prin memorarea momentului, tipului operației, codului utilizatorului și datelor accesate de acesta.
- Elaborarea de lucrări din bazele de date ale sistemului/subsistemului destinat preluării, prelucrării, stocării și transmiterii de date și informații clasificate se efectuează numai pe baza ordinelor rezolutive, ale conducerii unității, date pe adrese sau documente interne de lucru.

- Suportii de memorie externă (discurile, discurile portabile, dischetele, benzile magnetice, casetele de bandă magnetică, compact-discurile, discurile optice sau magneto-optice), utilizati în sistemul/subsistemu destina preluării, prelucrării, stocării și transmiterii de date și informații clasificate, au regimul documentelor cu caracter secret de stat și se păstrează la compartimentul de documente secrete, fiind supuși procedurilor restrictive identice acestora.
- Instalarea, depanarea sau modificarea configurației sistemului de calcul destinat preluării, prelucrării, stocării și transmiterii de date și informații clasificate se execută de personal abilitat, verificat contrainformativ și controlat.
- Săptămânal, administratorul sistemului informatic destinat preluării, prelucrării, stocării și transmiterii de date și informații clasificate va elmina fișierele temporare de lucru sau ieșite din uz și va verifica integritatea fișierelor stocate pe discuri.
- Intrarea și ieșirea atât a persoanelor cât și a materialelor vor fi controlate.
- În incinte în care sistemul/subsistemu poate fi modificat nu se va permite accesul unui singur angajat autorizat (se va institui regula celor doi).
- Persoane care solicită acces temporar sau intermitent în aceste încăperi vor obține aprobare de vizitator de la administratorul de sistem; vizitatorii trebuie supravegheați permanent pentru a preveni accesul la echipamentele informatiche în scopuri ilicite.

Un pericol în domeniul protecției informațiilor clasificate procesate, stocate și transmise prin sistemul de prelucrare automată a datelor îl reprezintă orice acțiune, inacțiune sau împrejurare de natură să afecteze integritatea, disponibilitatea sau confidențialitatea datelor, precum și funcționalitatea programelor și echipamentelor aferente unui sistem informatic.

Constituie pericole:

- pierderea, sustragerea, înlocuirea, alterarea sau distrugerea neautorizată ori accidentală a datelor, programelor, suportilor materiali ai acestora sau a echipamentelor aferente;
- operarea greșită în timpul preluării, prelucrării, transferului, stocării sau arhivării datelor;
- interceptarea și interpretarea transmisiilor efectuate în cadrul rețelei de calculatoare;
- forțarea accesului, accesul neautorizat sau întârzierea accesului autorizat la date, programe, suportii materiali ai acestora sau la echipamentele aferente;
- eludarea restricțiilor privind accesul la date, prin modificarea neautorizată a configurațiilor instalate, programelor sau a drepturilor de acces;
- copierea neautorizată a datelor;
- interceptarea și interpretarea radiațiilor electromagnetice sau acustice produse de echipamentele de calcul, dispozitivele de transmisie sau canalele de comunicație;
- interceptarea discuțiilor sau con vorbirilor telefonice referitoare la sistemul informatic;
- exploatarea informativă a personalului implicat în dezvoltarea, întreținerea sau exploatarea sistemului informatic;
- introducerea în exploatare de produse informaticice fără o prealabilă testare care să ofere garanții de funcționare corectă și controlată;
- păstrarea, amplasarea, exploatarea, întreținerea sau depozitarea în condiții improprii a sistemelor de calcul, suportilor materiali de date sau a dispozitivelor și echipamentelor destinate asigurării protecției și securității datelor;
- nerespectarea reglementărilor referitoare la secretul de stat sau a regulilor de compartimentare a muncii;
- nerespectarea regulilor privind depozitarea, manipularea sau distrugerea suportilor de memorie externă și a dispozitivelor și echipamentelor scoase din uz;

- nerespectarea prevederilor, metodologiilor și a documentațiilor tehnice de întreținere și exploatare a sistemelor informaticе;
- apariția de anomalii în funcționarea sistemelor de operare, pachetelor de programe sau programelor de aplicație;
- apariția de anomalii în funcționarea sistemelor informaticе;
- apariția de deranjamente ale canalelor de comunicație;
- discutarea în condiții de insecuritate sau cu persoane neautorizate, a unor aspecte privind sistemele de calcul, informațiile și datele înmagazinate;
- producerea de calamități naturale (cutremure, inundații, alunecări de teren, etc.);
- producerea de evenimente cu efect distructiv (explozii, incendii, spargeri de conducte, acte de sabotaj, acțiuni teroriste, acte de vandalism, șocuri electromagnetice, etc.);
- producerea pe orice cale de evenimente cu efecte similare.

POSIBILE PERICOLE, AMENINȚĂRI ORI ATACURI LA ADRESA SECURITĂȚII SISTEMULUI/REȚELELOR INFORMATICE

- ascultare pasivă (atac contra confidențialității): accesarea sistemului în scopul modificării informațiilor generate, transmise, stocate sau afișate pe componentele vulnerabile ale acestuia;
- intercepția: penetrarea neautorizată a sistemului, în scopul modificării informațiilor transmise pe o cale de comunicație;
- deducerea prin interferență: acțiunea unui utilizator autorizat de a corela informațiile la care are acces, în scopul deducerii unor informații clasificate la care nu are dreptul de acces;
- deghizarea ("înșelarea" mecanismelor de autentificare): însușirea și folosirea identității unui utilizator autorizat, pentru accesarea sistemului;
- crearea și utilizarea unor canale disimulate ("ocolirea" controalelor de acces) în scopul transmiterii de informații de la un utilizator autorizat către unul neautorizat;
- utilizarea așa-zisei "porți secrete" (trap-desk) pentru evitarea controalelor de acces.

ANEXA Nr. 10/D

MĂSURI DE PROTECȚIE ÎMPOTRIVA OBSERVĂRII ȘI ASCULTĂRII

Protecția împotriva ascultărilor pasive (posibile prin ascultare directă sau furnizate de comunicații nesigure) se realizează pe baza asistenței tehnice din partea instituțiilor abilitate, prin izolarea fonică a pereților, ușilor, podelelor și plafoanelor zonelor sensibile.

Protecția împotriva ascultărilor active (prin microfoane, radio-emitteri și alte dispozitive implantate) necesită inspecții de securitate tehnică și/sau fizică a structurii încăperii, accesoriilor, instalațiilor tehnico-sanitare, echipamentelor și mobilierului de birou, sistemelor de comunicații etc. Aceste inspecții vor fi realizate de instituții competente.

Zone sigure din punct de vedere tehnic

Accesul în zonele protejate împotriva ascultărilor se va controla în mod special.

Încăperile vor fi încuiate sau păzite corespunzător standardelor de securitate fizică., inclusiv când nu sunt ocupate, iar cheile vor fi tratate ca materiale clasificate. Periodic, se vor organiza inspecții fizice și/sau tehnice. De asemenea, astfel de inspecții se vor organiza, în mod obligatoriu, ca urmare a oricărei intrări neautorizate, a unei suspiciuni privind accesul personalului extern și după executarea lucrărilor de reparații, întreținere, zugrăvire, redescorare etc. Nici un obiect nu se va introduce în aceste zone, fără a fi verificat de către personal specializat în depistarea dispozitivelor de ascultare.

În mod curent, în zonele asigurate din punct de vedere tehnic nu se vor instala telefoane. Totuși, când instalarea acestora este absolut necesară, trebuie prevăzute cu un dispozitiv de deconectare pasiv.

Inspețiile de securitate tehnică în zonele unde se poartă discuții extrem de sensibile trebuie întreprinse în mod obligatoriu premergător începerii con vorbirilor, atât pentru identificarea fizică a dispozitivelor de ascultare cât și pentru verificarea sistemelor telefonice, electrice, sau de altă natură, care ar putea fi folosite ca mediu de atac.

Verificarea dotărilor electrice/electronice din birouri

Înainte de a fi folosite în zonele în care se lucrează ori se discută despre informații strict secrete de importanță deosebită și strict secrete, echipamentele de comunicații și dotările de orice fel din birouri, în principal cele electrice și electronice, trebuie verificate de specialiști în securitatea comunicațiilor, pentru a preveni transmiterea ilicită sau din neglijență a unor informații inteligibile.

În aceste zone se va organiza o evidență a tipului și numărului de inventar ale fiecărei piese de mobilier sau echipament introduse sau mutate din încăperi, care va fi păstrată sub cheie, iar cheile vor fi protejate corespunzător.

ANEXA Nr. 10/E

SOLUȚIONAREA CAZURILOA DE ÎNCĂLCARE A REGLEMENTĂRIILOR PRIVIND PROTECȚIA INFORMAȚIILOR CLASIFICATE

Cazurile de încălcare a reglementărilor de securitate vor fi comunicate imediat conducătorului instituției/agentului economic și instituțiilor abilitate.

Orice încălcare a reglementărilor de securitate va fi cercetată de persoane special desemnate, cu experiență în activitatea de securitate pentru a stabili:

- dacă și în ce mod au fost compromise informații clasificate;
- dacă persoanele neautorizate care au avut, sau ar fi putut avea acces la informații clasificate, prezintă suficientă încredere și loialitate, astfel încât rezultatul compromiterii să nu creeze prejudicii;
- măsurile de remediere, corective sau disciplinare (inclusiv juridice), care sunt recomandate.

În situația în care persoanele care au luat cunoștință de conținutul informațiilor clasificate prezintă încredere, vor fi instruite în mod corespunzător pentru a preveni disseminarea, în caz contrar se va proceda la evaluarea prejudiciului rezultat și vor fi întreprinse măsurile necesare diminuării acestuia.

Evidența încălcărilor reglementărilor de securitate

În cadrul autorităților și instituțiilor publice, agentilor economici cu capital integral sau parțial de stat și altor persoane juridice de drept public sau privat, deținătoare de informații clasificate, se va organiza evidența cazurilor de încălcare a reglementărilor de securitate, a rapoartelor de investigații și măsurilor corective întreprinse, în consecință. Aceste evidențe vor fi păstrate timp de trei ani de către structura/funcționarul de securitate și vor fi puse la dispoziție în timpul controalelor efectuate de reprezentanții autorizați ai instituțiilor abilitate.

Comunicarea compromiterilor

Informațiile clasificate sunt compromise când conținutul acestora (total sau parțial) este cunoscut de persoane neautorizate (care nu au autorizare valabilă de acces la acestea) ori când au fost supuse riscului acestei cunoșteri neautorizate (informațiile clasificate pierdute, chiar și temporar, în afara unei zone de securitate sunt considerate a fi compromise).

Instituțiile abilitate vor fi încunoștințate prin cel mai operativ sistem de comunicare asupra circumstanțelor compromiterii unor astfel de informații.

Scopul principal al comunicării compromiterii este de a da posibilitatea recuperării informațiilor, evaluării prejudiciilor și întreprinderii acțiunilor necesare sau aplicabile pentru minimalizarea consecințelor.

Informarea preliminară trebuie să conțină:

- a) o descriere a informațiilor respective (clasificare și marcare, numărul de înregistrare, numărul de exemplare, conținutul, data, emitentul);
- b) o scurtă prezentare a împrejurărilor în care a avut loc compromiterea, inclusiv data constatării, perioada în care informațiile au fost expuse compromiterii și, dacă se cunoaște, persoanele neautorizate care au avut sau ar fi putut avea acces la acestea;
- c) precizări cu privire la eventuala informare a emitentului.

La solicitarea instituțiilor abilitate, informările preliminare vor fi completate pe măsura derulării cercetărilor.

Evaluările proprii ale instituțiilor/agenților economici, referitoare la prejudiciile și acțiunile ce urmează a fi întreprinse pentru înlăturarea sau diminuarea acestora, vor fi prezentate în cel mai scurt timp instituțiilor abilitate.

Scoaterea din evidență a documentelor clasificate pierdute sau distruse

Când există indicii certe, confirmate în scris de instituțiile abilitate cu atribuții de control și investigare a compromiterii informațiilor clasificate, că documentul dat în răspundere este iremediabil pierdut (și nu rătăcit), acesta va fi scos din evidență compartimentului care l-a gestionat, numai după finalizarea cercetărilor, cu avizul instituțiilor abilitate.

ANEXA Nr. 10/F

MĂSURI DE INSTRUIRE ȘI EDUCAȚIE PROTECTIVĂ A PERSOANELOR CARE AU ATRIBUȚII PE LINIA PROTECȚIEI INFORMAȚIILOR CLASIFICATE ȘI A CELOR CARE AU ACCES LA ASTFEL DE INFORMAȚII

Educația protectivă are ca principal obiectiv instruirea persoanelor care au acces la informații clasificate în vederea aplicării măsurilor legale referitoare la protejarea informațiilor clasificate.

Educația personalului se realizează prin derularea unor activități specifice în cadrul cărora persoanelor care accesează informații clasificate le sunt prezentate:

- prevederile legislației în domeniul protecției informațiilor clasificate;
- conținutul programului de prevenire a surgerilor de informații clasificate;
- competențele instituțiilor abilitate în domeniul protecției datelor și informațiilor clasificate;
- aspectele semnificative pe linia protecției secretelor de stat cu relevanță în domeniul specific de activitate;
- mijloacele și metodele utilizate de structurile specializate în culegerea de date și informații clasificate;
- consecințele nerespectării normelor legale în domeniu;
- alte elemente de interes pentru siguranța națională.

Ca mijloace frecvent utilizate în procesul de educație protectivă se pot folosi documentare, filme de specialitate, diapositive, materiale publicitare etc.

ANEXA Nr. 11

ROMÂNIA

(UNITATEA) _____

Compartimentul _____

CONDICA DE PREDARE - PRIMIRE a cheilor de la încăperile și containerele de securitate

Nr. Crt	Numele și prenumele persoanei căreia i-a fost predată cutia cu chei	Data și ora primirii	Semnătura de primire	Nr. sigiliului	Data și ora predării	Numele și prenumele persoanei care ridică cutia cu chei	Semnătura de primire	Obs.

ANEXA Nr. 12

ROMÂNIA

(instituția) _____

Compartimentul _____

CERTIFICAT DE SECURITATE

Seria _____ **Nr.** _____ **din** _____

Prin prezentul certificat se autorizează accesul la informații secrete de stat, nivelul _____ , pentru dl./d-na (numele, prenumele, datele de identificare) _____ , angajat al instituției noastre în funcția de _____ .

Certificatul este valabil în perioada _____ .

Şeful

_____ (semnătura, stampila)

instituției,

Posesor: _____ (nume, prenume și semnătură)

ANEXA Nr. 13

ROMÂNIA

(instituția) _____

Compartimentul _____

AUTORIZAȚIE DE ACCES LA INFORMAȚII CLASIFICATE

Seria _____ **Nr.** _____ **din** _____

Prin prezenta se autorizează accesul la informații clasificate secret de stat, nivelul _____ , pentru dl./d-na (numele, prenumele, datele de identificare) _____ , angajat al instituției noastre în funcția de _____ .

Autorizația este valabilă în perioada _____.

Şeful
_____ (semnătura, stampila)

instituției,

Posesor: _____ (nume, prenume și semnătură)

ANEXA Nr. 14

ROMÂNIA

INSTITUȚIA DEJINĂTOARE

Nr. _____ din _____

Către

OFICIUL REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

În vederea eliberării certificatului de securitate/autorizației de acces la informații clasificate, nivel _____, pentru (numele, prenumele și datele de identificare ale persoanei) _____, angajat al (denumirea completă a instituției), în funcția de _____, vă rugăm să inițiați procedurile de verificare necesare.

Mentionăm că în prezent persoana deține/nu deține certificat de securitate/autorizație de acces la informații clasificate pentru nivelul _____.

Anexăm în original chestionarul de securitate corespunzător nivelului solicitat.

Semnătură
Şef instituție

ANEXA Nr. 15

Formular de bază - date personale

Nr. _____ din _____

SECRET DE SERVICIU

(după completare)
Ex. unic

SPAȚIU REZERVAT INSTITUȚIEI SOLICITANTE

Instituția solicitantă: _____

Nivelul de acces solicitat: **SECRET** || **s.s.** || **S.S.I.D.** ||

Motivul solicitării: _____

DATE GENERALE DESPRE SOLICITANT

NUME: _____

NUME ANTERIOARE: _____

PRENUME: _____

DATA NAȘTERII: _____

LOCUL NAȘTERII: sat: _____ comună: _____ oraș/municipiu: _____ județ: _____

CETĂȚENIA la naștere: _____ actuală: _____

CARTE/BULETIN DE IDENTITATE:

Seria: ____ Nr. _____ Eliberat de: _____ La data: _____

Cod numeric personal: _____

DOMICILIUL PERMANENT:

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____

Telefon fix: _____ Telefon mobil: _____

Fax: _____ E-mail: _____

DOMICILIUL FLOTANT:

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____

Telefon fix: _____ Telefon mobil: _____

Fax: _____ E-mail: _____

DOMICILII PERMANENTE ȘI FLOTANTE ÎN ULTIMII CINCI ANI:

Tipul de domiciliu: Permanent: _____ Flotant: _____

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____

Tipul de domiciliu: Permanent: _____ Flotant: _____

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____

**ADRESE ȘI REȘEDINȚE ÎN STRĂINĂTATE ÎN ULTIMII CINCI ANI:
(pentru perioade peste 3 luni)**

Perioada _____ Țara _____ Localitatea: _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____

Perioada _____ Țara _____ Localitatea: _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____

STUDII CIVILE ȘI MILITARE:

Nr. crt.	Perioada	Instituția	Felul studiilor

LIMBI STRĂINE CUNOSCUTE

Nr. crt.	Limba	Nivelul

(În cazul atestatelor se vor indica instituția și data)

SITUAȚIA MILITARĂ

Fără stagiu militar satisfăcut: |_| Militar activ: |_| În rezervă: |_|

Seria livretului militar: _____ Numărul livretului militar: _____

Eliberat de centrul militar: _____ la data: _____

PAȘAPOARTE:

Turistic

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

De serviciu

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

Diplomatic

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

CĂLĂTORII ÎN STRĂINĂTATE ÎN ULTIMII CINCI ANI:

Nr. crt.	Tara	Localitatea	Perioada	Scopul

SITUAȚIA PROFESIONALĂ:

CIVIL:

Profesia: _____

Ministerul: _____

Instituția, la care este încadrat: _____

De la data: _____

Funcția: _____

De la data: _____

Adresa de la locul de muncă: _____

Telefon: _____ Fax: _____ E-mail: _____

MILITAR:

Gradul: _____ Funcția: _____

Arma de bază: _____ Arma de încadrare: _____

Unitatea: _____

Indicativul eșalonului superior: _____

LOCURI DE MUNCĂ ÎN ULTIMII CINCI ANI:

Nr. crt.	INSTITUȚIA	PERIOADA	FUNCȚII DEJINUTE

SITUAȚIA FAMILIALĂ ACTUALĂ

Celibatar(ă): |_| Căsătorit(ă): |_| Concubinaj |_|

Despărțit(ă) în fapt: |_| Divorțat(ă): |_| Văduv(ă) |_|

Recăsătorit(ă): |_|

Alte situații: _____

Date referitoare la data și locul încheierii căsătoriei sau legate de situația actuală

DATE DESPRE PARTENERUL DE VIAȚĂ (SOȚ/SOȚIE, CONCUBIN/CONCUBINĂ)

NUME: _____

NUME ANTERIOARE: _____

PRENUMELE: _____

DATA NAȘTERII: _____

LOCUL NAȘTERII: comună: _____ oraș: _____ județ: _____

CETĂȚENIA.: la. naștere: _____ actuală: _____

PROFESIA: _____

LOCUL DE MUNCĂ: _____

DOMICILIUL PERMANENT:

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ____ Bloc: ____ Scara: ____ Etajul: ____ Apartamentul: ____ Codul poștal: _____

Telefon fix.: _____ Telefon mobil: _____

Fax: _____ E-mail: _____

DOMICILIUL FLOTANT:

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ____ Bloc: ____ Scara: ____ Etajul: ____ Apartamentul: ____ Codul poștal: _____

Telefon fix.: _____ Telefon mobil: _____

DOMICILII PERMANENTE ȘI FLOTANTE ÎN ULTIMII CINCI ANI:

Tipul de domiciliu: Permanent: _____ Flotant: _____

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ____ Bloc: ____ Scara: ____ Etajul: ____ Apartamentul: ____ Codul poștal: _____

Tipul de domiciliu: Permanent: _____ Flotant: _____

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ____ Bloc: ____ Scara: ____ Etajul: ____ Apartamentul: ____ Codul poștal: _____

Tipul de domiciliu: Permanent: _____ Flotant: _____

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ____ Bloc: ____ Scara: ____ Etajul: ____ Apartamentul: ____ Codul poștal: _____

COPII (inclusiv cei din alte căsătorii)

Nume și prenume	Data nașterii	Localitatea	Domiciliul	Locul de muncă	Funcția

DATE DESPRE PĂRINȚI**TATĂL**

NATURA RELAȚIEI: tată natural |_| tată adoptiv: |_| tată-vitreg: |_|

NUME: _____

NUME ANTERIOARE: _____

PRENUME: _____

PROFESIA: _____

DATA NAȘTERII: _____

LOCUL NAȘTERII: comună: _____ oraș: _____ județ: _____

CETĂȚENIA la naștere: _____ actuală: _____

DOMICILIUL PERMANENT:

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____

Telefon fix.: _____ Telefon mobil: _____

Fax: _____ E-mail: _____

DOMICILIUL FLOTANT:

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____

Telefon fix.: _____ Telefon mobil: _____

Fax: _____ E-mail: _____

MAMA

NATURA RELAȚIEI: mamă naturală: |_| mamă adoptivă: |_| mamă vitregă: |_|

NUME: _____

NUME ANTERIOARE: _____

PRENUME: _____

PROFESIA: _____

DATA NAȘTERII: _____

LOCUL NAȘTERII: comună: _____ oraș: _____ județ: _____

CETĂȚENIA la naștere: _____ actuală: _____

DOMICILIUL PERMANENT:

Localitatea: _____ Județul/Sectorul: _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____
Telefon fix.: _____ Telefon mobil: _____
Fax: _____ E-mail: _____

DOMICILIUL FLOTANT:

Localitatea: _____ Județul/Sectorul: _____
Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____
Telefon fix.: _____ Telefon mobil: _____
Fax: _____ E-mail: _____

DATE DESPRE FRAȚI/SURORI

NUME: _____
PRENUME: _____
DATA ȘI LOCUL NAȘTERII: _____
DOMICILIUL: _____
NUME: _____
PRENUME: _____
DATA ȘI LOCUL NAȘTERII: _____
DOMICILIUL: _____

ANTECEDENTE ȘI CAZIER

Ați fost vreodată reținut, arestat preventiv, anchetat, pus sub acuzare, judecat, condamnat (inclusiv la amendă penală sau interzicerea unor drepturi), grațiat, amnistiat, eliberat pe cauțiune, eliberat condiționat? DA |__| NU |__|

Ați fost vreodată anchetat administrativ, sănctionat administrativ, amendat de către poliție sau autorități civile (nu se menționează amenzile pentru abateri minore, cum sunt cele pentru parcare, dar se menționează cele pentru fapte grave, precum conducerea sub influența alcoolului sau tulburarea ordinii publice)? DA |__| NU |__|

Ați fost vreodată judecat în Consiliul de Onoare, anchetat, judecat sau condamnat de o Curte Martială, trimis într-o unitate disciplinară în timpul cât v-ați aflat în serviciul militar? DA |__| NU |__|

Dacă ați răspuns cu da la vreuna din întrebările de mai sus, detaliați în spațiul de mai jos, inclusiv perioadele și instituțiile care au sănctionat faptele dvs. .

Nr. crt.	FAPTA SĂVÂRШITĂ	PERIOADA	INSTITUȚIA

DATE DE SECURITATE

Ați fost vreodată implicat în acțiuni de: spionaj, terorism, tentative de subminare a ordinii democratice prin mijloace violente?

Solicitantul DA |__| NU |__|

Partenerul de viață DA |__| NU |__|

Ați fost vreodată membru sau simpatizant al unei grupări implicate în acțiuni menționate mai sus?

Solicitantul DA NU
Partenerul de viață DA NU

Ați fost vreodată în relații apropiate cu o persoană care a activat sau a simpatizat cu astfel de grupări?

Solicitantul DA NU
Partenerul de viață DA NU

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

Ați colaborat cu organele fostei Securități care au desfășurat activități de poliție politică?

Solicitantul DA NU
Partenerul de viață DA NU

Considerați că ați atras atenția vreunui serviciu de informații sau de securitate străin?

Solicitantul DA NU
Partenerul de viață DA NU

Considerați că au fost făcute presiuni asupra dumneavoastră sau asupra membrilor familiei dumneavoastră ca urmare a unui incident survenit pe teritoriul altor țări?

Solicitantul DA NU
Partenerul de viață DA NU

Sunteți în relații permanente de natură profesională sau personală cu cetățeni străini?

Solicitantul DA NU
Partenerul de viață DA NU

Considerați că vi s-a solicitat vreodată să furnizați informații clasificate în afara atribuțiilor de serviciu?

Solicitantul DA NU
Partenerul de viață DA NU

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

Aveți rude apropiate, din cele menționate mai sus, care locuiesc în străinătate sau care au locuit mai mult de trei luni în străinătate?

Solicitantul DA NU
Partenerul de viață DA NU

Dacă ați răspuns cu da detaliați mai jos.

Nr. crt.	NUMELE PRENUMELE	GRADUL DE RUDENIE	ȚARA	PERIOADA

DECLARAȚIE

Subsemnatul, _____

Declar că toate datele furnizate mai sus sunt reale.

Declar că am luat cunoștință de cerințele procedurii de verificare și avizare pentru acces la informațiile naționale clasificate și le accept.

Consimt ca toate datele pe care le furnizez să fie verificate, conștient fiind de consecințele legale ale declarațiilor false sau omisiunilor cu bună știință.

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

Sunt de acord ca neacordarea avizului de securitate să nu-mi fie motivată.

Data,

Semnătura,

Dată în prezență (numele și prenumele funcționarului de securitate)

Semnătura

ANEXA Nr. 16

FORMULAR SUPLIMENTAR

(se completează pentru nivelurile STRICT
SECRET și STRICT SECRET DE IMPORTANȚĂ
DEOSEBITĂ)

Nr. _____ din _____

SECRET DE SERVICIU

(după completare)

Ex. unic

SPAȚIU REZERVAT INSTITUȚIEI SOLICITANTE

Instituția solicitantă: _____

Nivelul de acces solicitat: s.s. |_| S.S.I.D. |_|

Motivul solicitării: _____

DATE PERSONALE ALE SOLICITANTULUI

NUME: _____

PRENUME: _____

DATA NAȘTERII: _____

LOCUL NAȘTERII: sat: _____ comună: _____ oraș/municipiu: _____ județ: _____

CETĂȚENIA actuală: _____

DATA COMPLETĂRII FORMULARULUI DE BAZĂ: _____

DATE SUPLIMENTARE DESPRE SOLICITANT

În afara domiciliilor, adreselor și reședințelor indicate în formularul de bază, în ultimii zece ani ați mai avut și altele?

ÎN ROMÂNIA

Perioada: _____ Județ: _____ Localitatea _____

Strada: _____ Numărul: ____ Bloc: ____ Scara: ____ Etajul: ____ Apartamentul: ____ Codul poștal: _____

Perioada: _____ Județ: _____ Localitatea _____

Strada: _____ Numărul: ____ Bloc: ____ Scara: ____ Etajul: ____ Apartamentul: ____ Codul poștal: _____

ÎN STRĂINĂTATE

Perioada: _____ Țara: _____ Localitatea _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____

Perioada: _____ Țara: _____ Localitatea _____

Strada: _____ Numărul: ___ Bloc: ___ Scara: ___ Etajul: ___ Apartamentul: ___ Codul poștal: _____

RUDE

Cumnați/cumnate

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

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

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

REFERINȚE

Nominalizați date de identificare a minimum două persoane, care sunt de acord să prezinte referințe despre dumneavoastră și care vă cunosc de cel puțin cinci ani.

Numele și prenumele	Ocupația	Locul de muncă	Domiciliul permanent	Tel/Fax	Observații

STARE DE SĂNĂTATE

Ați fost vreodată diagnosticat cu boală psihică?

Dacă răspunsul este afirmativ, detaliați:

Ați suferit incidente de natură medicală care au provocat pierderea temporară a cunoștinței?

Dacă răspunsul este afirmativ, detaliați:

Sunteți conștient de vreo altă problemă medicală, neacoperită de răspunsurile anterioare, care ar putea afecta protecția informațiilor clasificate?

Dacă răspunsul este afirmativ, detaliați:

Ați avut sau aveți probleme legate de consumul de alcool?

Dacă răspunsul este afirmativ, detaliați:

Ați consumat sau consumați substanțe care creează dependență sau droguri?

Dacă răspunsul este afirmativ, detaliați:

RELAȚIILE DE FAMILIE

Aveți neînțelegeri dese în familie:
DA NU

Detaliați cu privire la motivul acestora:

Aveți persoane în întreținere din afara căsătoriei?
DA NU Cunoscute Necunoscute

Faceți referire cu privire la relațiile pe care le aveți cu cununații/cumnatele stabilită/stabilitate în străinătate, precum și la părinții partenerului de viață stabiliți în străinătate.

DECLARAȚIE

Subsemnatul , _____

Declar că toate datele furnizate mai sus sunt reale.

Declar că am luat cunoștință de cerințele procedurii de verificare și avizare pentru acces la informațiile naționale clasificate și le accept.

Consimt ca toate datele pe care le furnizez să fie verificate, conștient fiind de consecințele legale ale declarațiilor false sau omisiunilor cu bună știință.

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

Sunt de acord ca neacordarea avizului de securitate să nu-mi fie motivată.

Data,

Semnătura,

Dată în prezență (numele și prenumele funcționarului de securitate)

Semnătura

ANEXA Nr. 17

Formular finanțier

Nr. _____ din _____
(Se completează numai pentru S.S.I.D.)

SECRET DE SERVICIU

(după completare)

Ex. unic

SPAȚIU REZERVAT INSTITUȚIEI SOLICITANTE

Instituția, solicitantă: _____

Motivul solicitării: _____

DATE GENERALE DESPRE SOLICITANT

NUME: _____

NUME ANTERIOARE: _____

PRENUME: _____

DATA NAȘTERII: _____

LOCUL NAȘTERII: sat: _____ comună: _____ oraș/municipiu: _____ județ: _____

CETĂȚENIA actuală: _____

SITUАȚIA FAMILIALĂ

Cum vă apreciați situația financiară ?
Confortabilă: Acceptabilă: Dificilă: Nu pot aprecia:

Locuință

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

Proprietate personală: Închiriată: Locuință de serviciu:

PROPRIETĂȚI MOBILE/IMOBILE

Detaliați:

Venituri și cheltuieli lunare tipice pentru dumneavoastră și partenerul de viață

Venit anual net realizat în urma activității principale. _____

Venituri suplimentare realizate din alte activități _____

Total venituri anuale pe gospodărie. _____

Evaluăți care este valoarea totală a debitelor curente care vă grevează _____

Sunteți dvs. sau partenerul de viață beneficiarii unor câștiguri provenind din jocuri de noroc sau alt gen de astfel de câștiguri: DA NU

Dacă _____ Da _____ detaliați:

Dumneavoastră și partenerul dumneavoastră de viață economisiți
Curent |__| Ocazional |__| Rar |__|

Comparativ cu anul anterior aveți obligații și datorii financiare:
Mai mari: |__| Mai mici: |__| Cam la fel: |__|

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

DA |__| NU |__|

Dacă "da", detaliați:

- denumirea societății comerciale, adresa, domeniul de activitate

- caracterul interesului (asociere, membru în Consiliul de administrație, consilier etc.)

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

Dacă da, detaliați:

- denumirea firmei, adresa, domeniul de activitate

- caracterul interesului (asociere, membru în Consiliul de administrație, consilier, contracte de
colaborare, concesionare, comision etc.)

- țara de înmatriculare.

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

DA |__| NU |__|

Dacă da, detaliați:

- motivul procedurii

- instanța judecătorească care a hotărât măsura

- autoritatea care a pus-o în aplicare

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

DA |__| NU |__|

Detaliați:

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

Detaliați:

DECLARAȚIE

Subsemnatul, _____

Declar că toate datele furnizate mai sus sunt reale.

Declar că am luat cunoștință de cerințele procedurii de verificare și avizare pentru acces la
informațiile naționale clasificate și le accept.

Consimt ca toate datele pe care le furnizez să fie verificate, conștient fiind de consecințele
legale ale declarațiilor false sau omisiunilor cu bună știință.

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

Sunt de acord ca neacordarea avizului de securitate să nu-mi fie motivată.

Data,

Semnătura,

Dată în prezență _____ (numele și prenumele funcționarului de securitate)
Semnătura

ANEXA Nr. 18

ROMÂNIA

(Instituția) _____

Compartimentul _____

REGISTRUL pentru evidența certificatelor de securitate/autorizațiilor de acces la informații clasificate

Nr. crt .	Numele, prenumele și datele de identificare ale posesorului	Funcția și departamentul/compartimentul în care își desfășoară activitatea	Nivelul de acces	Data eliberării certificatului/autorizației	Seria și numărul certificatului/autorizației	Perioada de valabilitate	Data retragerii	Motivul retragerii	Obs.

ANEXA Nr. 19

ROMÂNIA

**OFICIUL
AL INFORMAȚIILOR**
Nr. _____ din _____

**REGISTRULUI
SECRETE**

**NAȚIONAL
STAT**

Către

(Autoritatea desemnată de securitate)

În vederea eliberării avizului de securitate, nivel _____, pentru (numele, prenumele și datele de identificare ale persoanei) _____, angajat al (denumirea completă a instituției) _____, în funcția de _____, vă rugăm să inițiați procedurile de verificare necesare.

Mentionăm că în prezent persoana deține/nu deține certificat de securitate/autorizație de acces la informații clasificate pentru nivelul _____.

Anexăm în original chestionarul de securitate corespunzător nivelului solicitat.

Directorul general al Oficiului Registrului Național al Informațiilor Secrete de Stat,
(Semnătura)

ANEXA Nr. 20

ROMÂNIA

(Autoritatea desemnată de securitate)

Nr. _____ din _____

Către,

OFICIUL REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

La adresa dumneavoastră nr. _____ din _____ vă comunicăm avizarea pozitivă/negativă a accesului la informații secrete de stat de nivel _____ pentru (numele, prenumele și datele de identificare ale persoanei) _____ angajat al instituției (denumirea instituției solicitante) _____ în funcția de _____.

Şeful autorității desemnate de securitate.

ANEXA Nr. 21

ROMÂNIA

OFICIUL REGISTRULUI AL INFORMAȚIILOR SECRETE DE STAT

NAȚIONAL

Nr. _____ din. _____

Către

(Instituția solicitantă)

La adresa dumneavoastră nr. _____ din _____ vă comunicăm avizarea pozitivă/negativă a accesului la informații secrete de stat de nivel _____ pentru (numele, prenumele și datele de identificare ale persoanei) _____ angajat al instituției dvs. în funcția de _____.

Directorul general al Oficiului Registrului Național al Informațiilor Secrete de Stat,
(Semnătura,)

ANEXA Nr. 22

ROMÂNIA

(Instituția) _____

Nr. _____ din _____

Către

OFICIUL REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

Vă comunicăm eliberarea la data de _____ a certificatului de securitate/autorizației de acces la informații clasificate cu seria _____, nr. _____ pentru dl/d-na (numele, prenumele, datele de identificare) _____, angajat al instituției noastre în funcția de _____.

Certificatul/autorizația este valabilă în perioada _____, pentru accesul la informații clasificate de nivel _____.

Şeful instituției,
_____ (semnătura, stampila)

ANEXA Nr. 23

ROMÂNIA

(Instituția) _____

Compartimentul _____

REGISTRUL pentru evidența autorizațiilor speciale

Nr. Crt .	Numele, prenumele și datele de identificare ale posesorului	Denumirea și adresa completă a unității deținătorului	Data eliberării autorizați ei	Numărul și seria autorizației	Perioada de valabilitat e	Obs.

ANEXA Nr. 24

ANTETUL INSTITUȚIEI/AGENTULUI ECONOMIC

Adresă _____ Tel./Fax _____

Către ORNISS

CERERE pentru eliberarea autorizației de securitate industrială

Vă rugăm să eliberați autorizația de securitate industrială pentru _____ (denumirea completă a instituției/agentului economic) cu sediul în _____ (adresa completă) în vederea participării la proceduri de atribuire a contractelor clasificate.

Anexăm, în original, chestionarul de securitate industrială pentru obținerea autorizației de securitate.

Directorul instituției/agentului economic,
_____ (semnatura, stampila)

ANEXA Nr. 25

Secret de serviciu
(după completare)

(SE COMPLETEAZĂ NUMAI PENTRU ELIBERAREA
AUTORIZAȚIEI DE SECURITATE INDUSTRIALĂ)

CHESTIONAR de securitate industrială

1. AGENTUL ECONOMIC SOLICITANT

Denumire completă: _____

Nr. din Registrul Comerțului: _____

Data ultimei actualizări la Registrul Comerțului: _____

Denumiri anterioare (dacă este cazul): _____

Cod fiscal: _____ Cod SIRUES: _____

Stare Firmă

Adresa completă pentru sediul social:

Str. _____ nr. _____

Sectorul/județul _____ Localitatea _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Cod poștal (Căsuța poștală, dacă este cazul): _____

Adrese anterioare (dacă este cazul): _____

Statutul juridic: _____

Forma de proprietate: _____

Capitalul

Capitalul social: _____

Data ultimei modificări a capitalului social: _____

Capital subscris vărsat: _____

Capital disponibil _____

Nr. acțiuni: _____ Valoare acțiuni: _____

Acțiune nominativă. Există? Da |_| Nu |_|

Autoritatea/persoana care o deține _____

Adresa site Internet _____

Creștere preconizată _____ la data de: _____

Organograma societății (se atașează la chestionar)

Acționari persoane fizice (care dețin peste 5 % din capitalul social)

Număr _____

1. Nume, prenume _____

Data și locul nașterii _____

Nr. și seria actului de identitate _____

Adresa completă:

Str. _____ nr. _____

Sectorul/județul _____ Localitatea _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Cod poștal (Căsuța poștală, dacă este cazul): _____

Tara _____

Procentul de acțiuni/părți sociale deținut _____ % începând cu anul: _____

(În cazul în care sunt mai mulți se pot prezenta în anexă, după prezentul model)

ACTIONARI PERSOANE JURIDICE _____

AGENȚI ECONOMICI LA CARE FIRMA SOLICITANTĂ ESTE ACȚIONAR

NUMĂRUL DE AGENȚI ECONOMICI: _____

Ce reprezintă pentru dvs.?

Furnizor

Client

Altceva

PROCENTUL DE ACȚIUNI DEȚINUT _____ % Începând cu anul: _____

FIRMELE LA CARE PERSOANE DIN CONSILIUL DE ADMINISTRAȚIE SUNT ACȚIONARI:

1. Numele și prenumele persoanei: _____

DENUMIREA COMPLETĂ A FIRMEI: _____

NR. DIN REGISTRUL COMERȚULUI _____

2. CONDUCEREA AGENTULUI ECONOMIC ȘI FUNCȚIONARUL/STRUCTURA DE SECURITATE RESPONSABIL/RESPONSABILĂ

DIRECTOR GENERAL

NUME ȘI PRENUME: _____

PNUMELE TATĂLUI _____

DATA NUMIRII ÎN FUNCȚIE: _____

PREGĂTIRE PROFESIONALĂ _____

DATA NAȘTERII: _____ LOCUL: _____ ȚARA: _____

FIRME LA CARE ESTE ACȚIONAR, ÎN CONDUCERE, PROPRIETAR (DENUMIRE, ADRESĂ COMPLETĂ)

DIRECTOR ECONOMIC

NUME ȘI PRENUME: _____

PNUMELE TATĂLUI _____

DATA NUMIRII ÎN FUNCȚIE: _____

PREGĂTIRE PROFESIONALĂ _____

DATA NAȘTERII: _____ LOCUL: _____ ȚARA: _____

FIRME LA CARE ESTE ACȚIONAR, ÎN CONDUCERE, PROPRIETAR (DENUMIRE, ADRESĂ COMPLETĂ)

DIRECTOR ȘTIINȚIFIC/TEHNIC/COMERCIAL

NUME ȘI PRENUME: _____

PNUMELE TATĂLUI _____

DATA NUMIRII ÎN FUNCȚIE: _____

PREGĂTIRE PROFESIONALĂ _____

DATA NAȘTERII: _____ LOCUL: _____ ȚARA: _____

FIRME LA CARE ESTE ACȚIONAR, ÎN CONDUCERE, PROPRIETAR (DENUMIRE, ADRESĂ COMPLETĂ)

MEMBRII CONSILIULUI DE ADMINISTRAȚIE

1. NUME ȘI PRENUME: _____

PNUMELE TATĂLUI _____

Data numirii în funcție _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este |_| acționar, |_| în conducere, |_| proprietar (denumire, adresă completă):

- a)
- b)
- c) ____

2.

3.

4.

5.

3.

4.

5.

6.

Funcționarul/Structura de securitate responsabil/responsabilă cu protecția informațiilor secrete de stat din cadrul agentului economic solicitant:

Nume și prenume: _____

Prenumele tatălui _____

Funcția: _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este |_| acționar |_| în conducere |_| proprietar (denumire, adresă completă)

(Datele de la această rubrică se vor completa de către toate persoanele din structura de securitate a agentului economic)

3. DATE DESPRE PROFILUL ȘI ACTIVITATEA DESFĂȘURATĂ

Obiectul(ele) principal(e) de activitate: _____

Număr de angajați permanent: _____

Întreprinderea dvs. este distribuitorul autorizat al altor agenți economici? (situația în ultimii 5 ani)

|_| Da |_| Nu

Numele și adresa completă (dacă este cazul)

4. SCURT RAPORT PENTRU ULTIMII 3 ANI DE EXERCIȚIU FINANCIAR

Sfârșit perioadă financiară			
Active fixe - TOTAL			
Conturi în lei:			
Conturi în valută:			

Creanțe:			
Stocuri:			
Active circulante - TOTAL:			
Capital social:			
Capital vărsat:			
Împrumuturi pe termen lung:			
Împrumuturi pe termen scurt			
Datorii - TOTAL			
Total pasiv:			
Cifra de afaceri:			
Total venituri			
Total cheltuieli:			
Profit brut:			
Pierderi (unde este cazul):			

5. BONITATE ȘI GARANȚII BANCARE

Bănci cu care lucrați (se vor completa următoarele informații pentru fiecare bancă):

Denumire: _____

Adresă completă:

Str. _____ nr. _____

Sectorul/județul _____ localitatea _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Număr cont: _____

Data deschiderii contului: _____

Creditul este: garantat negarantat

Mărimea creditului: _____

Mijloace de plată la cumpărare

acreditiv ordin de plată transfer bancar condiții speciale

Altele: _____

Există reclamații împotriva firmei pentru plățile cu furnizorii sau clienții?

Da Nu

Dacă DA:

Numărul reclamațiilor: _____

Data înregistrării: _____

Pentru suma de (valoarea fiecărei plăți contestate):

Reclamația a fost rezolvată? |_| Da |_| Nu

Alte comentarii legate de aceasta: _____

6. INFORMAȚII DE SECURITATE

Considerați că firma dumneavoastră a atras atenția unui serviciu de informații sau de securitate străin?	DA	NU
Au existat cazuri când au fost solicitate informații cu caracter sensibil în afara atribuțiilor de serviciu?		
Instituția sau vreunul dintre angajați a fost implicat(ă) sau a sprijinit activități de: - spionaj		
- terorism		
- sabotaj?		
Ați avut vreodată angajați care au sprijinit sau au fost implicați în una dintre activitățile de mai sus?		
Aveți cunoștință de orice alte împrejurări, condiții (factori de risc), nedeclarate în răspunsurile precedente, care au putut influența activitatea dvs. sau a personalului din subordine, cum ar fi: obișnuința utilizării unor substanțe psihotrope, dependența de alcool, dificultăți financiare deosebite?		

7. DATE REFERITOARE LA SISTEMUL DE PROTECȚIE A INFORMAȚIILOR SECRETE DE STAT

7.1. PROTECȚIA INFORMAȚIILOR

MENTIONAȚI NIVELUL DE CLASIFICARE A INFORMAȚIILOR GESTIONATE:

|_| secrete de stat

- S.S.I.D. |_|

- S.S. |_|

- S |_|

|_| secrete de serviciu

7.1.1. LOCUL/LOCURILE UNDE SE CONCENTREAZĂ DATE ȘI INFORMAȚII SECRETE DE STAT

	DA	NU
- încăpere destinată numai protecției informațiilor		
- încăpere destinată numai sistemului/subsistemuilui de calcul destinat preluării, prelucrării, stocării și transmisiiei datelor și informațiilor secrete		

de stat		
- încăperile sunt prevăzute cu: - pereți antifonați		
- uși și încuietori speciale		
- podele și tavane speciale pentru zone sensibile		
- alte locuri unde se concentrează date și informații sau se desfășoară activități cu caracter secret de stat		

În legătură cu acestea se vor face precizări privind poziția față de punctul de acces și control, împrejurimi, garanții ce le prezintă în asigurarea protecției datelor și informațiilor ori activităților secrete de stat

7.1.2. MĂSURI DE PROTECȚIE FIZICĂ A ÎNCĂPERILOR SAU LOCURILOR UNDE SE PĂSTREAZĂ SAU SE CONCENTREAZĂ DATE ŞI INFORMAȚII SECRETE DE STAT ORI ACTIVITĂȚI CU CARACTER SECRET DE STAT

	DA	NU
Zone de securitate existente:		
Zonă de securitate clasa I/II (pentru gestionarea informațiilor secrete de stat)		
- perimetru este clar definit și protejat, având toate intrările și ieșirile controlate		
- accesul persoanelor neautorizate este permis conform prevederilor interne, cu escortă sau prin controale specifice		
Zonă administrativă (pentru manipularea și depozitarea informațiilor SECRETE DE SERVICIU)		
- perimetru oferă posibilitatea de control al personalului și/sau vehiculelor		
- sunt utilizate:		
registre și jurnale speciale pentru corespondență, evidență, transport etc.		
mape speciale de păstrare		
sigilii		
fișe de predare-primire		
ecusoane de acces		
mobilă de birou adecvată zonei administrative		
7.1.3. PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ŞI DE TELECOMUNICAȚII DESTINAT PRELUĂRII, PRELUCRĂRII, STOCĂRII ŞI TRANSMISIEI DE DATE ŞI INFORMAȚII SECRETE DE STAT		

Echipament de comunicație și de birotică existent (telefoane, fax, telex, xerox)

- în zona de securitate clasa I

- în zona de securitate clasa a II-a

Echipament informatic

- aveți acces la Internet

- este utilizat un sistem de securizare

pe server-ul principal

la nivel de utilizator

7.1.4. MĂSURI PROCEDURALE DE PROTECȚIE A INFORMAȚIILOR SECRETE DE STAT SAU A ACTIVITĂȚILOR CU CARACTER SECRET DE STAT

Aveți elaborate proceduri privind:

- clasificarea informațiilor după niveluri de securitate

- accesul pentru personalul propriu

- accesul pentru personalul din afară, inclusiv străini și reprezentanți ai mass-media

- multiplicarea, transportul și circulația documentelor în interiorul și în afara instituției, atât în timpul, cât și în afara programului de lucru

- protecția sistemului/subsistemuilui informatic și de telecomunicații

- controlul intern, activitatea de analiză și evaluare a modului în care se respectă prevederile legale în vigoare, din care să reiasă periodicitatea controalelor, cine le execută, documentele ce se întocmesc și cum se valorifică, răspunderi și sanctiuni

- instruirea personalului autorizat a avea acces

7.2. PROTECȚIA PERSONALULUI

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZĂ SĂ AIBĂ ACCES LA INFORMAȚII SECRETE DE STAT

NR. CRT.	NUME, PRENUME	PRENUME PĂRINȚI	DATĂ, LOC NAȘTERE	PROFESIE, FUNCȚIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVAȚII **

**) Se va înscrie ca mențiune dacă are/urmează să aibă acces și orice alte observații considerate necesare.

8. DATE CU PRIVIRE LA PROCESE PENALE SAU CONTRAVENȚII CA URMARE A ÎNCĂLCĂRII LEGILOR

	DA	NU
În ultimii 10 ani a fost declanșată împotriva întreprinderii dvs. o acțiune în justiție care să se fi soldat printr-o hotărâre definitivă ce a afectat grav activitatea acesteia?		
În caz de răspuns afirmativ, precizați când, de ce, denumirea instanței judecătoarești, sentința, pedeapsa și perioada de executare.		
În ultimii 5 ani întreprinderea pe care o conduceți a fost acuzată de încălcarea legii și, drept urmare, să fiți sancționat cu amendă?		
În caz de răspuns afirmativ, arătați când, cum, de ce, autoritatea care a constatat fapta și cantumul amenzii.		

Orice schimbare referitoare la datele cuprinse în chestionar se transmite imediat sub formă de completare la chestionar.

Funcția, numele, prenumele și semnătura
conducătorului unității solicitante _____

Stampila unității solicitante _____

Localitatea și data completării chestionarului

ANGAJAMENT

Subsemnatul(a) _____ (numele, inițiala tatălui, prenumele - cu majuscule) în calitate de _____ (funcția) la _____ (denumirea completă a instituției/agentului economic) cu sediul în _____ (adresa completă) certific pe propria-mi răspundere că informațiile declarate în prezentul chestionar sunt exacte.

Declar că personalul angajat care are/va avea acces la informații secrete de stat a luat la cunoștință de prevederile legale referitoare la protecția informațiilor secrete de stat și mă angajez că le voi respecta.

Am cunoștință de faptul că, dacă, prin imprudență și/sau neglijența noastră, o informație, un procedeu sau un fișier al cărui depozitar suntem și care are un nivel de clasificare, va fi distrus, deținut, sustras, reprobus sau adus la cunoștință fie publicului, fie unei persoane neautorizate, cei vinovați vor suporta consecințele potrivit legislației în vigoare.

Data _____

Semnătura _____

ANEXA Nr. 26

Secret de serviciu
(după completare)

(SE COMPLETEAZĂ NUMAI PENTRU CERTIFICATULUI DE SECURITATE INDUSTRIALĂ DE NIVEL "SECRET")

ELIBERAREA

CHESTIONAR de securitate industrială

Autorizare pentru nivelul de securitate:

|_| SECRET

1. AGENTUL ECONOMIC SOLICITANT

Denumire completă: _____

Nr. din Registrul Comerțului: _____

Data ultimei actualizări la Registrul Comerțului: _____

Denumiri anterioare (dacă este cazul): _____

Cod fiscal: _____ Cod SIRUES: _____

Stare Firmă

Adresa completă pentru sediul social:

Str. _____ nr. _____

Sectorul/județul _____ Localitatea _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Cod poștal (Căsuța poștală, dacă este cazul): _____

Adrese anterioare (dacă este cazul): _____

Statutul juridic: _____

Forma de proprietate: _____

Capitalul

Capitalul social: _____

Data ultimei modificări a capitalului social: _____

Capital subscris vărsat: _____

Capital disponibil _____

Nr. acțiuni/părți sociale: _____ Valoare acțiuni/părți sociale: _____

Acțiune nominativă. Există? Da |_| Nu |_|

Autoritatea/persoana care o deține _____

Adresa site Internet _____

Creștere preconizată _____ la data de: _____

Organigrama societății (se atașează la chestionar)

Acționari persoane fizice (care dețin peste 5 % din capitalul social)

Număr _____

1. Nume, prenume _____

Data și locul nașterii _____

Nr. și seria actului de identitate _____

Adresa completă:

Str. _____ nr. _____

Sectorul/județul _____ Localitatea _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Cod poștal (Căsuța poștală, dacă este cazul): _____

Țara _____

Procentul de acțiuni/părți sociale deținut _____ % începând cu anul: _____

(În cazul în care sunt mai mulți se pot prezenta în anexă, după prezentul model)

ACTIONARI persoane juridice _____

AGENȚI economici la care firma solicitantă este acționar

Numărul de agenți economici: _____

Ce reprezintă pentru dvs.?

Furnizor

Client

Altceva

Procentul de acțiuni/părți sociale deținut _____ % începând cu anul: _____

Firmele la care persoane din consiliul de administrație sunt acționari:

1. Numele și prenumele persoanei: _____

Denumirea completă a firmei: _____

Nr. din Registrul Comerțului _____

2. AUTORIZAREA DEJA OBȚINUTĂ

Autorizație: Da Nu

Numărul și seria autorizației de securitate:

Valabilă de la: _____ la _____

Autoritatea emitentă: _____

3. CONDUCEREA ÎNTreprinderii și FUNCȚIONARUL/STRUCTURA DE SECURITATE RESPONSABIL/RESPONSABILĂ

Director general

Nume și prenume: _____

Prenumele tatălui _____

Data numirii în funcție: _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar (denumire, adresă completă)

Director economic

Nume și prenume: _____

Prenumele tatălui _____

Data numirii în funcție _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar (denumire, adresă completă)

Director științific/tehnic/comercial

Nume și prenume: _____

Prenumele tatălui _____

Data numirii în funcție: _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar (denumire, adresă completă)

Membrii consiliului de administrație

1. Nume și prenume: _____

Prenumele tatălui _____

Data numirii în funcție _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar

Membrii Consiliului de Administrație

1. Nume și prenume: _____

Prenumele tatălui _____

Data numirii în funcție _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar (denumire, adresă completă):

a)

b)

c) ____

2.

3.

4.

5.

6.

Funcționarul/Structura de securitate responsabil/responsabilă cu protecția informațiilor secrete de stat din întreprinderea solicitantă:

Nume și prenume: _____

Prenumele tatălui _____

Funcția: _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar (denumire, adresă completă) (Datele de la această rubrică se vor completa de către toate persoanele din structura de securitate a agentului economic.)

4. DATE DESPRE PROFILUL ȘI ACTIVITATEA DESFĂȘURATĂ

Obiectul(ele) principal(e) de activitate: _____

Număr de angajați permanent: _____

Întreprinderea dvs. este distribuitorul autorizat al altor agenți economici? (situația în ultimii 5 ani)

Da Nu

Numele și adresa completă (dacă este cazul) _____

Mărci înregistrate

Nume și descriere (ce reprezintă) _____

Cărui tip de clienți se adresează activitatea/serviciile/produsele dvs.? _____

5. BONITATE ȘI GARANȚII BANCARE

Bănci cu care lucrați (se vor completa următoarele informații pentru fiecare bancă):

Denumire: _____

Adresă completă:

Str. _____ nr. _____

Sectorul/județul _____ localitatea _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Număr cont: _____

Data deschiderii contului: _____

Creditul este: garantat negarantat

Mărimea creditului: _____

Mijloace de plată la cumpărare

acreditiv ordin de plată transfer bancar condiții speciale

Altele: _____

Există reclamații împotriva firmei pentru plățile cu furnizorii sau clienții?

Da Nu

Dacă DA:

Numărul reclamațiilor: _____

Data înregistrării: _____

Pentru suma de (valoarea fiecărei plăți contestate): _____

Reclamația a fost rezolvată? Da Nu

Alte comentarii legate de aceasta: _____

6. SCURT RAPORT PENTRU ULTIMII 3 ANI DE EXERCIȚIU FINANCIAR

Sfârșit perioadă financiară			
Active fixe - TOTAL			
Conturi în lei:			
Conturi în valută:			
Creanțe:			
Stocuri:			
Active circulante - TOTAL:			
Capital social:			
Capital vărsat:			
Împrumuturi pe termen lung:			
Împrumuturi pe termen scurt			
Furnizori și conturi asimilate:			
Datorii - TOTAL			
Total pasiv:			
Cifra de afaceri:			
Total venituri			
Total cheltuieli:			
Profit brut:			
Pierderi (unde este cazul):			
Venituri din export			
Trezoreria netă:			

7. INFORMAȚII DE SECURITATE

Considerați că firma dumneavoastră a atras atenția unui serviciu de informații sau de securitate străin?	DA	NU
Au existat cazuri când au fost solicitate informații cu caracter sensibil în afara atribuțiilor de serviciu?		

Instituția sau vreunul dintre angajați a fost implicat(ă) sau a sprijinit activități de: - spionaj		
- terorism		
- sabotaj?		
Ați avut vreodată angajați care au sprijinit sau au fost implicați în una dintre activitățile de mai sus?		
Aveți cunoștință de orice alte împrejurări, condiții (factori de risc), nedeclarate în răspunsurile precedente, care au putut influența activitatea dvs. sau a personalului din subordine, cum ar fi: obișnuința utilizării unor substanțe psihotrope, dependența de alcool, dificultăți financiare deosebite?		

8. DATE REFERITOARE LA SISTEMUL DE PROTECȚIE A INFORMAȚIILOR SECRETE DE STAT

8.1. PROTECȚIA INFORMAȚIILOR

8.1.1. LOCUL/LOCURILE UNDE SE CONCENTREAZĂ DATE ȘI INFORMAȚII SECRETE DE STAT

	DA	NU
- încăpere destinată numai protecției informațiilor		
- încăpere destinată numai sistemului/subsistemuui de calcul destinat preluării, prelucrării, stocării și transmisiei datelor și informațiilor secrete de stat		
- încăperile sunt prevăzute cu: - pereți antifonați		
- uși și încuietori speciale		
- podele și tavane speciale pentru zone sensibile		
- alte locuri unde se concentrează date și informații sau se desfășoară activități cu caracter secret de stat		

În legătură cu acestea se vor face precizări privind poziția față de punctul de acces și control, împrejurimi, garanții ce le prezintă în asigurarea protecției datelor și informațiilor ori activităților secrete de stat.

8.1.2. MĂSURI DE PROTECȚIE FIZICĂ A ÎNCĂPERILOR SAU LOCURILOR UNDE SE PĂSTREAZĂ SAU SE CONCENTREAZĂ DATE ȘI INFORMAȚII SECRETE DE STAT ORI ACTIVITĂȚI CU CARACTER SECRET DE STAT

	DA	NU
Zone de securitate existente: Zonă de securitate clasa a II-a (pentru gestionarea informațiilor până la nivelul SECRET, cu acces		

neautorizat conform prevederilor interne, cu escortă sau prin controale specifice)		
- perimetru este clar definit și protejat, având toate intrările și ieșirile controlate		
- accesul persoanelor neautorizate este permis conform prevederilor interne, cu escortă sau prin controale specifice		
Zonă administrativă (pentru manipularea și depozitarea informațiilor SECRETE DE SERVICIU)		
- perimetru oferă posibilitatea de control al personalului și/sau vehiculelor		
- sunt utilizate:		
registre și jurnale speciale pentru corespondență, evidență, transport etc.		
mape speciale de păstrare		
sigilii		
fișe de predare-primire		
ecusoane de acces		
mobilă de birou adecvată zonei administrative		
8.1.3. PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ȘI DE TELECOMUNICAȚII DESTINAT PRELUĂRII, PRELUCRĂRII, STOCĂRII ȘI TRANSMISIEI DE DATE ȘI INFORMAȚII SECRETE DE STAT		
Echipament de comunicație și de birotică existent (telefoane, fax, telex, xerox)		
- în zona de securitate clasa I		
- în zona de securitate clasa a II-a		
Echipament informatic		
- aveți acces la Internet		
- este utilizat un sistem de securizare		
pe server-ul principal		
la nivel de utilizator		
8.1.4. MĂSURI PROCEDURALE DE PROTECȚIE A INFORMAȚIILOR SECRETE DE STAT SAU A ACTIVITĂȚILOR CU CARACTER SECRET DE STAT		
Aveți elaborate proceduri privind:		

- clasificarea informațiilor după niveluri de securitate		
- accesul pentru personalul propriu		
- accesul pentru personalul din afară, inclusiv străini și reprezentanți ai mass-media		
- multiplicarea, transportul și circulația documentelor în interiorul și în afara instituției, atât în timpul, cât și în afara programului de lucru		
- protecția sistemului/subsistemului informatic și de telecomunicații		
- controlul intern, activitatea de analiză și evaluare a modului în care se respectă prevederile legale în vigoare, din care să reiasă periodicitatea controalelor, cine le execută, documentele ce se întocmesc și cum se valorifică, răspunderi și sanctiuni		
- instruirea personalului autorizat a avea acces		

8.2. PROTECȚIA PERSONALULUI

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZĂ SĂ AIBĂ ACCES LA INFORMAȚII SECRETE DE STAT

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZĂ SĂ AIBĂ ACCES LA INFORMAȚII SECRETE DE STAT							
NR. CRT.	NUME, PRENUME	PRENUME PĂRINȚI	DATĂ, LOC NAȘTERE	PROFESIE, FUNCȚIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVAȚII **

**) Se va înscrive ca mențiune dacă are/urmează să aibă acces și orice alte observații considerate necesare.

9. DATE CU PRIVIRE LA PROCESE PENALE SAU CONTRAVENȚII CA URMARE A ÎNCĂLCĂRII LEGILOR

	DA	NU
În ultimii 10 ani a fost declanșată împotriva întreprinderii dvs. o acțiune în justiție?		
În caz de răspuns afirmativ, precizați când, de ce, denumirea instanței judecătorești, sentința, pedeapsa și perioada de executare.		
În ultimii 5 ani întreprinderea pe care o conduceți a fost acuzată de încălcarea legii?		
În caz de răspuns afirmativ, arătați când, cum, de ce, autoritatea care a constatat fapta și quantumul amenzii.		

Orice schimbare referitoare la datele cuprinse în chestionar se transmite imediat sub formă de completare la chestionar.

Funcția, numele, prenumele și semnătura
conducătorului unității solicitante _____

Stampila unității solicitante _____
Localitatea și data completării chestionarului

ANGAJAMENT

Subsemnatul(a) _____ (numele, inițiala tatălui, prenumele - cu majuscule) în calitate de _____ (funcția) la _____ (denumirea completă a instituției/agentului economic) cu sediul în _____ (adresa completă) certific pe propria-mi răspundere că informațiile declarate în prezentul chestionar sunt exacte.

Declar că personalul angajat care are/va avea acces la informații secrete de stat a luat la cunoștință de prevederile legale referitoare la protecția informațiilor secrete de stat și mă angajez că le voi respecta.

Am cunoștință de faptul că, dacă, prin imprudență și/sau neglijența noastră, o informație, un procedeu sau un fișier al cărui depozitar suntem și care are un nivel de clasificare, va fi distrus, deturat, sustras, reprobus sau adus la cunoștință fie publicului, fie unei persoane neautorizate, cei vinovați vor suporta consecințele potrivit legislației în vigoare.

Data _____

Semnătura _____

ANEXA Nr. 27

Secret de serviciu
(după completare)

(SE COMPLETEAZĂ NUMAI PENTRU ELIBERAREA CERTIFICATULUI DE SECURITATE INDUSTRIALĂ DE NIVEL "STRICT SECRET" ȘI "STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ")

Observație! Pentru nivelul "STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ" se completează și rubricile cu **.

CHESTIONAR de securitate industrială

Autorizare pentru nivelul de securitate:

STRICT SECRET

* STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ

1. AGENTUL ECONOMIC SOLICITANT

Denumire completă: _____

Nr. din Registrul Comerțului: _____

Data ultimei actualizări la Registrul Comerțului: _____

Denumiri anterioare (dacă este cazul):

Cod fiscal: _____ Cod SIRUES: _____

Stare Firmă

Adresa completă pentru sediul social:

Str. _____ nr. _____

Sectorul/județul _____ localitatea _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Cod poștal (căsuța poștală, dacă este cazul): _____

Adrese anterioare (dacă este cazul): _____

Statutul juridic _____

Forma de proprietate: _____

Capitalul

Capitalul social: _____

Data ultimei modificări a capitalului social: _____

Capitalul subscris vărsat: _____

Capital disponibil _____

Nr. acțiuni/părți sociale: _____ Valoarea unei acțiuni/părți sociale: _____

Acțiune nominativă. Există? Da Nu

Autoritatea/persoana care o deține _____

Adresa site Internet _____

Creștere preconizată _____ la data de: _____

Organograma societății (se atașează la chestionar)

Asociați persoane fizice (care dețin peste 5 % din capitalul social)

Număr _____

1. Nume, prenume _____

Data și locul nașterii _____

Nr. și seria actului de identitate _____

Adresa completă:

Str. _____ nr. _____

Sectorul/județul _____ localitatea _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Cod poștal (căsuța poștală, dacă este cazul): _____

Tara _____

Procentul de acțiuni/părți sociale deținut _____ % începând cu anul: _____

(În cazul în care sunt mai mulți, se pot prezenta în anexă, după prezentul model.)

Asociați persoane juridice

Se completează un chestionar identic cu cel al agentului economic solicitant, până la capitolul 7 inclusiv, de către acționarii care nu dețin autorizație/certificat de securitate.

* Agenți economici la care firma solicitantă este asociată

Numărul de agenți economici: _____

Pentru fiecare agent economic se vor completa următoarele date:

Denumirea: _____

Adresa completă:

Str. _____ nr. _____

Sectorul/județul _____ localitatea _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Cod poștal (căsuța poștală, dacă este cazul): _____

Țara _____

Ce reprezintă pentru dvs.?

Furnizor

Client

Altceva

Procentul de acțiuni/părți sociale deținut _____ % începând cu anul: _____

* Firmele la care persoane din consiliul de administrație sunt acționari

1. Numele și prenumele persoanei: _____

Denumirea completă a firmei: _____

Nr. din Registrul Comerțului _____

2. NIVELUL DE AUTORIZARE DEJA OBȚINUT

Autorizație/Certificat obținut Da Nu

Nivelul de acces al certificatului deținut:

Seria și numărul autorizației/certificatului de securitate:

Valabil de la: _____ la _____

Autoritatea emitentă: _____

3. CONDUCEREA ÎNTreprinderii și FUNCȚIONARUL/STRUCTURA DE SECURITATE

Director general

Nume și prenume: _____

Prenumele tatălui _____

Data numirii în funcție: _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar (denumire, adresă completă)

Director economic

Nume și prenume: _____

Prenumele tatălui _____

Data numirii în funcție: _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar (denumire, adresă completă)

Director științific/tehnic/comercial

Nume și prenume: _____

Prenumele tatălui _____

Data numirii în funcție: _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar (denumire, adresă completă)

Membrii consiliului de administrație

1. Nume și prenume: _____

Prenumele tatălui _____

Data numirii în funcție _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar (denumire, adresă completă):

a)

b)

c) ____

2.

3.

4.

5.

6.

Funcționarul/Structura de securitate responsabil/responsabilă cu protecția informațiilor clasificate din instituția solicitantă:

Nume și prenume: _____

Prenumele tatălui _____

Funcția: _____

Pregătire profesională _____

Data nașterii: _____ locul: _____ țara _____

Firme la care este acționar, în conducere, proprietar (denumire, adresă completă)

(Datele de la această rubrică se vor completa de către toate persoanele din structura de securitate a agentului economic.)

* 4. SUCURSALE, FILIALE SAU PUNCTE DE LUCRU

* Denumire completă:

Denumiri anterioare (dacă este cazul):	Datele schimbărilor
--	---------------------

* Adresa completă:

Str. _____ nr. _____

Sectorul/județul _____ localitatea _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Cod poștal (căsuța poștală, dacă este cazul): _____

Tara _____

Adrese anterioare (dacă este cazul): _____

* Forma de deținere a spațiului:	<input type="checkbox"/> proprietate Numărul actului și forma juridică: _____	<input type="checkbox"/> închiriată De la (denumire, adresă completă): _____
----------------------------------	--	---

* Agentul economic deține:

birouri magazine hoteluri fabrici depozite

ateliere laboratoare șantiere spații de prezentare

camere securizate Altele: _____

* Descrierea amplasamentului sediului:

zonă comercială centrală zonă comercială periferică zonă rurală

zonă industrială incintă comercială zonă rezidențială

* Spații subînchiriate altor agenți economici, cu specificarea denumirii și obiectului lor de activitate: _____

5. DATE DESPRE PROFILUL ȘI ACTIVITATEA DESFĂȘURATĂ

Obiectul(e) principal(e) de activitate: _____

Număr de angajați permanent: _____

Cu studii superioare: _____

Cu studii medii: _____

Personal auxiliar: _____

Număr de colaboratori

Persoane fizice _____

Persoane juridice _____

* Vânzări la intern (situația în ultimii 5 ani)

Procentul din vânzările totale _____

Termenele de livrare (în zile) _____

Condiții de plată (numerar, cec, ordin de plată, cont curent etc.) _____

* Importuri (situația în ultimii 5 ani)

Procentul importurilor la realizarea produselor _____

Ce se importă (materie primă și/sau ansamblu, subansamblu, produse finite) _____

Tările de unde se importă: _____

Termene de import (în zile) _____

Condiții de plată (numerar, cec, ordin de plată, cont curent etc.) _____

* Exporturi (situația în ultimii 5 ani)

Procent din activitate reprezentat de importuri: _____

Ce se exportă (materie primă și/sau ansamblu, subansamblu, produse finite) _____

Tările în care se exportă: _____

Termene de export (în zile) _____

Condiții de plată (numerar, cec, ordin de plată, cont curent etc.) _____

Instituția dvs. este distribuitorul autorizat al altor agenți economici? (situația în ultimii 5 ani)

|_| Da |_| Nu

Numele și adresa completă (dacă este cazul) _____

Mărci înregistrate

Nume și descriere (ce reprezintă) _____

Căror tip de clienți se adresează activitatea/serviciile/produsele dvs.? _____

* Principalii clienți cu care instituția dvs. are contract (denumire, adresă completă)	Valoarea fiecărui contract	Perioada
---	-------------------------------	----------

6. BONITATE ȘI GARANȚII BANCARE

Bănci cu care lucrați (se vor completa următoarele informații pentru fiecare bancă):

Denumire: _____

Adresă completă:

Str. _____ nr. _____

Sectorul/județul _____ localitate _____

Nr. telefon _____ fax: _____

Telex _____ e-mail _____

Adresă site Internet _____

Număr cont: _____

Data deschiderii contului: _____

Creditul este: |_| garantat |_| negarantat

Mărimea creditului: _____

Natura garanției (dacă este credit "garantat"): _____

* Creditul este utilizat în totalitate? |_| Da |_| Nu

* Banca a acordat facilitatea de neacoperire a contului? |_| Da |_| Nu

* Dacă DA, până la ce sumă poate merge neacoperirea: _____

* Dacă DA, această facilitate este folosită? |_| Da |_| Nu

Mijloace de plată la cumpărare

acreditiv ordin de plată transfer bancar condiții speciale

Altele: _____

Există reclamații împotriva firmei?

Da Nu

Dacă DA:

Numărul reclamațiilor: _____

Data înregistrării: _____

Pentru suma de (valoarea fiecărei plăți contestate): _____

Reclamația a fost rezolvată: Da Nu

Alte comentarii legate de aceasta: _____

* Planuri viitoare (noi investiții, pătrundere pe noi piețe etc.) _____

7. SCURT RAPORT PENTRU ULTIMII 3 ANI DE EXERCIȚIU FINANCIAR

Sfârșit perioadă financiară			
Active fixe - TOTAL			
Conturi în lei:			
Conturi în valută:			
Creanțe:			
Stocuri:			
Active circulante - TOTAL:			
Total active:			
Capital social:			
Capital vărsat:			
Capitaluri proprii:			
Împrumuturi pe termen lung:			
Împrumuturi pe termen scurt			
Furnizori și conturi asimilate:			
Datorii - TOTAL			
Total pasiv:			
Cifra de afaceri:			
Total venituri			

Total cheltuieli:			
Profit brut:			
Pierderi (unde este cazul):			
Venituri din export			
Trezoreria netă:			

8. INFORMAȚII DE SECURITATE

	DA	NU
Considerați că firma dumneavoastră a atras atenția unui serviciu de informații sau de securitate străin?		
Credeți că au fost făcute presiuni asupra firmei sau angajaților ca urmare a unui incident survenit pe teritoriul altei țări?		
Sunt menținute relații permanente, profesionale, personale cu cetăteni străini ? Natura acestora.		
Au existat cazuri când au fost solicitate informații cu caracter sensibil în afara atribuțiilor de serviciu?		
Întreprinderea sau vreunul din angajați a fost implicat(ă) sau a sprijinit activități de: spionaj		
terorism		
sabotaj?		
Ați avut vreodată angajați care au sprijinit sau au fost implicați într-una dintre activitățile de mai sus?		
Aveți cunoștință de orice alte împrejurări, condiții (factori de risc), nedeclarate în răspunsurile precedente, care au putut influența activitatea dvs. sau a personalului din subordine, cum ar fi: obișnuința utilizării unor substanțe psihotrope, dependența de alcool, dificultăți financiare deosebite?		

9. DATE REFERITOARE LA SISTEMUL DE PROTECȚIE A INFORMAȚIILOR SECRETE DE STAT

9.1. PROTECȚIA INFORMAȚIILOR

9.1.1. LOCUL/LOCURILE UNDE SE CONCENTREAZĂ DATE ȘI INFORMAȚII SECRETE DE STAT		
	DA	NU
- încăpere destinată numai protecției informațiilor secrete de stat		

- încăpere destinată numai sistemului/subsistemuui de calcul destinat preluării, prelucrării, stocării și transmisiei datelor și informațiilor secrete de stat		
- încăperile sunt prevăzute cu: - pereți antifonați		
- uși și încuietori speciale		
- podele și tavane speciale pentru zone sensibile		
- alte locuri unde se concentrează date și informații sau se desfășoară activități cu caracter secret de stat		

În legătură cu acestea se vor face precizări privind poziția față de punctul de acces și control, împrejurimi, garanții ce le prezintă în asigurarea protecției datelor și informațiilor ori activităților secrete de stat _____

9.1.2. MĂSURI DE PROTECȚIE FIZICĂ A ÎNCĂPERILOR SAU LOCURILOR UNDE SE PĂSTREAZĂ SAU SE CONCENTREAZĂ DATE ȘI INFORMAȚII SECRETE DE STAT ORI ACTIVITĂȚI CU CARACTER SECRET DE STAT		
	DA	NU

Zone de securitate existente:

Zonă de securitate clasa I (pentru gestionarea informațiilor până la nivelul STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ, cu acces autorizat)

- perimetru este clar definit și protejat, având toate intrările și ieșirile controlate		
- este marcată zona specificarea restricției și menționarea zonei de securitate		
- există control al sistemului de intrare, care să permită doar accesul persoanelor autorizate pentru intrarea în zonă		

(Dacă DA, descrieți sistemul(e) de protecție mecanică, electrică, electronică, informațională, optică, acustică etc.)

- sistemul de protecție utilizat este omologat și/sau aprobat de un serviciu specializat		
--	--	--

(Dacă DA, menționați care.)

Zonă de securitate clasa a II-a (pentru gestionarea informațiilor până la nivelul SECRET, cu acces neautorizat conform prevederilor interne, cu escortă sau prin controale specifice)

- perimetru este clar definit și protejat, având toate intrările și ieșirile controlate		
- accesul persoanelor neautorizate este permis conform prevederilor		

interne, cu escortă sau prin controale specifice		
Zonă administrativă (pentru manipularea și depozitarea informațiilor SECRETE DE SERVICIU)		
- perimetru oferă posibilitatea de control a personalului și/sau vehiculelor		
- sunt utilizate:		
registre și jurnale speciale pentru corespondență, evidență, transport etc.		
mape speciale de păstrare		
sigilii		
fișe de predare-primire		
ecusoane de acces		
mobilă de birou adecvată zonei administrative		
9.1.3. PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ȘI DE TELECOMUNICATII DESTINAT PRELUĂRII, PRELUCRĂRII, STOCĂRII ȘI TRANSMISIEI DE DATE ȘI INFORMATII SECRETE DE STAT		
Echipament de comunicație și de birotică existent (telefoane, fax, telex, xerox)		
- în zona de securitate clasa I		
- în zona de securitate clasa a II-a		
Echipament informatic		
- număr calculatoare _____		
- utilizați calculatoarele în rețea Intranet		
- aveți acces la Internet		
- este utilizat un sistem de securizare		
pe server-ul principal		
la nivel de utilizator		
* Menționați tipul server-ului principal și distribuitorul, administratorul (în cazul în care este o firmă specializată care asigură servicii), precum și locul/locurile unde sunt amplasate calculatoarele conectate în rețea la server-ul care stochează informații clasificate		
9.1.4. MĂSURI PROCEDURALE DE PROTECȚIE A INFORMATIILOR SECRETE DE STAT SAU A ACTIVITĂȚILOR CU CARACTER SECRET DE STAT		
Aveți elaborate proceduri privind:		

- clasificarea informațiilor după niveluri de securitate		
- accesul pentru personalul propriu		
- accesul pentru personalul din afară, inclusiv străini și reprezentanți ai mass-media		
- multiplicarea, transportul și circulația documentelor în interiorul și în afara întreprinderii, atât în timpul cât și în afara programului de lucru		
- protecția sistemului/subsistemuinformatic și de telecomunicații		
- controlul intern, activitatea de analiză și evaluare a modului în care se respectă prevederile legale în vigoare, din care să reiasă periodicitatea controalelor, cine le execută, documentele ce se întocmesc și cum se valorifică, răspunderi și sanctiuni		
- instruirea personalului autorizat a avea acces		

9.2. PROTECȚIA PERSONALULUI

9.2.1. LISTA PERSOANELOR CARE AU ACCES SAU URMEAZĂ SĂ AIBĂ ACCES LA INFORMAȚII SECRETE DE STAT

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZĂ SĂ AIBĂ ACCES LA INFORMAȚII SECRETE DE STAT							
NR. CRT.	NUME, PRENUME	PRENUME PĂRINȚI	DATĂ, LOC NAȘTERE	PROFESIE, FUNCȚIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVAȚII **

**) Se va înscrie ca mențiune dacă are/urmează să aibă acces și orice alte observații considerate necesare.

9.2.2. LISTA PERSOANELOR AUTORIZATE SĂ ADMINISTREZE SISTEMUL/SUBSISTEMUL INFORMATIC ȘI DE TELECOMUNICAȚII, PRECUM ȘI CEI CARE LUCREAZĂ ÎN REȚEAUA INTRANET CU ACCES LA INFORMAȚII SECRETE DE STAT

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZĂ SĂ AIBĂ ACCES LA INFORMAȚII SECRETE DE STAT							
NR. CRT.	NUME, PRENUME	PRENUME PĂRINȚI	DATĂ, LOC NAȘTERE	PROFESIE, FUNCȚIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVAȚII **

*) Se va înscrie echipamentul pe care-l administrează sau faptul că are acces Intranet.

10. DATE CU PRIVIRE LA PROCESE PENALE SAU CONTRAVENȚII CA URMARE A ÎNCĂLCĂRII LEGILOR

	DA	NU
În ultimii 10 ani a fost declanșată împotriva întreprinderii dvs. o acțiune în justiție?		
În caz de răspuns afirmativ, precizați când, de ce, denumirea instanței judecătorești, sentința, pedeapsa și perioada de executare.		
În ultimii 5 ani întreprinderea pe care o conduceți a fost acuzată de încălcarea legii?		

În caz de răspuns afirmativ, arătați când, cum, de ce, autoritatea care a constatat fapta și cantumul amenzii.

Orice schimbare referitoare la datele cuprinse în chestionar se transmite imediat sub formă de completare la chestionar.

Funcția, numele, prenumele și semnătura
conducătorului unității solicitante _____

Stampila unității solicitante _____

Localitatea și data completării chestionarului

ANGAJAMENT ⁽¹⁾

Subsemnatul(a) _____ (numele, inițiala tatălui, prenumele - cu majuscule) în calitate de _____ (funcția) la _____ (denumirea completă a instituției/agentului economic) cu sediul în _____ (adresa completă) certific pe propria-mi răspundere că informațiile declarate în prezentul chestionar sunt exacte.

Declar că personalul angajat care are/va avea acces la informații secrete de stat a luat la cunoștință de prevederile legale referitoare la protecția informațiilor secrete de stat și mă angajez că le voi respecta.

Am cunoștință de faptul că, dacă, prin imprudență și/sau neglijența noastră, o informație, un procedeu sau un fișier al cărui depozitar suntem și care are un nivel de clasificare, va fi distrus, deținut, sustras, reprobus sau adus la cunoștință fie publicului, fie unei persoane neautorizate, cei vinovați vor suporta consecințele potrivit legislației în vigoare.

Data _____

Semnătura _____

⁽¹⁾ Se completează atât pentru nivelul "STRICT SECRET", cât și pentru nivelul "STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ".

ANEXA Nr. 28

ROMÂNIA

OFICIUL REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

AUTORIZAȚIE DE SECURITATE INDUSTRIALĂ

Nr. _____ din _____

Oficiul Registrului Național al Informațiilor Secrete de Stat autorizează _____ (denumirea completă a instituției/agentului economic) pentru participarea la proceduri de negociere a unui contract, în cadrul căruia sunt gestionate informații clasificate.

Prezenta autorizație este valabilă până la data de _____.

Directorul general al Oficiului Registrului Național al Informațiilor Secrete de Stat
_____ (semnătura, stampila)

ANEXA Nr. 29

ROMÂNIA

OFICIUL REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

CERTIFICAT D E SECURITATE INDUSTRIALĂ

Nr. _____ din _____

Oficiul Registrului Național al Informațiilor Secrete de Stat certifică _____ (denumirea completă a instituției/agentului economic) pentru derularea contractului în care sunt gestionate informații secrete de stat de nivelul _____.

Prezentul certificat este valabil pe durata derulării contractului.

Directorul general al Oficiului Registrului Național al Informațiilor Secrete de Stat
_____ (semnătura, stampila.)

ANEXA Nr. 30

ANTETUL INSTITUȚIEI/AGENTULUI ECONOMIC

Adresa _____ Tel./Fax:

Către ORNISS

CERERE

pentru eliberarea certificatului de securitate industrială

Vă rugăm să eliberați certificatul de securitate industrială nivel _____ pentru _____ (denumirea completă a instituției/agentul economic;) cu sediul în _____ (adresa completă) în vederea derulării contractului clasificat _____.

Obiectul contractului este _____.

Beneficiarul este _____.

Menționăm că în prezent întreprinderea noastră deține/nu deține autorizație de securitate/certificat de securitate industrială pentru nivelul _____.

Anexăm, în original, chestionarul de securitate industrială.

Directorul instituției/agentului economic
_____ (semnătura, ștampila.)

ANEXA Nr. 31

ROMÂNIA

(Instituția) _____

Compartimentul _____

REGISTRUL pentru evidența autorizațiilor de securitate industrială

Nr. crt .	Denumirea și adresa completă a obiectivului industrial	Data eliberării autorizației de securitate industrială	Seria și numărul autorizației de securitate industrială	Perioada de valabilitate	Data retragerii	Motivul retragerii	Obs.

ANEXA Nr. 32

ROMÂNIA

(Instituția) _____

Compartimentul _____

REGISTRUL pentru evidența certificatelor de securitate industrială

Nr. crt .	Denumirea și adresa completă a obiectivului industrial	Nivelul de acces	Data eliberării certificatei de securitate industrială	Seria și numărul certificatei de securitate industrială	Perioada de valabilitate	Data retragerii	Motivul retragerii	Obs.

Publicat în Monitorul Oficial cu numărul 485 din data de 5 iulie 2002