HOTĂRÂRE nr. 585 din 13 iunie 2002

pentru aprobarea Standardelor naţionale de protectie a informatiilor clasificate în România

CAPITOLUL I
Dispoziţii generale

ART. 1

Standardele naţionale de protecţie a informaţiilor clasificate în România cuprind normele de aplicare a Legii nr. 182/2002
privind protecţia informaţiilor clasificate referitoare la:

a) clasificările informaţiilor secrete de stat şi normele privind măsurile minime de protecţie în cadrul fiecărei clase;

b) obligaţiile şi răspunderile autorităţilor şi instituţiilor publice, ale agenţilor economici şi ale altor persoane juridice de drept public sau privat privind protecţia informaţiilor secrete de stat;

c) normele privind accesul la informaţiile clasificate, precum şi procedura verificărilor de securitate;

d) regulile generale privind evidenţa, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea informaţiilor secrete de stat;

e) regulile de identificare şi marcare, inscripţionările şi menţiunile obligatorii pe documentele secrete de stat, în funcţie de nivelurile de secretizare, cerinţele de evidenţă a numerelor de exemplare şi a destinatarilor, termenele şi regimul de păstrare, interdicţiile de reproducere şi circulaţie;

f) condiţiile de fotografiere, filmare, cartografiere şi executare a unor lucrări de arte plastice în obiective sau locuri care prezintă importanţă deosebită pentru protecţia informaţiilor secrete de stat;

g) regulile privitoare la accesul străinilor la informaţiile secrete de stat;

h) protecţia informaţiilor clasificate care fac obiectul contractelor industriale secrete - securitatea industrială;

i) protecţia surselor generatoare de informaţii - INFOSEC.

ART. 2

(1) Prezentele standarde instituie sistemul naţional de protecţie a informaţiilor clasificate, în concordanţă cu interesul naţional, cu criteriile şi recomandările NATO şi sunt obligatorii pentru toate persoanele juridice sau fizice care gestionează astfel de informaţii.

(2) Echivalenţa informaţiilor naţionale clasificate, pe niveluri de secretizare, cu informaţiile NATO clasificate este:

a) Strict secret de importanţă deosebită - NATO top secret

b) Strict secret - NATO secret

c) Secret - NATO confidential

d) Secret de serviciu - NATO restricted

ART. 3

Termenii folosiţi în prezentele standarde au următorul înţeles:

- Autoritate Desemnată de Securitate - ADS - instituţie abilitată prin lege să stabilească, pentru domeniul său de activitate şi responsabilitate, structuri şi măsuri proprii privind coordonarea şi controlul activităţilor referitoare la protecţia informaţiilor secrete de stat. Sunt autorităţi desemnate de securitate, potrivit legii: Ministerul Apărării Naţionale, Ministerul de Interne, Ministerul Justiţiei, Serviciul Român de Informaţii, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Pază, Serviciul de Telecomunicaţii Speciale;

– autorizaţie de acces la informaţii clasificate - document eliberat cu avizul instituţiilor abilitate, de conducătorul persoanei juridice deţinătoare de astfel de informaţii, prin care se confirmă ca, în exercitarea atribuţiilor profesionale, posesorul acestuia poate avea acces la informaţii secrete de stat de un anumit nivel de secretizare, potrivit principiului necesităţii de a cunoaşte;

– autorizaţie de securitate industrială - document eliberat de Oficiul Registrului Naţional al Informaţiilor Secrete de Stat - ORNISS - unui obiectiv industrial, prin care se atestă ca este abilitat să participe la procedura de negociere a unui contract clasificat;

– autorizaţie specială - document eliberat de către ORNISS prin care se atestă verificarea şi acreditarea unei persoane de a desfăşura activităţi de fotografiere, filmare, cartografiere şi lucrări de arte plastice pe teritoriul României, în obiective, zone sau locuri care prezintă importanţă deosebită pentru protectia informaţiilor 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 protecţiei informaţiilor clasificate vehiculate în derularea contractului încheiat;

– certificat de securitate - document eliberat persoanei cu atribuţii nemijlocite în domeniul protecţiei informaţiilor clasificate, respectiv funcţionarului de securitate sau salariatului din structura de securitate, care atestă verificarea şi acreditarea de a deţine, de a avea acces şi de a lucra cu informaţii 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 activităţi industriale şi/sau de cercetare ce presupun accesul la informaţii clasificate;

– clasificarea informaţiilor - încadrarea informaţiilor într-o clasă şi nivel de secretizare;

– contract clasificat - orice contract încheiat între părţi, în condiţiile legii, în cadrul căruia se cuprind şi se vehiculeaza informaţii clasificate;

– contractant - unitate industrială, comercială, de execuţie, 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 informaţiilor clasificate - orice activitate de verificare a modului în care sunt gestionate documentele clasificate;

– declasificare - suprimarea menţiunilor de clasificare şi scoaterea informaţiei clasificate de sub incidenţa reglementărilor protective prevăzute de lege;

– diseminarea informaţiilor clasificate - activitatea de difuzare a informaţiilor clasificate către unităţi sau persoane abilitate să aibă acces la astfel de informaţii;

– document clasificat - orice suport material care conţine informaţii clasificate, în original sau copie, precum:

a) hârtie - documente olografe, dactilografiate sau tipărite, schite, hărţi, planşe, fotografii, desene, indigo, listing;

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

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

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

- funcţionar de securitate - persoana care îndeplineşte atribuţiile de protecţie a informaţiilor clasificate în cadrul autorităţilor, instituţiilor publice, agenţilor economici cu capital integral sau parţial de stat şi altor persoane juridice de drept public sau privat;

– gestionarea informaţiilor clasificate - orice activitate de elaborare, luare în evidenţă, accesare, procesare, multiplicare, manipulare, transport, transmitere, inventariere, păstrare, arhivare sau distrugere a informaţiilor clasificate;

– incident de securitate - orice acţiune sau inacţiune contrară reglementărilor de securitate a cărei consecinţă a determinat sau este de natură să determine compromiterea informaţiilor clasificate;

– indicator de interdicţie text sau simbol care semnalează interzicerea accesului sau derulării unor activităţi în zone, obiective, sectoare sau locuri care prezintă importanţă deosebită pentru protecţia informaţiilor clasificate;

– informaţie clasificată compromisă - informaţie clasificată care şi-a pierdut integritatea, a fost rătăcită, pierdută ori accesată, total sau parţial, de persoane neautorizate;

– instituţie cu atribuţii de coordonare a activităţii şi de control al măsurilor privitoare la protecţia informaţiilor clasificate sau instituţie abilitată - Ministerul Apărării Naţionale, Ministerul de Interne, Ministerul Justiţiei, Serviciul Român de Informaţii, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Pază, Serviciul de Telecomunicaţii Speciale, potrivit competenţelor stabilite prin lege;

– marcare - activitatea de inscripţionare a nivelului de secretizare a informaţiei şi de semnalare a cerinţelor speciale de protecţie a acesteia;

– material clasificat - document sau produs prelucrat ori în curs de prelucrare, care necesită a fi protejat împotriva cunoaşterii neautorizate;

– necesitatea de a cunoaşte - principiul conform căruia accesul la informaţii clasificate se acordă în mod individual numai persoanelor care, pentru îndeplinirea îndatoririlor de serviciu, trebuie să lucreze cu astfel de informaţii sau să aibă acces la acestea;

– negocieri - activităţile circumscrise adjudecării unui contract sau subcontract, de la notificarea intenţiei de organizare a licitaţiei, până la încheierea acesteia;

– obiectiv industrial - unitate de cercetare sau cu activitate de producţie, care desfăşoară activităţi ştiinţifice, tehnologice sau economice ce au legătură cu siguranţa sau cu apărarea naţională, ori prezintă importanţă deosebită pentru interesele economice şi tehnico-ştiinţifice ale României;

– obiectiv, sector sau loc de importanţă deosebită pentru protecţia informaţiilor secrete de stat - incintaă sau perimetru anume desemnat, în care sunt gestionate informaţii secrete de stat;

– parte contractantă - oricare dintre părţile care convin să negocieze, să încheie sau să deruleze un contract clasificat;

– protecţia surselor generatoare de informaţii - ansamblul măsurilor destinate protecţiei informaţiilor elaborate, stocate sau transmise prin sisteme ori reţele de prelucrare automată a datelor şi/sau de comunicaţii;

– securitate industrială - sistemul de norme şi măsuri care reglementează protecţia informaţiilor clasificate în domeniul activităţilor contractuale;

– sistem de protecţie a informaţiilor clasificate - ansamblul de măsuri de natură juridică, procedurală, fizică, de protecţie a personalului şi a surselor generatoare de informaţii, destinate securităţii materialelor şi documentelor clasificate;

– structura de securitate - compartiment specializat în protecţia informaţiilor clasificate, organizat în cadrul autorităţilor, instituţiilor publice, agenţilor economici cu capital integral sau parţial de stat şi al altor persoane juridice de drept public sau privat;

– subcontractant - parte care îşi asumă executarea unei părţi a contractului clasificat sub coordonarea contractantului;

– trecerea la un alt nivel de clasificare sau de secretizare - schimbarea clasificării, respectiv a nivelului de secretizare a informaţiilor secrete de stat;

– unitate deţinatoare de informaţii clasificate sau unitate - autoritate sau instituţie publică, agent economic cu capital integral sau parţial de stat ori o altă persoană juridica de drept public sau privat care, potrivit legii, are dreptul de a deţine informaţii clasificate;

– verificare de securitate - totalitatea măsurilor intreprinse de autorităţile desemnate de securitate, conform competenţelor, pentru stabilirea onestităţii şi profesionalismului persoanelor, în scopul avizării eliberării certificatului de securitate sau autorizaţiei de acces la informaţii clasificate;

– zona de securitate - perimetru delimitat şi special amenajat unde sunt gestionate informaţii clasificate.

CAPITOLUL II
Clasificarea şi declasificarea informaţiilor. Măsuri minime de protecţie specifice claselor şi nivelurilor de secretizare

SECŢIUNEA 1
Clasificarea informaţiilor

ART. 4

(1) Potrivit legii, informaţiile sunt clasificate secrete de stat sau secrete de serviciu, în raport de importanţa pe care o au pentru securitatea naţională şi de consecinţele ce s-ar produce ca urmare a dezvăluirii sau diseminării lor neautorizate.

(2) Informaţiile secrete de stat sunt informaţiile a căror divulgare poate prejudicia siguranţa naţională şi apărarea ţării şi care, în funcţie de importanţa valorilor protejate, se includ în urmatoarele niveluri de secretizare prevăzute de lege:

a) strict secret de importanţă deosebită;

b) strict secret;

c) secret.

(3) Informaţiile 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) Autorităţile publice care elaborează ori lucrează cu informaţii secrete de stat au obligaţia să întocmeasca un ghid pe baza căruia se va realiza clasificarea corectă şi uniformă a acestora.

(2) Ghidul prevăzut la alin. (1) se aprobă personal şi în scris de către imputerniciţii sau, după caz, funcţionarii superiori abilitaţi să atribuie nivelurile de secretizare, conform legii.

ART. 6

Autorităţile şi instituţiile publice întocmesc liste proprii cuprinzând categoriile de informaţii secrete de stat în domeniile lor de activitate, care se aprobă şi se actualizează prin hotărâre a Guvernului.

ART. 7

Listele cu informaţii secrete de serviciu se stabilesc de conducătorii unităţilor deţinatoare de astfel de informaţii.

ART. 8

În listele cu informaţii secrete de serviciu vor fi incluse informaţiile care se referă la activitatea unităţii şi care, fără a constitui, în înţelesul legii, secrete de stat, nu trebuie cunoscute decat de persoanele cărora le sunt necesare pentru îndeplinirea atribuţiilor de serviciu, divulgarea lor putând prejudicia interesul unităţii.

ART. 9

Unităţile care gestionează informaţii clasificate au obligaţia să analizeze ori de câte ori este necesar listele informaţiilor secrete de stat şi, după caz, să prezinte Guvernului spre aprobare propuneri de actualizare şi completare a acestora, conform legii.

ART. 10

Atribuirea clasei şi nivelului de secretizare a informaţiilor se realizează prin consultarea ghidului de clasificare, a listelor cu informaţii secrete de stat şi a listelor cu informaţii secrete de serviciu, elaborate potrivit legii.

ART. 11

Şeful ierarhic al emitentului are obligaţia să verifice dacă informaţiile au fost clasificate corect şi să ia măsuri în consecinţă, când constată ca au fost atribuite niveluri de secretizare necorespunzătoare.

ART. 12

(1) Termenele de clasificare a informaţiilor secrete de stat vor fi stabilite de emitent, în funcţie de importanţa acestora şi de consecinţele care s-ar produce ca urmare a dezvăluirii sau diseminării lor neautorizate.

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

- 100 de ani pentru informaţiile clasificate strict secret de importanţă deosebită;

– 50 de ani pentru informaţiile clasificate strict secret;

– 30 de ani pentru informaţiile clasificate secret.

(3) Termenele prevăzute la alin. (2) pot fi prelungite prin hotărâre a Guvernului, pe baza unei motivaţii temeinice, la solicitarea conducătorilor unităţilor deţinătoare de informaţii clasificate sau, după caz, a împuterniciţilor şi funcţionarilor superiori abilitaţi să atribuie nivelurile de secretizare.

ART. 13

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

ART. 14

(1) Documentul elaborat pe baza prelucrarii informaţiilor cu niveluri de secretizare diferite va fi clasificat conform noului conţinut, care poate fi superior originalelor.

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

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

ART. 15

Marcarea informaţiilor clasificate are drept scop atenţionarea persoanelor care le gestionează sau le accesează că sunt în posesia unor informaţii în legătură cu care trebuie aplicate măsuri specifice de acces şi protecţie, în conformitate cu legea.

ART. 16

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

ART. 17

(1) Informaţiile vor fi clasificate numai în cazul în care se impune protecţia acestora, iar nivelurile de secretizare şi termenele de clasificare subzista atât timp cât dezvăluirea sau diseminarea lor neautorizată ar putea prejudicia siguranţa naţională, apărarea ţării, ordinea publică sau interesele persoanelor juridice de drept public sau privat.

(2) Supraevaluarea sau subevaluarea nivelului de secretizare a informaţiilor şi a duratei pentru care au fost clasificate se pot contesta de către orice persoană fizica sau juridica română, în contencios administrativ.

ART. 18

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

(2) Până la stabilirea noilor niveluri de secretizare, informaţiile secrete de stat şi secrete de serviciu menţionate la alin. (1) îşi păstrează nivelul şi termenul de secretizare şi vor fi protejate potrivit prezentelor standarde.

SECŢIUNEA a 2-a
Declasificarea şi trecerea informaţiilor clasificate la un nivel inferior de secretizare

ART. 19

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

ART. 20

(1) Informaţiile se declasifică dacă:

a) termenul de clasificare a expirat;

b) dezvaluirea informaţiilor nu mai poate prejudicia siguranţa naţională, apărarea ţării, ordinea publică, ori interesele persoanelor de drept public sau privat deţinătoare;

c) a fost atribuit de o persoană neîmputernicită prin lege.

(2) Declasificarea sau trecerea la un alt nivel de secretizare a informaţiilor secrete de stat se realizează de împuterniciţii şi funcţionarii superiori abilitaţi prin lege să atribuie niveluri de secretizare, cu avizul prealabil al instituţiilor care coordonează activitatea şi controlul măsurilor privitoare la protecţia informaţiilor clasificate, potrivit competenţelor materiale.

(3) Emitenţii documentelor secrete de stat vor evalua periodic necesitatea menţinerii în nivelurile de secretizare acordate anterior şi vor prezenta împuterniciţilor şi funcţionarilor superiori abilitaţi prin lege să atribuie niveluri de secretizare, propuneri în consecinţă.

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 iniţial unei informaţii, emitentul este obligat să încunoştinţeze structura/funcţionarul de securitate, care va face menţiunile necesare în registrele de evidenţă.

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

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

ART. 23

(1) Informaţiile 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 informaţiilor respective ori a suportului material al acestora, cu acordul scris al emitentului.

ART. 24

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

SECŢIUNEA a 3-a
Măsuri minime de protecţie a informaţiilor clasificate

ART. 25

Măsurile de protecţie a informaţiilor clasificate vor fi stabilite în raport cu:

a) clasele şi nivelurile de secretizare a informaţiilor;

b) volumul şi suportul informaţiilor;

c) calitatea, funcţia şi numărul persoanelor care au sau pot avea acces la informaţii, potrivit certificatului de securitate şi autorizaţiei de acces şi cu respectarea principiului necesităţii de a cunoaşte;

d) ameninţările, riscurile şi vulnerabilitatile ce pot avea consecinţe asupra informaţiilor clasificate.

ART. 26

Transmiterea informaţiilor clasificate către alţi utilizatori se va efectua numai dacă aceştia deţin certificate de securitate sau autorizaţii de acces corespunzător nivelului de secretizare.

ART. 27

Certificatele de securitate aparţinând persoanelor al căror comportament, atitudini sau manifestări pot crea premise de insecuritate pentru informaţiile secrete de stat vor fi imediat retrase, cu încunoştinţarea instituţiilor investite cu atribuţii de coordonare a activităţii şi de control al măsurilor privitoare la protecţia informaţiilor clasificate, potrivit competenţelor.

ART. 28

Conducătorii unităţilor şi persoanele care gestionează informaţii clasificate au obligaţia de a aduce la cunoştinţa instituţiilor cu atribuţii de coordonare şi control în domeniu orice indicii din care pot rezulta premise de insecuritate pentru astfel de informaţii.

SECŢIUNEA a 4-a
Structura/funcţionarul de securitate

ART. 29

(1) Pentru implementarea măsurilor de protecţie a informaţiilor clasificate, în unităţile deţinătoare de astfel de informaţii se înfiinţează, în condiţiile legii, structuri de securitate cu atribuţii specifice.

(2) În situaţia în care unitatea deţine un volum redus de informaţii clasificate, atribuţiile structurii de securitate vor fi îndeplinite de funcţionarul de securitate.

(3) Structura de securitate se organizează şi se încadrează potrivit legii.

(4) Seful structurii de securitate, respectiv funcţionarul de securitate, este un adjunct al conducătorului persoanei juridice sau un membru al consiliului de administraţie al unităţii.

ART. 30

Şeful structurii de securitate, respectiv funcţionarul de securitate, deţine certificat de securitate corespunzător celui mai înalt nivel de clasificare a informaţiilor secrete de stat gestionate de unitate.

ART. 31

(1) Structura/funcţionarul de securitate are următoarele atribuţii generale:

a) elaborează şi supune aprobării conducerii unităţii normele interne privind protecţia informaţiilor clasificate, potrivit legii;

b) întocmeşte programul de prevenire a scurgerii de informaţii clasificate şi îl supune avizării instituţiilor abilitate, iar după aprobare, acţionează pentru aplicarea acestuia;

c) coordonează activitatea de protecţie a informaţiilor clasificate, în toate componentele acesteia;

d) asigură relaţionarea cu instituţia abilitată să coordoneze activitatea şi să controleze măsurile privitoare la protecţia informaţiilor clasificate, potrivit legii;

e) monitorizează activitatea de aplicare a normelor de protecţie a informaţiilor clasificate şi modul de respectare a acestora;

f) consiliază conducerea unităţii în legătură cu toate aspectele privind securitatea informaţiilor clasificate;

g) informează conducerea unităţii despre vulnerabilitatile şi riscurile existente în sistemul de protecţie a informaţiilor clasificate şi propune măsuri pentru înlăturarea acestora;

h) acordă sprijin reprezentanţilor autorizaţi ai instituţiilor abilitate, potrivit competenţelor legale, pe linia verificării persoanelor pentru care se solicită accesul la informaţii clasificate;

i) organizează activităţi de pregătire specifică a persoanelor care au acces la informaţii clasificate;

j) asigură păstrarea şi organizează evidenţa certificatelor de securitate şi autorizaţiilor de acces la informaţii clasificate;

k) actualizează permanent evidenţa certificatelor de securitate şi a autorizaţiilor de acces;

l) întocmeşte şi actualizează listele informaţiilor clasificate elaborate sau păstrate de unitate, pe clase şi niveluri de secretizare;

m) prezintă conducătorului unităţii propuneri privind stabilirea obiectivelor, sectoarelor şi locurilor de importanţă deosebită pentru protecţia informaţiilor clasificate din sfera de responsabilitate şi, după caz, solicită sprijinul instituţiilor abilitate;

n) efectuează, cu aprobarea conducerii unităţii, controale privind modul de aplicare a măsurilor legale de protecţie a informaţiilor clasificate;

o) exercita alte atribuţii în domeniul protectiei informaţiilor clasificate, potrivit legii.

(2) Atribuţiile personalului din structura de securitate, respectiv ale funcţionarului de securitate, se stabilesc prin fişa postului, aprobată de conducătorul unităţii.

ART. 32

Persoanele care lucrează în structura de securitate sau, după caz, funcţionarul de securitate vor fi incluse în programe permanente de pregătire organizate de instituţiile investite cu atribuţii de coordonare a activităţii şi de control al măsurilor privitoare la protecţia informaţiilor clasificate, potrivit legii.

SECŢIUNEA a 5-a
Accesul la informaţiile clasificate

ART. 33

Accesul la informaţii clasificate este permis cu respectarea principiului necesităţii de a cunoaşte numai persoanelor care deţin certificat de securitate sau autorizaţie de acces, valabile pentru nivelul de secretizare al informaţiilor necesare îndeplinirii atribuţiilor de serviciu.

ART. 34

Persoanele care au acces la informaţii strict secrete de importanţă deosebită, în condiţiile prevăzute de prezentele standarde, vor fi înregistrate în fişa de consultare, prevăzută la anexa nr. 1, care va fi păstrată la deţinătorul de drept al documentului.

ART. 35

(1) Persoanele cărora le-au fost eliberate certificate de securitate sau autorizaţii de acces vor fi instruite, atât la acordarea acestora, cât şi periodic, cu privire la conţinutul reglementărilor privind protecţia informaţiilor clasificate.

(2) Activităţile de instruire vor fi consemnate de structura/funcţionarul de securitate, sub semnatură, în fişa de pregătire individuală, prezentată la anexa nr. 2.

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

ART. 36

(1) În cazuri excepţionale, determinate de situaţii de criză, calamităţi sau evenimente imprevizibile, conducătorul unităţii poate acorda acces temporar la informaţii clasificate anumitor persoane care nu deţin certificat de securitate sau autorizaţie de acces, cu condiţia asigurării unui sistem corespunzător de evidenţă.

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

ART. 37

În cazul informaţiilor strict secrete de importanţă deosebită, accesul temporar va fi acordat, pe cât posibil, persoanelor care deţin deja certificate de securitate pentru acces la informaţii strict secrete sau secrete.

ART. 38

(1) Transmiterea informaţiilor clasificate între unităţi se va efectua cu aprobarea emitentului şi cu respectarea principiului necesităţii de a cunoaşte.

(2) Predarea-primirea informaţiilor clasificate între unitatea deţinătoare şi unitatea primitoare se face cu respectarea măsurilor de protecţie prevăzute în prezentele standarde.

ART. 39

Structura/funcţionarul de securitate al unităţii deţinătoare se va asigura că reprezentantul unităţii primitoare deţine certificatul de securitate sau autorizaţia de acces corespunzătoare nivelului de secretizare a informaţiilor clasificate ce fac obiectul predării-primirii.

CAPITOLUL III
Reguli generale privind evidenţa, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea informaţiilor clasificate

ART. 40

(1) În unităţile deţinătoare de informaţii clasificate se organizează compartimente speciale pentru evidenţa, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea acestora în condiţii de siguranţă.

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

ART. 41

La redactarea documentelor ce conţin informaţii clasificate se vor respecta următoarele reguli:

a) menţionarea, în antet, a unităţii emitente, a numărului şi datei înregistrării, a clasei sau nivelului de secretizare, a numărului de exemplare şi, după caz, a destinatarului;

b) numerele de înregistrare se înscriu pe toate exemplarele documentului şi 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 importanţă deosebită şi de litera "S" pentru secrete de serviciu;

c) la sfârşitul documentului se înscriu în clar, după caz, rangul, funcţia, numele şi prenumele conducătorului unităţii emitente, precum şi ale celui care îl întocmeşte, urmate de semnăturile acestora şi ştampila unităţii;

d) înscrierea, pe fiecare pagină a documentului, a clasei sau nivelului de secretizare atribuit acestuia;

e) pe fiecare pagină a documentelor ce conţin informaţii clasificate se înscriu numărul curent al paginii, urmat de numărul total al acestora.

ART. 42

(1) În situaţia în care documentul de bază este însoţit de anexe, la sfârşitul textului se indică, pentru fiecare anexă, numărul de înregistrare, numărul de file al acesteia şi clasa sau nivelul de secretizare.

(2) Anexele se clasifică în funcţie de conţinutul lor şi nu de cel al documentelor pe care le însoţesc.

(3) Adresa de însoţire a documentului nu va cuprinde informaţii detaliate referitoare la conţinutul documentelor anexate.

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

(5) Aplicarea, pe documentele anexate, a ştampilei unităţii emitente este obligatorie.

ART. 43

(1) Când documentele ce conţin informaţii clasificate se semnează de o singură persoană, datele privind rangul, funcţia, numele şi prenumele acesteia se înscriu sub text, în centrul paginii.

(2) Când semneaza două sau mai multe persoane, rangul, funcţia, numele şi prenumele conducătorului unităţii se înscriu în partea stângă, iar ale celorlalţi semnatari în partea dreaptă, în ordinea rangurilor şi funcţiilor.

ART. 44

Când documentele care conţin informaţii clasificate se emit în comun de două sau mai multe unităţi, denumirile acestora se înscriu separat în antet, iar la sfârşit se semnează de către conducătorii unităţilor respective, de la stanga la dreapta, aplicându-se ştampilele corespunzătoare.

ART. 45

Informaţiile clasificate vor fi marcate, inscriptionate şi gestionate numai de către persoane care au autorizaţie sau certificat de securitate corespunzător nivelului de clasificare a acestora.

ART. 46

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

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

a) în partea dreaptă sus şi jos, pe exteriorul copertelor, pe pagina cu titlul şi pe prima pagină a documentului;

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

c) sub legendă, titlu sau scara de reprezentare şi în exterior - pe verso - atunci când acestea sunt pliate, pe toate schemele, diagramele, hărţile, desenele şi alte asemenea documente.

ART. 47

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

ART. 48

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

ART. 49

(1) Toate documentele clasificate aflate în lucru sau în stadiu de proiect vor avea inscrise menţiunile "Document în lucru" sau "Proiect" şi vor fi marcate potrivit clasei sau nivelului de secretizare a informaţiilor ce le conţin.

(2) Gestionarea documentelor clasificate aflate în lucru sau în stadiu de proiect se face în aceleaşi condiţii ca şi a celor în forma definitivă.

ART. 50

Documentele sau materialele care conţin informaţii clasificate şi sunt destinate unei persoane strict determinate vor fi inscripţionate, sub destinatar, cu menţiunea "Personal".

ART. 51

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

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

ART. 52

(1) Clasa sau nivelul de secretizare a informaţiilor înregistrate pe benzi audio se imprimă verbal, atât la începutul înregistrării, cât şi la sfârşitul acesteia.

(2) Marcarea clasei sau a nivelului de secretizare pe benzi video trebuie să asigure afişarea 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 şi la sfârşitul benzii video.

(3) Benzile audio şi video care conţin informaţii 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 adaugarea unei înregistrări cu nivel superior de secretizare.

ART. 53

Proiecţiile de imagini trebuie să afişeze, la începutul şi sfârşitul acestora, numărul şi data înregistrării, precum şi 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 informaţii 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 şi la sfârşitul fiecărui pasaj, se va menţiona clasa sau nivelul de secretizare.

(3) În cazul detaşării 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 suporţii în care se păstrează documente sau materiale ce conţin informaţii clasificate vor avea inscripţionat clasa sau nivelul de secretizare, numărul şi data înregistrării în evidenţe şi 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 şi data iniţială 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 unităţilor vor asigura măsurile necesare de evidenţă şi control al informaţiilor clasificate, astfel încât să se poată stabili, în orice moment, locul în care se află aceste informaţii.

ART. 59

(1) Evidenţa materialelor şi documentelor care conţin informaţii clasificate se ţine în registre speciale, întocmite potrivit modelelor prevăzute în anexele nr. 4, 5 şi 6.

(2) Fiecare document sau material va fi inscripţionat cu numărul de înregistrare şi data când este înscris în registrele de evidenţă.

(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 şi borderourile se înregistrează în registrul unic de evidenţă a registrelor, condicilor, borderourilor şi a caietelor pentru însemnări clasificate, conform modelului din anexa nr. 7.

(5) Fac excepţie actele de gestiune, imprimatele inseriate şi alte documente sau materiale cuprinse în forme de evidenţă specifice.

ART. 60

(1) Documentele sau materialele care conţin informaţii clasificate înregistrate în registrele prevăzute în art. 59 nu vor fi înregistrate în alte forme de evidenţă.

(2) Emitentii şi deţinătorii de informaţii clasificate sunt obligaţi să înregistreze şi să ţină evidenţa tuturor documentelor şi materialelor primite, expediate sau a celor întocmite de unitatea proprie, potrivit legii.

(3) În registrele pentru evidenţa informaţiilor clasificate vor fi menţionate numele şi 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 evidenţă se face consecutiv, pe parcursul unui an calendaristic.

(2) Numerele de înregistrare se înscriu obligatoriu pe toate exemplarele documentelor sau materialelor care conţin informaţii clasificate, precum şi pe documentele anexate.

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

(4) Clasarea documentelor sau materialelor care conţin informaţii clasificate se face separat, în funcţie de suportul şi formatul acestora, cu folosirea mijloacelor de păstrare şi protejare adecvate.

ART. 62

(1) Informaţiile strict secrete de importanţă deosebită vor fi compartimentate fizic şi înregistrate separat de celelalte informaţii.

(2) Evidenţa documentelor strict secrete şi secrete poate fi operată în acelaşi registru.

ART. 63

Hărţile, planurile topografice, asamblajele de hărţi şi alte asemenea documente se înregistrează în registrele pentru evidenţa informaţiilor clasificate prevăzute în anexele nr. 4, 5 şi 6.

ART. 64

Atribuirea aceluiaşi număr de înregistrare unor documente cu conţinut diferit este interzisă.

ART. 65

Registrele de evidenţă vor fi completate de persoana desemnată care deţine autorizaţie sau certificat de securitate corespunzător.

ART. 66

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

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

ART. 67

(1) Documentelor care conţin informaţii clasificate rezultate în procesul de multiplicare li se atribuie numere din registrul de evidenţă a informaţiilor clasificate multiplicate, conform modelului din anexa nr. 9.

(2) Numerele se atribuie consecutiv, începând cu cifra 1, pe parcursul unui an calendaristic şi se înscriu obligatoriu pe toate exemplarele documentului.

ART. 68

(1) Evidenţierea operaţiunii de multiplicare se face prin marcare atât pe original, cât şi 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 operaţiune, 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 operaţiunea se efectuează de mai multe ori şi la date diferite.

ART. 69

(1) Multiplicarea documentelor clasificate se face în baza aprobării conducătorului unităţii deţinătoare, cu avizul structurii/funcţionarului de securitate, ambele înscrise pe cererea pentru copiere sau pe adresa de însoţire în care se menţionează necesitatea multiplicării.

(2) Parchetele, instanţele şi comisiile de cercetare pot multiplica documente care conţin informaţii clasificate numai în condiţiile prezentelor standarde.

(3) Extrasul dintr-un document care conţine informaţii clasificate se face în baza cererii pentru copiere, cu aprobarea conducătorului unităţii, iar documentul rezultat va avea menţionat sub numărul de exemplar cuvantul "Extras" şi numărul de înregistrare al documentului original.

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

ART. 70

(1) Dacă emitentul doreşte să aibă control exclusiv asupra reproducerii, documentul va conţine o indicaţie vizibilă cu următorul conţinut: "Reproducerea acestui document, totală sau parţială, este interzisa".

(2) Informaţiile clasificate înscrise pe documente cu regim restrictiv de reproducere care au menţiunea "Reproducerea interzisă" nu se multiplică.

ART. 71

În cazul copierii unui document care conţine informaţii clasificate se procedează astfel:

a) se stabileşte numărul de exemplare în care va fi multiplicat;

b) se completează şi se aprobă cererea pentru multiplicare, potrivit art. 69 alin. (1), după care aceasta se înregistrează în registrul de evidenţă - anexa nr. 4 sau anexa nr. 5, după caz;

c) documentul original se predă operatorului pe bază de semnatură;

d) după verificarea exemplarelor rezultate, beneficiarul semnează în registrul de evidenţă a informaţiilor clasificate multiplicate, conform modelului din anexa nr. 9;

e) repartiţia în vederea difuzării exemplarelor copiate se consemnează de către structura/funcţionarul de securitate pe spatele cererii pentru copiere;

f) cererea pentru copiere împreună cu exemplarele copiate se predau pe bază de semnatură structurii/funcţionarului de securitate în vederea difuzării sau expedierii.

ART. 72

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

(2) Atunci când numărul destinatarilor este mare se întocmeşte 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 şi 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 suporţi magnetici în următoarele condiţii:

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

b) microfilmelor, discurilor optice sau suporţilor magnetici de stocare să li se asigure aceeaşi protecţie ca a documentului original;

c) toate microfilmele, discurile optice sau suporţii magnetici de stocare să fie înregistrate intr-o evidenţă specifică şi supuse, ca şi documentele originale, verificării anuale.

ART. 74

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

(2) Informaţiile clasificate pot fi redifuzate de către destinatarul iniţial la alţi destinatari, cu respectarea normelor din prezentele standarde.

(3) Emitentul este obligat să indice clar toate restricţiile care trebuie respectate pentru difuzarea unei informaţii clasificate. Când se impun astfel de restricţii, 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 fişa de consultare, conform modelului din anexa nr. 1.

ART. 76

(1) Informaţiile clasificate iesite din termenul de clasificare se arhivează sau se distrug.

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

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

(4) Distrugerea documentelor clasificate sau a ciornelor care conţin informaţii 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 conţin informaţii clasificate, de regulă, se distrug.

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

ART. 78

(1) Informaţiile strict secrete de importanţă deosebită destinate distrugerii vor fi înapoiate unităţii emitente cu adresa de restituire.

(2) Fiecare asemenea informaţie va fi trecută pe un proces-verbal de distrugere, care va fi aprobat de conducerea unităţii şi semnat de şeful structurii/funcţionarul de securitate şi de persoana care asistă la distrugere, autorizată să aibă acces la informaţii strict secrete de importanţă deosebită.

(3) În situaţii de urgenţă, protecţia, inclusiv prin distrugere, a materialelor şi documentelor strict secrete de importanţă deosebită va avea întotdeauna prioritate faţă de alte documente sau materiale.

(4) Procesele-verbale de distrugere şi documentele de evidenţă ale acestora vor fi arhivate şi păstrate cel puţin 10 ani.

ART. 79

(1) Distrugerea informaţiilor strict secrete, secrete şi secrete de serviciu va fi evidenţiată într-un proces-verbal semnat de două persoane asistente autorizate să aibă acces la informaţii de acest nivel, avizat de structura/funcţionarul de securitate şi aprobat de conducătorul unităţii.

(2) Procesele-verbale de distrugere şi documentele de evidenţă a informaţiilor strict secrete, secrete şi secrete de serviciu vor fi păstrate de compartimentul care a executat distrugerea, o perioadă de cel puţin trei ani, după care vor fi arhivate şi păstrate cel puţin 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 întocmeşte în situaţia în care acestea au fost înregistrate într-o formă de evidenţă.

ART. 81

(1) Documentele şi materialele ce conţin informaţii clasificate se transportă, pe teritoriul României, prin intermediul unităţii specializate a Serviciului Român de Informaţii, potrivit normelor stabilite prin hotărâre a Guvernului.

(2) Documentele şi materialele care conţin informaţii clasificate se transportă în străinătate prin valiza diplomatică, de către curierii diplomatici selecţionaţi şi pregătiţi de Serviciul de Informaţii Externe.

(3) Este interzisă expedierea documentelor şi materialelor ce conţin informaţii clasificate prin S.N. "Poşta Română" ori prin alte societăţi comerciale de transport.

ART. 82

Conducătorii unităţilor deţinătoare de informaţii clasificate vor desemna, din structura de securitate proprie, în condiţiile prezentelor standarde, cel puţin un delegat împuternicit pentru transportul şi executarea operaţiunilor de predare-primire a corespondenţei clasificate, între aceasta şi unitatea specializată a Serviciului Român de Informaţii.

CAPITOLUL IV
Protecţia informaţiilor secrete de stat

SECŢIUNEA 1
Obligaţiile şi răspunderile ce revin autorităţilor şi instituţiilor publice, agenţilor economici şi altor persoane juridice pentru protecţia informaţiilor secrete de stat

ART. 83

Protecţia informaţiilor secrete de stat reprezintă o obligaţie ce revine tuturor persoanelor autorizate care le emit, le gestionează sau care intră în posesia lor.

ART. 84

(1) Conducătorii unităţilor deţinătoare de informaţii secrete de stat sunt răspunzatori de aplicarea măsurilor de protecţie a informaţiilor secrete de stat.

(2) Persoanele juridice de drept privat deţinătoare de informaţii secrete de stat au obligaţia să respecte şi să aplice reglementările în vigoare stabilite pentru autorităţile şi instituţiile publice, în domeniul lor de activitate.

ART. 85

Până la înfiinţarea şi organizarea structurii de securitate sau, după caz, până la numirea funcţionarului de securitate, conducătorii unităţilor deţinătoare de informaţii secrete de stat vor desemna o persoană care să îndeplinească temporar atribuţiile specifice protecţiei informaţiilor clasificate, prin cumul de funcţii.

ART. 86

(1) Conducătorul unităţii care gestionează informaţii secrete de stat este obligat:

a) să asigure organizarea activităţii structurii de securitate, respectiv a funcţionarului de securitate şi compartimentelor speciale pentru gestionarea informaţiilor clasificate, în condiţiile legii;

b) să solicite instituţiilor abilitate efectuarea de verificări pentru avizarea eliberarii certificatului de securitate şi autorizatiei de acces la informaţii clasificate pentru angajatii proprii;

c) să notifice la ORNISS eliberarea certificatului de securitate sau autorizaţiei de acces pentru fiecare angajat care lucrează cu informaţii clasificate;

d) să aprobe listele cu personalul verificat şi avizat pentru lucrul cu informaţiile secrete de stat şi evidenţa deţinătorilor de certificate de securitate şi autorizaţii de acces şi să le comunice la ORNISS şi la instituţiile abilitate să coordoneze activitatea şi controlul măsurilor privitoare la protecţia informaţiilor clasificate, potrivit legii;

e) să întocmească lista informaţiilor secrete de stat şi a termenelor de menţinere în nivelurile de secretizare şi să o supună aprobării Guvernului, potrivit legii;

f) să stabilească obiectivele, sectoarele şi locurile din zona de competenţă care prezintă importanţă deosebită pentru protecţia informaţiilor secrete de stat şi să le comunice Serviciului Român de Informaţii pentru a fi supuse spre aprobare Guvernului;

g) să solicite asistenţa de specialitate instituţiilor abilitate să coordoneze activitatea şi să controleze măsurile privitoare la protecţia informaţiilor secrete de stat;

h) să supună avizării instituţiilor abilitate programul propriu de prevenire a scurgerii de informaţii clasificate şi să asigure aplicarea acestuia;

i) să elaboreze şi să aplice măsurile procedurale de protecţie fizică şi de protecţie a personalului care are acces la informaţii clasificate;

j) să întocmeasca ghidul pe baza căruia se va realiza încadrarea corectă şi uniforma în nivelurile de secretizare a informaţiilor secrete de stat, în strictă conformitate cu legea şi să îl prezinte, spre aprobare, împuterniciţilor şi funcţionarilor superiori abilitaţi prin lege să atribuie nivelurile de secretizare;

k) să asigure aplicarea şi respectarea regulilor generale privind evidenţa, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea informaţiilor secrete de stat şi a interdicţiilor de reproducere şi circulaţie, în conformitate cu actele normative în vigoare;

l) să comunice instituţiilor abilitate, potrivit competenţelor, lista funcţiilor din subordine care necesită acces la informaţii secrete de stat;

m) la încheierea contractelor individuale de muncă, a contractelor de colaborare sau convenţiilor de orice natură să precizeze obligaţiile ce revin părţilor pentru protecţia informaţiilor clasificate în interiorul şi în afara unităţii, în timpul programului şi după terminarea acestuia, precum şi la încetarea activităţii în unitatea respectivă;

n) să asigure includerea personalului structurii/funcţionarului de securitate în sistemul permanent de pregătire şi perfecţionare, conform prezentelor standarde;

o) să aprobe normele interne de aplicare a măsurilor privind protecţia informaţiilor clasificate, în toate componentele acesteia, şi să controleze modul de respectare în cadrul unităţii;

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

q) să analizeze, ori de câte ori este necesar, dar cel puţin semestrial, modul în care structura/funcţionarul de securitate şi personalul autorizat asigură protecţia informaţiilor clasificate;

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

s) să sesizeze instituţiile prevăzute la art. 25 din Legea nr. 182/2002, conform competenţelor, în legătură cu incidentele de securitate şi riscurile la adresa informaţiilor secrete de stat;

t) să dispună efectuarea de cercetări şi, după caz, să sesizeze organele de urmărire penală în situaţia compromiterii informaţiilor clasificate.

(2) De la prevederile alin. (1) lit f) şi h) se exceptează instituţiile prevăzute la art. 25 din Legea nr. 182/2002

SECŢIUNEA a 2-a
Protecţia juridică

ART. 87

Conducătorii unităţilor deţinătoare de secrete de stat vor asigura condiţiile necesare pentru ca toate persoanele care gestionează astfel de informaţii să cunoască reglementările în vigoare referitoare la protecţia informaţiilor clasificate.

ART. 88

(1) Conducătorii unităţilor deţinătoare de informaţii secrete de stat au obligaţia de a înştiinta, în scris, instituţiile prevăzute la art. 25 din Legea nr. 182/2002, potrivit competenţelor, prin cel mai operativ sistem de comunicare, despre compromiterea unor astfel de informaţii.

(2) Înştiinţarea prevăzută la alin. (1) se face în scopul obţinerii sprijinului necesar pentru recuperarea informaţiilor, evaluarea prejudiciilor, diminuarea şi înlăturarea consecinţelor.

(3) Înştiinţarea trebuie să conţină:

a) prezentarea informaţiilor compromise, respectiv clasificarea, marcarea, conţinutul, data emiterii, numărul de înregistrare şi de exemplare, emitentul şi 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 informaţiile au fost expuse compromiterii şi 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 instituţiilor competente, înstiinţările preliminare vor fi completate pe măsura derulării cercetărilor.

(5) Documentele privind evaluarea prejudiciilor şi activităţile ce urmează a fi intreprinse ca urmare a compromiterii vor fi prezentate instituţiilor competente.

ART. 89

Pentru prejudiciile cauzate deţinătorului informaţiei 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 informaţiile respective au fost compromise;

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

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

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

(3) În cazul săvaârşirii de infracţiuni la protecţia secretului de stat, unitatile deţinătoare au obligaţia de a sesiza organele de urmărire penală şi de a pune la dispoziţia acestora datele şi materialele necesare probării faptelor.

ART. 91

(1) Structura/funcţionarul de securitate are obligaţia de a tine evidenţa cazurilor de încălcare a reglementărilor de securitate, a documentelor de cercetare şi a măsurilor de solutionare şi să le pună la dispoziţia autorităţilor desemnate de securitate, conform competenţelor ce le revin.

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

ART. 92

Litigiile cu privire la calitatea de emitent ori deţinător sau cele determinate de conţinutul informaţiilor secrete de stat, inclusiv drepturile patrimoniale ce revin emitentului din contractele de cesiune şi licenţă, precum şi litigiile referitoare la nerespectarea dispoziţiilor legale privind dreptul de autor şi drepturile conexe, invenţiile şi inovaţiile, protecţia modelelor industriale, combaterea concurenţei neloiale şi a celor stipulate în tratatele, acordurile şi înţelegerile la care România este parte, sunt de competenţa instanţelor judecătoreşti.

SECŢIUNEA a 3-a
Protecţia prin măsuri procedurale

ART. 93

Toate unităţile care deţin informaţii secrete de stat au obligaţia sa stabilească norme interne de lucru şi de ordine interioară destinate protecţiei acestor informaţii, potrivit actelor normative în vigoare.

ART. 94

(1) Măsurile procedurale de protecţie a informaţiilor secrete de stat vor fi integrate în programul de prevenire a scurgerii de informaţii clasificate, întocmit potrivit anexei nr. 10,

care va fi prezentat, spre avizare, autorităţii abilitate să coordoneze activitatea şi să controleze măsurile privitoare la protecţia informaţiilor clasificate, potrivit legii.

(2) Sunt exceptate de obligativitatea prezentării, spre avizare, a programului de prevenire a scurgerii de informaţii, menţionat la alin. (1), instituţiile prevăzute la art. 25 alin. (4) din Legea nr. 182/2002.

ART. 95

Angajamentele de confidenţialitate întocmite potrivit reglementărilor în vigoare vor garanta ca informaţiile la care se acordă acces sunt protejate corespunzător.

SECŢIUNEA a 4-a
Protecţia fizică

ART. 96

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

ART. 97

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

a) nivelul de secretizare a informaţiilor, volumul şi localizarea acestora;

b) tipul containerelor în care sunt depozitate informaţiile;

c) caracteristicile clădirii şi zonei de amplasare.

ART. 98

Zonele în care sunt manipulate sau stocate informaţii secrete de stat trebuie organizate şi administrate în aşa fel încât sş corespundă uneia din următoarele categorii:

a) zona de securitate clasa I, care presupune ca orice persoană aflată în interiorul acesteia are acces la informaţii secrete de stat, de nivel strict secret de importanţă deosebită şi strict secret, şi care necesită:

- perimetru clar determinat şi protejat, în care toate intrarile şi iesirile sunt supravegheate;

– controlul sistemului de intrare, care să permită numai accesul persoanelor verificate corespunzător şi autorizate în mod special;

– indicarea clasei şi a nivelului de secretizare a informaţiilor existente în zona;

b) zona de securitate clasa a II-a, care presupune ca gestionarea informaţiilor de nivel secret se realizează prin aplicarea unor măsuri specifice de protecţie împotriva accesului persoanelor neautorizate şi care necesită:

- perimetru clar delimitat şi protejat, în care toate intrările şi ieşirile sunt supravegheate;

– controlul sistemului de intrare care să permită accesul neînsoţit numai persoanelor verificate şi autorizate să pătrunda în această zonă;

– reguli de însoţire, supraveghere şi prevenire a accesului persoanelor neautorizate la informaţii 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 informaţiile 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 şi al vehiculelor.

ART. 101

(1) Accesul în zonele de securitate clasa I şi clasa a II-a va fi controlat prin verificarea permisului de acces sau printr-un sistem de recunoaştere individuală aplicat personalului.

(2) Unităţile deţinătoare de informaţii 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 unităţii emitente sau locul în care deţinătorul are acces.

ART. 103

Unităţile vor organiza, la intrarea sau la ieşirea din zonele de securitate clasa I sau clasa a II-a, controale planificate şi inopinate ale bagajelor, incluzând colete, genţi şi alte tipuri de suporţi în care s-ar putea transporta materiale şi informaţii secrete de stat.

ART. 104

Personalul inclus în sistemul de pază şi apărare a obiectivelor, sectoarelor şi locurilor în care sunt gestionate informaţii secrete de stat trebuie să deţină autorizaţie de acces corespunzător nivelului de secretizare a informaţiilor necesare îndeplinirii atribuţiilor ce îi revin.

ART. 105

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

ART. 106

Conducătorii unităţilor deţinătoare de informaţii secrete de stat vor stabili reguli cu privire la circulaţia şi ordinea interioară în zonele de securitate, astfel încât accesul să fie

permis exclusiv posesorilor de certificate de securitate şi autorizaţii de acces, cu respectarea principiului necesităţii de a cunoaşte.

ART. 107

Accesul pentru intervenţii tehnice, reparaţii sau activităţi de deservire în locuri în care se lucrează cu informaţii secrete de stat ori în care se păstrează, se prelucrează sau se multiplică astfel de informaţii este permis numai angajaţilor unităţii care deţin autorizaţii de acces, corespunzător celui mai înalt nivel de secretizare a informaţiilor pe care le-ar putea cunoaşte.

ART. 108

(1) Pentru a distinge persoanele care au acces în diferite locuri sau sectoare în care sunt gestionate informaţii secrete de stat, acestea vor purta însemne sau echipamente specifice.

(2) În locurile şi sectoarele în care sunt gestionate informaţii secrete de stat, însemnele şi echipamentele distinctive se stabilesc prin regulamente de ordine interioară.

(3) Evidenţa legitimaţiilor, permiselor şi a altor însemne şi echipamente distinctive va fi ţinută de structura/funcţionarul de securitate al unităţii.

ART. 109

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

(2) În situaţiile menţionate la alin. (1), conducătorul instituţiei va dispune cercetarea împrejurărilor în care s-au produs şi va informa autoritatea desemnată de securitate competentă.

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

ART. 110

Accesul fiecărui angajat al unităţii deţinătoare de informaţii 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 individualizate prin aplicarea unor semne distinctive.

(2) Permisele de acces se vizează semestrial.

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

ART. 112

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

ART. 113

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

ART. 114

(1) Accesul angajaţilor agenţilor economici care efectuează lucrări de construcţii, reparaţii şi întreţinere a clădirilor, instalaţiilor sau utilităţilor în zonele administrative ori în zonele de securitate se realizează cu documente de acces temporar eliberate de conducătorii unităţilor beneficiare, pe baza actelor de identitate, la solicitarea reprezentanţilor autorizaţi ai agenţilor economici în cauză.

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

(3) Documentul de acces temporar are valabilitate pe durata executării lucrărilor şi se vizează trimestrial, iar la terminarea activităţilor se restituie emitentului.

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

ART. 115

Reprezentanţii instituţiilor care, potrivit competenţelor legale, au atribuţii de coordonare şi control pe linia protecţiei informaţiilor clasificate au acces la obiectivele, sectoarele şi locurile în care sunt gestionate informaţii clasificate, pe baza legitimaţiei de serviciu şi a delegaţiei speciale, semnată de conducătorul autorităţii pe care o reprezintă.

ART. 116

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

ART. 117

Persoanele care solicită angajări, audienţe, ori care prezintă reclamaţii şi sesizări vor fi primite în afara zonelor administrative sau în locuri special amenajate, cu aprobarea conducătorului unităţii.

ART. 118

În afara orelor de program şi în zilele nelucrătoare, se vor organiza patrulări pe perimetrul unităţii, la intervale care vor fi stabilite prin instrucţiuni elaborate pe baza planului de pază şi apărare al obiectivului.

ART. 119

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

(2) Timpul de reacţie a personalului de pază şi apărare va fi testat periodic pentru a garanta intervenţia operativă în situaţii de urgenţă.

ART. 120

(1) Unităţile care gestionează informaţii secrete de stat vor întocmi planul de pază şi apărare a obiectivelor, sectoarelor şi locurilor care prezintă importanţă deosebită pentru protecţia informaţiilor clasificate.

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

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

a) date privind delimitarea şi marcarea zonelor de securitate, dispunerea posturilor de pază şi măsurile de supraveghere a perimetrului protejat;

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

c) măsurile de avertizare şi alarmare pentru situaţii de urgenţă;

d) planul de evacuare a documentelor şi modul de acţiune în caz de urgenţă;

e) procedura de raportare, cercetare şi evidenţă a incidentelor de securitate.

ART. 121

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

a) containere clasa A, autorizate la nivel naţional pentru păstrarea informaţiilor strict secrete de importanţă deosebită în zona de securitate clasa I;

b) containere clasa B, autorizate la nivel naţional pentru păstrarea informaţiilor strict secrete şi secrete în zone de securitate clasa I sau clasa a II-a.

ART. 122

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

(2) Standardele în care trebuie să se încadreze containerele din clasele A şi 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 informaţiile secrete de stat pot fi păstrate pe rafturi deschise sau pot fi expuse pe hărţi, planşe ori diagrame.

(2) Pereţii, podelele, plafoanele, uşile şi încuietorile încăperilor de securitate vor asigura protecţia echivalentă clasei containerului de securitate aprobat pentru păstrarea informaţiilor clasificate potrivit nivelului de secretizare.

ART. 124

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

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

ART. 125

În situaţii de urgenţă, dacă informaţiile secrete de stat trebuie evacuate, se vor utiliza lăzi metalice autorizate la nivel naţional din clasa corespunzătoare nivelului de secretizare a acestor informaţii.

ART. 126

Încuietorile folosite la containerele şi încăperile de securitate în care sunt păstrate informaţii 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 şi încuietorilor, pe grupe de utilizare, se stabilesc de ORNISS.

ART. 128

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

ART. 129

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

(2) Predarea şi primirea cheilor de la încăperile şi containerele de securitate se vor face, pe bază de semnătura, în condica special destinată - anexa nr. 11.

ART. 130

(1) Pentru situaţiile de urgenţă, un rând de chei suplimentare sau, după caz, o evidenţă scrisă a combinaţiilor încuietorilor, vor fi păstrate în plicuri mate sigilate, în containere separate, într-un compartiment stabilit de conducerea unităţii, sub control corespunzător.

(2) Evidenţa fiecărei combinaţii se va păstra în plic separat.

(3) Cheilor şi plicurilor cu combinaţii trebuie să li se asigure acelaşi nivel de protecţie ca şi informaţiilor la care permit accesul.

ART. 131

Combinaţiile încuietorilor de la încăperile şi containerele de securitate vor fi cunoscute de un număr restrâns de persoane desemnate de conducerea unităţii.

ART. 132

Cheile şi combinaţiile 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 situaţii de natură să le facă vulnerabile;

c) la intervale regulate, de preferinţă o dată la şase luni, fără a se depăşi 12 luni.

ART. 133

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

(2) Orice defecţiune sau intervenţie neautorizată asupra sistemelor de alarmă sau de supraveghere destinate protecţiei informaţiilor secrete de stat trebuie să avertizeze personalul care le monitorizează.

(3) Dispozitivele de alarmare trebuie să intre în funcţiune în cazul penetrării pereţilor, podelelor, tavanelor şi deschizăturilor, sau la mişcări în interiorul încăperilor de securitate.

ART. 134

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

ART. 135

Unităţile deţinătoare de informaţii secrete de stat au obligaţia de a asigura protecţia acestora împotriva ascultărilor neautorizate, pasive sau active.

ART. 136

(1) Protecţia împotriva ascultării pasive a discuţiilor confidenţiale se realizează prin izolarea fonică a încăperilor.

(2) Protecţia împotriva ascultărilor active, prin microfoane, radio-emiţători şi alte dispozitive implantate, se realizează pe baza inspecţiilor de securitate a încăperilor, accesoriilor, instalaţiilor, sistemelor de comunicaţii, echipamentelor şi mobilierului de birou, realizate de unităţile specializate, potrivit competenţelor 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 inspecţii fizice şi tehnice.

(3) Inspecţiile fizice şi tehnice vor fi organizate, în mod obligatoriu, în urma oricărei intrări neautorizate sau suspiciuni privind accesul persoanelor neautorizate şi după executarea lucrărilor de reparaţii, întreţinere, zugrăvire sau redecorare.

(4) Niciun 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 discuţii confidenţiale şi 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) Inspecţiile de securitate tehnică în zonele prevăzute în alin. (1) trebuie efectuate, în mod obligatoriu, înaintea începerii convorbirilor, pentru identificarea fizică a dispozitivelor de ascultare şi verificarea sistemelor telefonice, electrice sau de alta natură, care ar putea fi utilizate ca mediu de atac.

ART. 139

(1) Echipamentele de comunicaţii şi dotările din birouri, în principal cele electrice şi electronice, trebuie verificate de specialişti ai autorităţilor desemnate de securitate competente, înainte de a fi folosite în zonele în care se lucrează ori se discută despre informaţii strict secrete sau strict secrete de importanţă deosebită, pentru a preveni transmiterea sau interceptarea, în afara cadrului legal, a unor informaţii inteligibile.

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

SECŢIUNEA a 5-a
Protecţia personalului

ART. 140

(1) Unităţile deţinătoare de informaţii secrete de stat au obligaţia de a asigura protecţia personalului desemnat să asigure securitatea acestora ori care are acces la astfel de informaţii, potrivit prezentelor standarde.

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

a) să prevină accesul persoanelor neautorizate la informaţii secrete de stat;

b) să garanteze ca informaţiile secrete de stat sunt distribuite deţinătorilor de certificate de securitate/autorizaţii de acces, cu respectarea principiului necesităţii de a cunoaşte;

c) să permită identificarea persoanelor care, prin acţiunile sau inacţiunile lor, pot pune în pericol securitatea informaţiilor secrete de stat şi să prevină accesul acestora la astfel de informaţii.

(3) Protecţia personalului se realizează prin: selecţionarea, verificarea, avizarea şi autorizarea accesului la informaţiile secrete de stat, revalidarea, controlul şi instruirea personalului, retragerea certificatului de securitate sau autorizaţiei de acces.

ART. 141

(1) Acordarea certificatului de securitate - anexa nr. 12 - şi autorizaţiei de acces la informaţii clasificate - anexa nr. 13, potrivit nivelului de secretizare, este condiţionată de avizul autorităţii desemnate de securitate.

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

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

(4) În funcţie de avizul comunicat de autoritatea desemnată, ORNISS va aproba eliberarea certificatului de securitate sau autorizaţiei de acces şi va încunoştiinţa oficial conducătorul unităţii.

(5) După obţinerea aprobării menţionate la alin. (4), conducătorul unităţii va notifica la ORNISS şi va elibera certificatul de securitate sau autorizaţia de acces, conform art. 154.

ART. 142

Certificatul de securitate sau autorizaţia 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 atenţie specială persoanelor care:

a) urmeaza să aibă acces la informaţii strict secrete şi strict secrete de importanţă deosebită;

b) ocupa funcţii ce presupun accesul permanent la un volum mare de informaţii secrete de stat;

c) pot fi vulnerabile la acţiuni ostile, ca urmare a importanţei funcţiei în care vor fi numite, a mediului de relaţii sau a locului de muncă anterior.

ART. 144

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

(2) Când persoanele urmează să îndeplinească funcţii care le pot facilita accesul la informaţii secrete de stat doar în anumite circumstanţe - paznici, curieri, personal de întreţinere - se va acorda atenţie primei verificări de securitate.

ART. 145

Unităţile care gestionează informaţii clasificate sunt obligate să ţină un registru de evidenţă a certificatelor de securitate şi autorizaţiilor de acces la informaţii clasificate - anexa nr. 18.

ART. 146

(1) Ori de câte ori apar indicii că deţinătorul certificatului de securitate sau autorizaţiei de acces nu mai îndeplineşte criteriile de compatibilitate privind accesul la informaţiile secrete de stat, verificările de securitate se reiau la solicitarea conducătorului unităţii adresată ORNISS.

(2) ORNISS poate solicita reluarea verificărilor, la sesizarea autorităţilor competente, în situaţia în care sunt semnalate incompatibilităţi privind accesul la informaţii secrete de stat.

ART. 147

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

ART. 148

(1) Structura/funcţionarul de securitate are obligaţia să pună la dispoziţia persoanei selecţionate formularele tip corespunzătoare nivelului de acces pentru care se solicită eliberarea certificatului de securitate/autorizaţiei de acces şi să acorde asistenţă în vederea completării acestora.

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

a) pentru acces la informaţii strict secrete de importanţă deosebită - 90 de zile lucrătoare;

b) pentru acces la informaţii strict secrete - 60 de zile lucrătoare;

c) pentru acces la informaţii secrete - 30 de zile lucrătoare.

ART. 149

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

ART. 150

(1) După primirea formularelor, instituţia abilitată va efectua verificările în termenele prevăzute la art. 148 şi va comunica, în scris - anexa nr. 20, la ORNISS, avizul privind acordarea certificatului de securitate sau autorizaţiei de acces la informaţii 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 situaţia în care sunt semnalate elemente relevante din punct de vedere al protecţiei informaţiilor 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/autorizaţiei de acces la informaţii secrete de stat şi va comunica unităţii solicitante - anexa nr. 21.

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

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

ART. 152

(1) Verificarea în vederea avizării pentru accesul la informaţii secrete de stat se efectuează cu respectarea legislaţiei în vigoare privind responsabilitatile în domeniul protecţiei unor asemenea informaţii, de către următoarele instituţii:

a) Serviciul Român de Informaţii, pentru:

- personalul propriu;

– personalul autorităţilor şi instituţiilor publice din zona de competenţă, potrivit legii;

– personalul agenţilor economici cu capital integral sau parţial de stat şi al persoanelor juridice de drept public sau privat, altele decât cele date în competenţa instituţiilor menţionate la lit. b), c) şi d);

– personalul din cadrul Parchetului Naţional Anticorupţie.

b) Ministerul Apărării Naţionale, pentru:

– personalul militar şi civil propriu;

– personalul Oficiului Central de Stat pentru Probleme Speciale, Administraţiei Naţionale a Rezervelor de Stat şi altor persoane juridice stabilite prin lege şi personalul militar care îşi desfăşoară activitatea în străinătate;

c) Serviciul de Informaţii Externe, pentru:

- personalul militar sau civil propriu;

– personalul român al reprezentanţelor diplomatice, misiunilor permanente, consulare, centrelor culturale, organismelor internaţionale şi altor reprezentante ale statului român în străinătate;

– cetatenii români aflaţi în străinătate în cadrul unor contracte, stagii de perfecţionare, programe de cercetare sau în calitate de angajaţi la firme;

d) Ministerul Administraţiei şi Internelor, Serviciul de Protecţie şi Pază şi Serviciul de Telecomunicaţii Speciale, pentru personalul propriu şi al persoanelor juridice a căror activitate o coordonează.

e) Ministerul Justiţiei, pentru personalul propriu şi al persoanelor juridice a căror activitate o coordonează, altul decât cel pentru care verificarea este de competenţa Serviciului Român de Informaţii.

(2) Instituţiile menţionate la alin. (1) sunt abilitate să solicite şi să primească informaţii de la persoane juridice şi fizice, în vederea acordării avizului de acces la informaţii clasificate.

ART. 153

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

ART. 154

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

ART. 155

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

ART. 156

Pentru cadrele proprii, Ministerul Apărării Naţionale, Ministerul de Interne, Ministerul Justiţiei, Serviciul Român de Informaţii, Serviciul de Informaţii Externe, Serviciul de Telecomunicaţii Speciale şi Serviciul de Protecţie şi Pază vor elabora instrucţiuni interne privind verificarea, avizarea, eliberarea şi evidenţa certificatelor de securitate/autorizaţiilor de acces.

ART. 157

Decizia privind avizarea eliberării certificatului de securitate/autorizaţiei de acces va fi luată pe baza tuturor informaţiilor disponibile şi va avea în vedere:

a) loialitatea indiscutabilă a persoanei;

b) caracterul, obiceiurile, relaţiile şi discreţia persoanei, care să ofere garanţii asupra:

- corectitudinii în gestionarea informaţiilor secrete de stat;

– oportunităţii accesului neînsoţit în compartimente, obiective, zone şi locuri de securitate în care se află informaţii secrete de stat;

– respectării reglementărilor privind protecţia informaţiilor secrete de stat din domeniul său de activitate.

ART. 158

(1) Principalele criterii de evaluare a compatibilităţii în acordarea avizului pentru eliberarea certificatului de securitate/autorizaţiei de acces vizează atât trasăturile de caracter, cât şi situaţiile sau împrejurările din care pot rezultă riscuri şi vulnerabilităţi de securitate.

(2) Sunt relevante şi vor fi luate în considerare, la acordarea avizului de securitate, caracterul, conduita profesională sau socială, concepţiile şi mediul de viaţă al soţului/sotiei sau concubinului/concubinei persoanei solicitante.

ART. 159

Următoarele situaţii imputabile atât solicitantului, cât şi soţului/soţiei sau concubinului/concubinei acestuia reprezintă elemente de incompatibilitate pentru acces la informaţii secrete de stat:

a) dacă a comis sau a intenţionat să comită, a fost complice, a complotat sau a instigat la comiterea de acte de spionaj, terorism, trădare ori alte infracţiuni contra siguranţei statului;

b) dacă a încercat, a susţinut, a participat, a cooperat sau a sprijinit acţiuni de spionaj, terorism ori persoane suspectate de a se încadra în această categorie sau de a fi membre ale unor organizaţii ori puteri străine inamice ordinii de drept din ţara noastră;

c) dacă este sau a fost membru al unei organizaţii care a încercat, încearcă sau susţine răsturnarea ordinii constituţionale prin mijloace violente, subversive sau alte forme ilegale;

d) dacă este sau a fost un susţinător al vreunei organizaţii prevăzute la lit. c), este sau a fost în relaţii apropiate cu membrii unor astfel de organizaţii intr-o formă de natură să ridice suspiciuni temeinice cu privire la încrederea şi loialitatea persoanei.

ART. 160

Constituie elemente de incompatibilitate pentru accesul solicitantului la informaţii secrete de stat oricare din următoarele situaţii:

a) dacă în mod deliberat a ascuns, a interpretat eronat sau a falsificat informaţii cu relevanţă în planul siguranţei naţionale ori a minţit în completarea formularelor tip sau în cursul interviului de securitate;

b) are antecedente penale sau a fost sancţionat contravenţional pentru fapte care indică tendinţe infracţionale;

c) are dificultăţi financiare serioase sau există o discordanţă semnificativă între nivelul său de trai şi veniturile declarate;

d) consumă în mod excesiv băuturi alcoolice ori este dependent de alcool, droguri sau de alte substanţe interzise prin lege care produc dependenţă;

e) are sau a avut comportamente imorale sau deviaţii de comportament care pot genera riscul ca persoana să fie vulnerabilă la şantaj sau presiuni;

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

g) a încălcat reglementările privind protecţia informaţiilor clasificate;

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

i) poate fi supus la presiuni din partea rudelor sau persoanelor apropiate care ar putea genera vulnerabilităţi exploatabile de către serviciile de informaţii ale căror interese sunt ostile României şi aliaţilor săi.

ART. 161

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

a) în exercitarea atribuţiilor profesionale lucrează cu date şi informaţii de nivel secret;

b) fac parte din personalul de execuţie sau administrativ şi, în virtutea acestui fapt, pot intra în contact cu date şi informaţii de acest nivel;

c) este de presupus că vor lucra cu date şi informaţii de nivel secret, datorită funcţiei pe care o deţin;

d) se presupune că nu pot avansa profesional în funcţie, dacă nu au acces la astfel de informaţii.

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

a) verificarea corectitudinii datelor menţionate în formularul de bază, anexa nr. 15;

b) referinţe de la locurile de muncă şi din mediile frecventate, de la cel puţin trei persoane.

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

ART. 162

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

a) în exercitarea atribuţiilor profesionale lucrează cu date şi informaţii de nivel strict secret;

b) fac parte din personalul de execuţie sau administrativ şi, în virtutea acestui fapt, pot intra în contact cu date şi informaţii de acest nivel;

c) este de presupus că vor lucra cu date şi informaţii de nivel strict secret, datorită funcţiei pe care o deţin;

d) se presupune că nu pot avansa profesional în funcţie, dacă nu au acces la astfel de informaţii.

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

a) verificarea corectitudinii datelor personale menţionate în formularul de bază şi în formularul suplimentar, anexele nr. 15 şi 16;

b) referinţe minime de la locurile de muncă şi din mediile frecventate de la cel puţin trei persoane;

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

d) investigaţii la locul de muncă şi la domiciliu, care să acopere o perioadă de zece ani anteriori datei avizului sau începând de la vârsta 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/autorizaţiilor de acces la informaţii strict secrete de importanţă deosebită se efectuează verificări asupra persoanelor care:

a) în exercitarea atribuţiilor profesionale lucrează cu date şi informaţii de nivel strict secret de importanţă deosebită;

b) fac parte din personalul de execuţie sau administrativ şi, în virtutea acestui fapt, pot intra în contact cu informaţii de acest nivel.

(2) Avizarea accesului la informaţiile strict secrete de importanţă deosebită se va baza pe:

a) verificarea corectitudinii datelor menţionate în formularul de bază, formularul suplimentar şi formularul financiar, anexele nr. 15, 16 şi 17;

b) investigaţii de cunoaştere a conduitei şi antecedentelor la domiciliul actual şi cele anterioare, la locul de muncă actual şi la cele anterioare, precum şi la instituţiile de învăţământ urmate, începând de la vârsta de 18 ani, investigaţii care nu se vor limita la audierea persoanelor indicate de solicitantul avizului;

c) verificări ale mediului relaţional pentru a identifica existenţa 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 intreprinse, 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 informaţii ce evidenţiază riscuri de securitate, se va realiza o verificare suplimentară, cu folosirea metodelor şi mijloacelor specifice instituţiilor cu atribuţii în domeniul siguranţei naţionale.

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

ART. 165

În funcţie de nivelul de secretizare a informaţiilor secrete de stat la care se acordă accesul, investigaţia de cunoaştere a antecedentelor va avea în vedere, gradual, următoarele:

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

b) verificarea cazierului judiciar, în evidenţele centrale şi locale ale poliţiei, în baza de date a Registrului Comerţului, precum şi în alte evidenţe;

c) stabilirea naţionalităţii persoanei şi cetăţeniei prezente şi anterioare;

d) confirmarea pregătirii în şcolile, universităţile şi alte instituţii de învăţământ urmate de titular, de la împlinirea vârstei de 18 ani;

e) cunoaşterea conduitei la locul de muncă actual şi la cele anterioare, cu referinţe obţinute din dosarele de angajare, aprecierile anuale asupra performanţelor şi eficienţei activităţii, ori furnizate de şefii instituţiilor, şefii de compartimente sau colegi;

f) organizarea de interviuri şi discuţii cu persoane care pot face aprecieri asupra trecutului, activităţii, comportamentului şi corectitudinii persoanei verificate;

g) cunoaşterea comportării pe timpul serviciului militar şi a modalităţii în care a fost trecut în rezervă;

h) existenţa unor riscuri de securitate datorate unor eventuale presiuni exercitate din străinătate;

i) solvabilitatea şi reputaţia financiară a persoanei;

j) stabilirea indiciilor şi obţinerea de probe conform cărora persoana solicitantă este sau a fost membru ori afiliat al vreunei organizaţii, asociaţii, mişcări, grupări străine sau autohtone, care au sprijinit sau au susţinut comiterea unor acte de violenţă, în scopul

afectării drepturilor altor persoane, sau care încearcă să schimbe ordinea de stat prin mijloace neconstituţionale.

ART. 166

(1) În cazul în care o persoană deţine certificat de securitate/autorizaţie de acces la informaţii naţionale clasificate, acesteia i se poate elibera şi certificat de securitate pentru acces la informaţii NATO clasificate valabil pentru acelaşi nivel de secretizare sau pentru un nivel inferior.

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

(3) Valabilitatea certificatului/autorizaţiei eliberate în condiţiile alin. (1) şi (2) încetează la expirarea termenului de valabilitate al certificatului/autorizaţiei initiale.

ART. 167

(1) Revalidarea avizului privind accesul la informaţii clasificate presupune reverificarea persoanei deţinătoare a unui certificat de securitate/autorizaţie de acces în vederea menţinerii sau retragerii acesteia.

(2) Revalidarea poate avea loc la solicitarea unităţii în care persoana îşi desfăşoară activitatea, sau a ORNISS, în oricare din următoarele situaţii:

a) atunci când pentru îndeplinirea sarcinilor de serviciu ale persoanei deţinătoare este necesar accesul la informaţii de nivel superior;

b) la expirarea perioadei de valabilitate a certificatului de securitate/autorizaţiei de acces deţinute anterior;

c) în cazul în care apar modificări în datele de identificare ale persoanei;

d) la apariţia unor riscuri de securitate din punct de vedere al compatibilităţii accesului la informaţii clasificate.

ART. 168

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

a) în cazul în care se constată neconcordanţe între datele declarate în formularele tip şi cele reale;

b) în cazul în care, pe parcursul perioadei de valabilitate a certificatului de securitate/autorizaţiei de acces s-au evidenţiat riscuri de securitate;

c) În cazul în care ORNISS solicită acest lucru, în mod expres.

ART. 169

Pentru revalidarea accesului la informaţii secrete de stat se derulează aceleaşi activităţi ca şi la acordarea avizului iniţial, verificările raportându-se la perioada scursă de la eliberarea certificatului de securitate sau autorizaţiei de acces anterioare.

ART. 170

(1) Persoanele cărora li se eliberează certificate de securitate/autorizaţii de acces vor fi instruite, obligatoriu, cu privire la protecţia informaţiilor clasificate, înaintea începerii activităţii şi ori de câte ori este nevoie.

(2) Activitatea de pregătire se efectuează planificat, în scopul prevenirii, contracarării şi eliminării riscurilor şi ameninţărilor la adresa securităţii informaţiilor clasificate.

(3) Pregătirea personalului se realizează diferenţiat, potrivit nivelului de secretizare a informaţiilor la care certificatul de securitate sau autorizaţia de acces permite accesul şi va fi înscrisă în fişa individuală de pregătire, care se păstrează la structura/funcţionarul de securitate.

(4) Toate persoanele încadrate în funcţii care presupun accesul la informaţii clasificate trebuie să fie instruite temeinic, atât în perioada premergătoare numirii în funcţie, cat şi la intervale prestabilite, asupra necesităţii şi modalităţilor de asigurare a protecţiei acestor informaţii.

(5) După fiecare instruire, persoana care deţine certificat de securitate sau autorizaţie de acces va semna că a luat act de conţinutul reglementărilor privind protecţia informaţiilor secrete de stat.

ART. 171

(1) Pregătirea personalului urmăreşte însuşirea corectă a standardelor de securitate şi a modului de implementare eficientă a măsurilor de protecţie a informaţiilor clasificate.

(2) Organizarea şi coordonarea activităţii de pregătire a structurilor/funcţionarilor de securitate sunt asigurate de autorităţile desemnate de securitate.

ART. 172

(1) Planificarea şi organizarea activităţii de pregătire a personalului se realizează de către structura/funcţionarul de securitate.

(2) Autorităţile desemnate de securitate vor controla, potrivit competenţelor, modul de realizare a activităţii de pregătire a personalului care accesează informaţii secrete de stat.

ART. 173

(1) Pregătirea individuală a persoanelor care deţin certificate de securitate/autorizaţii de acces se realizează în raport cu atribuţiile profesionale.

(2) Toate persoanele care gestionează informaţii clasificate au obligaţia să cunoască reglementările privind protecţia informaţiilor clasificate şi procedurile interne de aplicare a măsurilor de securitate specifice.

ART. 174

(1) Pregătirea personalului se realizează sub formă de lecţii, informări, prelegeri, simpozioane, schimb de experienţă, seminarii, şedinţe cu caracter aplicativ şi se poate finaliza prin verificări sau certificări ale nivelului de cunoştinţe.

(2) Activităţile de pregătire vor fi organizate de structura/funcţionarul de securitate, conform tematicilor cuprinse în programele aprobate de conducerea unităţii.

ART. 175

Certificatul de securitate sau autorizaţia de acces îşi încetează valabilitatea şi se va retrage în următoarele cazuri:

a) la solicitarea ORNISS;

b) prin decizia conducătorului unităţii care a eliberat certificatul/autorizaţia;

c) la solicitarea autorităţii desemnate de securitate competente;

d) la plecarea din unitate sau la schimbarea locului de muncă al deţinătorului în cadrul unităţii, dacă noul loc de muncă nu presupune lucrul cu astfel de informaţii secrete de stat;

e) la schimbarea nivelului de acces.

ART. 176

La retragerea certificatului de securitate sau autorizaţiei de acces, în cazurile prevăzute la art. 175 lit. a)-d), angajatului i se va interzice accesul la informaţii secrete de stat, iar conducerea unităţii 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 autorizaţiei de acces, după care va distruge ambele exemplare, pe bază de proces-verbal.

SECŢIUNEA a 6-a
Accesul cetăţenilor străini, al cetăţenilor români care au şi cetăţenia altui stat, precum şi al persoanelor apatride la informaţiile secrete de stat şi în locurile în care se desfăşoară activităţi, se expun obiecte sau se execută lucrări din această categorie

ART. 178

Cetăţenii străini, cetăţenii români care au şi cetăţenia altui stat, precum şi persoanele apatride pot avea acces la informaţii secrete de stat, cu respectarea principiului necesităţii de a cunoaşte şi a convenţiilor, protocoalelor, contractelor şi altor înţelegeri încheiate în condiţiile legii.

ART. 179

(1) Persoanele prevăzute la art. 178 vor fi verificate şi avizate conform prezentelor standarde, la solicitarea conducătorului unităţii în cadrul căreia acestea urmează să desfăşoare activităţi care presupun accesul la informaţii secrete de stat.

(2) Conducătorul unităţii va elibera persoanelor respective o autorizaţie de acces corespunzătoare nivelului de secretizare a informaţiilor la care urmeaza să aibă acces, valabilă numai pentru perioada desfăşurării activităţilor comune, în baza acordului comunicat de ORNISS.

ART. 180

(1) Persoanele prevăzute la art. 178 care desfăşoară activităţi de asistenţa tehnică, consultanţă, colaborare ştiintifică ori specializare vor purta ecusoane distincte faţă de cele folosite de personalul propriu şi vor fi însoţite permanent de persoane anume desemnate de conducerea unităţii respective.

(2) Conductorul unităţii este obligat să delimiteze strict sectoarele şi compartimentele în care persoanele menţionate la art. 178 pot avea acces şi va stabili măsuri pentru prevenirea prezentei acestora în alte locuri în care se gestionează informaţii secrete de stat.

ART. 181

(1) Structura/funcţionarul de securitate are obligaţia de a instrui persoanele prevăzute la art. 178 în legătură cu regulile pe care trebuie să le respecte privind protecţia informaţiilor secrete de stat.

(2) Autorizaţia de acces se va elibera numai după însuşirea reglementărilor privind protecţia informaţiilor clasificate şi semnarea angajamentului de confidenţialitate.

ART. 182

Nerespectarea de către persoanele prevăzute la art. 178 a regulilor privind protecţia informaţiilor clasificate va determina, obligatoriu, retragerea autorizaţiei de acces.

CAPITOLUL V
Condiţiile de fotografiere, filmare, cartografiere şi executare a unor lucrări de arte plastice în obiective sau locuri care prezintă importanţă deosebită pentru protecţia informaţiilor 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 importanţă deosebită pentru protecţia informaţiilor secrete de stat, fără autorizaţie specială eliberată de către ORNISS, care va ţine evidenţa acestora, conform anexei nr. 23.

(2) Autorizaţia specială va fi eliberată de către ORNISS în baza avizului dat de ADS, precum şi de autorităţile sau instituţiile care au obiective, zone şi locuri de importanţă pentru protecţia informaţiilor clasificate în arealul în care urmează să se desfăşoare activităţi de această natură.

(3) Obiectivele şi mijloacele prevăzute la art. 17 din Legea nr. 182/2002
pot fi filmate şi fotografiate de către personalul militar, pentru nevoile interne ale instituţiilor militare, pe baza aprobării scrise a miniştrilor sau conducătorilor instituţiilor respective, pentru obiectivele, zonele sau locurile din competenţa lor.

ART. 184

Trupele Ministerului Apărării Naţionale, Ministerului de Interne şi Serviciului Român de Informaţii, aflate la instructie, în aplicaţii ori în interiorul obiectivelor prevăzute la art. 17 din Legea nr. 182/2002, pot fi fotografiate sau filmate în scopuri educative şi de pregătire militară, cu aprobarea conducătorilor acestor instituţii sau a împuterniciţilor desemnaţi.

ART. 185

Fotografierea, filmarea, cartografierea sau executarea de lucrări de arte plastice în zonele de securitate şi administrative ale unităţilor deţinătoare de secrete de stat este permisă numai cu aprobarea scrisă a împuterniciţilor abilitaţi să atribuie niveluri de secretizare conform art. 19 din Legea 182/2002, potrivit competenţelor materiale.

ART. 186

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

(2) Termenul de răspuns este de 60 de zile lucrătoare de la data primirii cererii. Pentru zborurile aerofotogrammetrice efectuate la scări de zbor mai mari de 1:20.000 în scopul realizării pe planuri topografice şi cadastrale, termenul este de 30 de zile lucrătoare.

(3) Titularii autorizaţiei speciale sunt obligaţi să se prezinte, înaintea începerii lucrărilor, la conducătorii instituţiilor unde acestea vor fi executate, pentru a se pune de acord cu privire la modalitatea de acţiune şi verificarea aparaturii ce va fi folosită.

ART. 187

Dacă solicitantul poseda autorizaţie de nivel corespunzător obiectivului vizat, autorizaţia specială va fi eliberată în termen de 15 zile lucrătoare de la data primirii solicitării, cu respectarea principiului nevoii de a cunoaşte.

ART. 188

Obiectivele, zonele şi locurile în care fotografierea, filmarea, cartografierea sau executarea de lucrări de arte plastice se efectuează numai cu autorizare vor fi marcate cu indicatoare de interdicţie în acest sens, care vor fi instalate prin grija instituţiilor cărora le aparţin, cu avizul de specialitate al organelor administraţiei publice locale.

ART. 189

(1) Emiterea, deţinerea sau folosirea de date şi documente geodezice, topo-fotogrammetrice şi cartografice, ce constituie secrete de stat, urmează, în privinţa clasificării, marcării, inscripţionării, procesării, manipulării, evidenţei, întocmirii, multiplicării, transmiterii, păstrării, transportului şi distrugerii acestora, regimul prevăzut de reglementările în vigoare privitoare la protecţia informaţiilor clasificate în România.

(2) Ministerele şi celelalte organe ale administraţiei publice centrale şi locale, care întocmesc documente geodezice, topo-fotogrammetrice şi cartografice cu caracter secret

de stat, le vor nominaliza în listele proprii de informaţii clasificate, potrivit dispoziţiilor legale în vigoare.

ART. 190

(1) Activitatea de aerofotografiere cu camere fotogrammetrice digitale sau analogice a teritoriului României, la o scară de zbor mai mare de 1:20.000, se efectuează pe baza autorizaţiei speciale eliberate de ORNISS şi în prezenţa reprezentantului Ministerului Apărării Naţionale.

(2) În vederea eliberării autorizaţiei menţionate la alin. (1), cererea adresată ORNISS trebuie să conţină, pe lângă datele prevăzute la art. 186 alin. (1), şi scara de zbor la care vor fi efectuate activităţile de aerofotografiere.

(3) Activităţile de developare a materialului fotografic şi scanarea negativelor, după caz, se pot realiza, în prezenţa reprezentantului Ministerului Apărării Naţionale, de către persoane juridice care îndeplinesc condiţiile legale privind protecţia informaţiilor clasificate.

(4) Materialele obţinute din activităţile de aerofotografiere prevăzute la alin. (1) se predau persoanelor juridice autorizate, pe bază de documente justificative, în prezenţa reprezentantului Ministerului Apărării Naţionale.

(5) ORNISS ţine evidenţa autorizaţiilor speciale şi dispune retragerea acestora, la propunerea motivată a organelor de control abilitate.

(6) Developarea materialului fotografic şi scanarea negativelor de către persoanele juridice autorizate se realizează exclusiv pe teritoriul naţional.

(7) Materialele rezultate în urma procesului de developare şi scanare, precum şi cele rezultate în urma activităţilor de aerofotografiere cu camere fotogrammetrice digitale sunt declasificate, cu avizul Autorităţilor Desemnate de Securitate (ADS), de către Ministerul Apărării Naţionale, în termen de 30 de zile lucrătoare de la primirea acestora.

(8) În termenul prevăzut la alin. (7) produsele finale rezultate în urma declasificării se vor preda la ORNISS, prin grija reprezentantului Ministerului Apărării Naţionale, pentru a fi puse la dispoziţie beneficiarului.

(9) Se exceptează de la obligaţia îndeplinirii procedurii prevăzute la alin. (1)-(8) activităţile de aerofotografiere, efectuate pe teritoriul României, la o scară de zbor mai mică sau egală cu 1:20.000.

CAPITOLUL VI
Exercitarea controlului asupra măsurilor privitoare la protecţia informaţiilor clasificate

ART. 191

(1) Serviciul Român de Informaţii, prin unitatea sa specializată, are competenţa generală de exercitare a controlului asupra modului de aplicare a măsurilor de protecţie de către instituţiile publice şi unităţile deţinătoare de informaţii clasificate.

(2) Activitatea de control în cadrul Ministerului Apărării Naţionale, Ministerului de Interne, Ministerului de Justiţie, Serviciului Român de Informaţii, Serviciului de Informaţii Externe, Serviciului de Protecţie şi Pază şi Serviciului de Telecomunicaţii Speciale se reglementează prin ordine ale conducătorilor acestor instituţii, potrivit legii.

(3) Controlul privind măsurile de protecţie a informaţiilor clasificate în cadrul Parlamentului, Administraţiei Prezidenţiale, Guvernului şi Consiliului Suprem de Apărare a Ţării se organizează conform legii.

(4) Activitatea de control în cadrul reprezentanţelor României în străinătate se reglementează şi se realizează de către Serviciul de Informaţii Externe.

ART. 192

Controlul are ca scop:

a) evaluarea eficienţei măsurilor concrete de protecţie adoptate la nivelul deţinătorilor de informaţii clasificate, în conformitate cu legea, cu prevederile prezentelor standarde şi altor norme în materie, precum şi cu programele de prevenire a scurgerii de informaţii clasificate;

b) identificarea vulnerabilităţilor existente în sistemul de protecţie a informaţiilor clasificate, care ar putea conduce la compromiterea acestor informaţii, în vederea luării măsurilor de prevenire necesare;

c) luarea măsurilor de remediere a deficienţelor şi de perfecţionare a cadrului organizatoric şi funcţional la nivelul structurii controlate;

d) constatarea cazurilor de nerespectare a normelor de protecţie a informaţiilor clasificate şi aplicarea sancţiunilor contravenţionale sau, după caz, sesizarea organelor de urmărire penală, în situaţia în care fapta constituie infracţiune;

e) informarea Consiliului Suprem de Apărare a Ţării şi Parlamentului cu privire la modul în care unităţile deţinătoare de informaţii clasificate aplică reglementările în materie.

ART. 193

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

(2) În cazul în care controlul relevă fapte şi disfuncţionalităţi de natură să reprezinte riscuri majore de securitate pentru protecţia informaţiilor clasificate va fi informat, de îndată, Consiliul Suprem de Apărare a Ţării, iar instituţia controlată va dispune măsuri imediate de remediere a deficienţelor constatate, va iniţia cercetarea administrativă şi, după caz, va aplica măsurile sancţionatorii şi va sesiza organele de urmărire penală, în situaţia în care rezultă indicii că s-ar fi produs infracţiuni.

ART. 194

În funcţie de obiectivele urmărite, controalele pot fi:

a) controale de fond, care urmăresc verificarea întregului sistem organizatoric, structural şi funcţional de protecţie a informaţiilor clasificate;

b) controale tematice, care vizează anumite domenii ale activităţii de protecţie a informaţiilor clasificate;

c) controale în situaţii de urgenţă, care au ca scop verificarea unor aspecte punctuale, stabilite ca urmare a identificării unui risc de securitate.

ART. 195

În funcţie de modul în care sunt stabilite şi organizate, controalele pot fi:

a) planificate;
b) inopinate;
c) determinate de situaţii de urgenţă.

ART. 196

Conducătorii unităţilor care fac obiectul controlului au obligaţia sa pună la dispoziţia echipelor de control toate informaţiile solicitate privind modul de aplicare a măsurilor prevăzute de lege pentru protecţia informaţiilor clasificate.

ART. 197

Conducătorii unităţilor deţinătoare de informaţii clasificate au obligaţia să organizeze anual şi ori de câte ori este nevoie controale interne privind gestionarea acestora.

CAPITOLUL VII
Securitatea industrială

SECŢIUNEA 1
Dispoziţii generale

ART. 198

Prevederile prezentului capitol se vor aplica tuturor persoanelor juridice de drept public sau privat care desfăşoară ori solicită să desfăşoare activităţi contractuale ce presupun accesul la informaţii clasificate.

SECŢIUNEA a 2-a
Atribuţiile Oficiului Registrului Naţional al Informaţiilor Secrete de Stat şi ale autorităţilor desemnate de securitate în domeniul protectiei informaţiilor clasificate care fac obiectul activităţilor contractuale

ART. 199

În domeniul protecţiei informaţiilor clasificate care fac obiectul activităţilor contractuale, ORNISS are următoarele atribuţii:

a) stabileşte strategia de implementare unitară la nivel naţional a măsurilor de protecţie a informaţiilor clasificate care fac obiectul activităţilor contractuale;

b) eliberează autorizaţia şi certificatul de securitate industrială, la cererea persoanelor juridice interesate;

c) gestionează, la nivel naţional, evidenţele privind: persoanele juridice deţinătoare de autorizaţii de securitate industrială; persoanele juridice deţinătoare de certificate de securitate industrială; persoanele fizice care deţin certificate de securitate sau autorizaţii de acces eliberate în scopul negocierii sau executării unui contract clasificat.

ART. 200

În sfera lor de competenţă legală, autorităţile desemnate de securitate au următoarele atribuţii:

a) efectuează verificările de securitate necesare acordării avizului de securitate industrială, pe care îl transmite la ORNISS în vederea eliberării autorizaţiei sau, după caz, a certificatului de securitate industrială;

b) asigura asistenţa de specialitate obiectivelor industriale în vederea implementării standardelor de securitate în domeniul protecţiei informaţiilor clasificate vehiculate în cadrul activităţilor industriale;

c) desfăşoară activităţi de pregătire a personalului cu atribuţii pe linia protecţiei informaţiilor clasificate, vehiculate în cadrul activităţilor industriale;

d) efectuează verificări în situaţiile în care s-au semnalat încălcări ale reglementărilor de protecţie, distrugeri, dispariţii, dezvăluiri neautorizate de informaţii clasificate, furnizate sau produse în cadrul unui contract clasificat;

e) se asigură că fiecare obiectiv industrial, în cadrul căruia urmeaza să fie gestionate informaţii clasificate, a desemnat o structură/funcţionar de securitate în vederea exercitării efective a atribuţiilor pe linia protecţiei acestora, în cadrul contractelor clasificate;

f) monitorizează, în condiţiile legii, modul de asigurare a protecţiei informaţiilor clasificate în procesul de negociere şi derulare a contractelor, iar în cazul în care constată factori de risc şi vulnerabilităţi, informează imediat ORNISS şi propune măsurile necesare;

g) avizează programele de prevenire a scurgerii informaţiilor clasificate din obiectivele industriale, anexele de securitate ale contractelor clasificate şi monitorizează respectarea prevederilor acestora;

h) efectuează controale de securitate şi informează ORNISS asupra concluziilor rezultate;

i) verifică şi prezintă ORNISS propuneri de soluţionare a sesizărilor, reclamaţiilor şi observaţiilor referitoare la modul de aplicare şi respectare a standardelor de protecţie în cadrul contractelor clasificate.

SECŢIUNEA a 3-a
Protecţia informaţiilor clasificate care fac obiectul activităţilor contractuale

ART. 201

(1) Clauzele şi procedurile de protecţie vor fi stipulate în anexa de securitate a fiecărui contract clasificat, care presupune acces la informaţii clasificate.

(2) Anexa de securitate prevăzută la alin. (1) va fi întocmită de partea contractantă deţinătoare de informaţii clasificate ce vor fi utilizate în derularea contractului clasificat.

(3) Clauzele şi procedurile de protecţie vor fi supuse, periodic, inspecţiilor şi verificărilor de către autoritatea desemnată de securitate competentă.

ART. 202

Partea contractantă deţinătoare de informaţii clasificate ce vor fi utilizate în derularea unui contract este responsabilă pentru clasificarea şi definirea tuturor componentelor

acestuia, în conformitate cu normele în vigoare, sens în care poate solicita sprijin de la ADS, conform competenţelor materiale stabilite prin lege.

ART. 203

La clasificarea contractelor se vor aplica următoarele reguli generale:

a) în toate stadiile de planificare şi execuţie, contractul se clasifica pe niveluri corespunzătoare, în functie de conţinutul informaţiilor;

b) clasificările se aplică numai acelor părţi ale contractului care trebuie protejate;

c) când în derularea unui contract se folosesc informaţii din mai multe surse, cu niveluri de clasificare diferite, contractul va fi clasificat în funcţie de nivelul cel mai înalt al informaţiilor, iar măsurile de protecţie vor fi stabilite în mod corespunzător;

d) declasificarea sau trecerea la o altă clasă sau nivel de secretizare a unei informaţii din cadrul contractului se aprobă de conducătorul persoanei juridice care a autorizat clasificarea iniţială.

ART. 204

În cazul în care apare necesitatea protejării informaţiilor dintr-un contract care, anterior, nu a fost necesar a fi clasificat, contractorul are obligaţia declanşării procedurilor de clasificare şi protejare conform reglementărilor în vigoare.

ART. 205

În cazul în care contractantul cedează unui subcontractant realizarea unei părţi din contractul clasificat, se va asigura că acesta deţine autorizaţie sau certificat de securitate industrială şi este obligat sa înştiinţeze contractorul, iar la încheierea subcontractului să prevadă clauze şi proceduri de protecţie în conformitate cu prevederile prezentelor standarde.

ART. 206

(1) În procesul de negociere a unui contract clasificat pot participa doar reprezentanţi autorizaţi ai obiectivelor industriale care deţin autorizaţie de securitate industrială eliberată de către ORNISS, care va ţine evidenţa acestora.

(2) Autorizaţiile de securitate industrială se eliberează pentru fiecare contract clasificat în parte.

(3) În cazul în care obiectivul industrial nu deţine autorizaţii de securitate industrială pentru participarea la negocierea acelui contract, este obligatorie iniţierea procedurii de autorizare.

ART. 207

(1) Invitaţiile la licitaţii sau prezentări de oferte, în cazul contractelor clasificate, trebuie să conţină o clauză prin care potenţialul ofertant este obligat sa înapoieze documentele clasificate care i-au fost puse la dispoziţie, în cazul în care nu depune oferta până la data stabilită sau nu câştigă competiţia într-un termen precizat de organizator, care să nu depăşească 15 zile de la comunicarea rezultatului.

(2) În situaţiile menţionate la alin. (1), ofertantul care a pierdut licitaţia are obligaţia să păstreze confidenţialitatea informaţiilor la care a avut acces.

ART. 208

Contractorul păstrează evidenţa tuturor participanţilor la întâlnirile de negociere, datele de identificare ale acestora şi angajamentele de confidenţialitate, organizaţiile pe care le reprezintă, tipul şi scopul întâlnirilor, precum şi informaţiile la care aceştia au avut acces.

ART. 209

Contractanţii care intenţionează să deruleze activităţi industriale cu subcontractanţi sunt obligaţi să respecte procedurile prevăzute în acest capitol.

ART. 210

Contractantul şi subcontractanţii sunt obligaţi să implementeze şi să respecte toate măsurile de protecţie a informaţiilor clasificate puse la dispoziţie sau care au fost generate pe timpul derulării contractelor.

ART. 211

Autorităţile desemnate de securitate vor verifica, potrivit competenţelor, dacă obiectivul industrial îndeplineşte următoarele cerinţe:

a) posedă structura/funcţionar de securitate responsabilă cu protecţia informaţiilor clasificate care fac obiectul activităţilor contractuale;

b) asigură sprijinul necesar pentru efectuarea inspecţiilor de securitate periodice, pe întreaga durată a contractului clasificat;

c) nu permite diseminarea, fără autorizaţie scrisă din partea emitentului, a nici unei informaţii clasificate ce i-a fost încredinţată în cadrul derulării unui contract clasificat;

d) aprobă accesul la informaţiile vehiculate în cadrul contractului clasificat numai persoanelor care deţin certificat de securitate sau autorizaţie de acces, în conformitate cu principiul necesităţii de a cunoaşte;

e) dispune de posibilităţile necesare pentru a informa asupra oricărei compromiteri, divulgări, distrugeri, sustrageri, sabotaje sau activităţi subversive ori altor riscuri la adresa securităţii informaţiilor clasificate vehiculate sau a persoanelor angajate în derularea contractului respectiv şi orice schimbări privind proprietatea, controlul sau managementul obiectivului industrial cu implicaţii asupra statutului de securitate al acestuia;

f) impune subcontractanţilor obligaţii de securitate similare cu cele aplicate contractantului;

g) nu utilizează în alte scopuri decât cele specifice contractului informaţiile clasificate la care are acces, fără permisiunea scrisă a emitentului;

h) înapoiază toate informaţiile clasificate ce i-au fost încredinţate, precum şi pe cele generate pe timpul derulării contractului, cu excepţia cazului în care asemenea informaţii 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 protecţia informaţiilor clasificate legate de contract.

ART. 212

După adjudecarea contractului clasificat, contractantul are obligaţia de a informa ORNISS, în vederea iniţierii procedurii de obţinere a certificatului de securitate industrială.

ART. 213

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

a) ORNISS a emis certificatul de securitate industrială;

b) au fost eliberate certificate de securitate sau autorizaţii de acces pentru persoanele care, în îndeplinirea sarcinilor ce le revin, necesită acces la informaţii secrete de stat;

c) personalul autorizat al contractantului a fost instruit asupra reglementărilor de securitate industrială de către structura/funcţionarul de securitate şi a semnat fişa individuală de pregătire.

SECŢIUNEA a 4-a
Procedura de verificare, avizare şi certificare a obiectivelor industriale care negociază şi derulează contracte clasificate

ART. 214

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

ART. 215

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

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

(3) Evidenţa autorizaţiilor 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 şi 27 şi a copiei anexei de securitate menţionată la art. 201.

(3) ORNISS va tine evidenţa certificatelor de securitate industrială potrivit anexei nr. 32.

ART. 217

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

a) prevenirea accesului persoanelor neautorizate la informaţii clasificate;

b) garantarea că informaţiile clasificate sunt distribuite pe baza existenţei certificatului de securitate industrială şi a principiului necesităţii de a cunoaşte;

c) identificarea persoanelor care, prin acţiunile lor, pot pune în pericol protecţia informaţiilor clasificate şi interzicerea accesului acestora la astfel de informaţii;

d) garantarea faptului că obiectivele industriale au capacitatea de a proteja informaţiile clasificate în procesul de negociere, respectiv de derulare a contractului.

ART. 218

(1) Pentru a i se elibera autorizaţia şi certificatul de securitate, obiectivul industrial trebuie să îndeplinească următoarele cerinţe:

a) să posede program de prevenire a scurgerii de informaţii clasificate, avizat conform reglementărilor în vigoare;

b) să fie stabil din punct de vedere economic;

c) să nu fi înregistrat o greşeală de management cu implicaţii grave asupra stării de securitate a informaţiilor clasificate pe care le gestionează;

d) să fi respectat obligaţiile de securitate din cadrul contractelor clasificate derulate anterior;

e) personalul implicat în derularea contractului să deţină certificat de securitate de nivel egal celui al informaţiilor vehiculate în cadrul contractului clasificat.

(2) Neîndeplinirea cerinţelor menţionate la alin. (1), precum şi furnizarea intenţionată a unor informaţii inexacte în completarea chestionarului sau în documentele prezentate în vederea certificării constituie elemente de incompatibilitate în procesul de eliberare a autorizaţiei 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 îşi îndeplineşte obligaţiile financiare către stat;

e) nu şi-a îndeplinit la timp, în mod sistematic, obligaţiile financiare către persoane fizice sau juridice.

ART. 220

(1) Un obiectiv industrial nu corespunde din punct de vedere al protecţiei informaţiilor clasificate dacă se constată că prezintă riscuri de securitate.

(2) Sunt considerate riscuri de securitate:

a) derularea unor activităţi ce contravin intereselor de siguranţă naţională sau angajamentelor pe care România şi le-a asumat în cadrul acordurilor bilaterale sau multinaţionale;

b) relaţiile cu persoane fizice sau juridice străine ce ar putea aduce prejudicii intereselor statului român;

c) asociaţiile, persoane fizice şi juridice, care pot reprezenta factori de risc pentru interesele de stat ale României.

ART. 221

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

a) cererea de eliberare a autorizaţiei, respectiv a certificatului de securitate industrială;

b) chestionarul de securitate completat, introdus într-un plic separat, sigilat.

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

ART. 222

În termen de 7 zile lucrătoare de la primirea cererii, ORNISS va solicita autorităţii 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 şi normele privind accesul persoanelor la informaţii clasificate;

c) obiectivul industrial este solvabil din punct de vedere financiar;

d) obiectivul industrial nu a fost şi nu este implicat sub nici o formă în activitatea unor organizaţii, asociaţii, mişcări, grupări de persoane străine sau autohtone care au adoptat sau adoptă o politică de sprijinire sau aprobare a comiterii de acte de sabotaj, subversive au teroriste.

ART. 224

Verificările de securitate se realizează astfel:

a) verificarea de securitate de nivel I - pentru eliberarea avizului necesar autorizaţiei 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 importanţă deosebită.

ART. 225

În cadrul verificării de securitate se desfăşoară următoarele activităţi:

(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 scurgerii de informaţii clasificate;

c) evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociaţi/acţionari, administratori, persoanele din comitetul director şi structura de securitate - ori executiva implicată în negocierea contractului clasificat;

d) verificarea datelor minime referitoare la bonitatea şi stabilitatea economică a obiectivului industrial - domeniu şi obiect de activitate, statut juridic, acţionari, garanţii bancare.

(2) Pentru verificările de securitate de nivel II:

a) verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială - anexa nr. 26;

b) evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociaţi/acţionari, administratori, persoanele din comitetul director şi structura de securitate - ori executivă implicată în derularea contractului clasificat;

c) verificarea unor date minime referitoare la bonitatea şi stabilitatea economică a obiectivului industrial - domeniu şi obiect de activitate, statut juridic, acţionari, garanţii bancare;

d) verificarea modului de implementare şi de aplicare a normelor şi măsurilor de securitate fizică, de securitate a personalului şi 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 - asociaţi/acţionari, administratori, persoanele din comitetul director şi structura de securitate - ori executivă implicată în derularea contractului clasificat, precum şi a celor desemnate să participe la activităţile de negociere a acestuia;

c) verificarea datelor referitoare la bonitatea şi stabilitatea economică a agentului economic - domeniu şi obiect de activitate, statut juridic, acţionari, garanţii bancare - incluzând şi aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;

d) verificarea existenţei autorizării sistemului informatic şi de comunicaţii propriu, pentru nivelul strict secret;

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

f) discuţii cu proprietarii, membrii consiliului director, funcţionarii de securitate, angajaţii, 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 - asociaţi/acţionari, administratori, persoanele din comitetul director şi structura de securitate - ori executivă implicată în derularea contractului clasificat;

c) verificarea informaţiilor detaliate referitoare la bonitatea şi stabilitatea economică a agentului economic - domeniu şi obiect de activitate, statut juridic, acţionari, garanţii bancare - incluzând şi aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;

d) verificarea existenţei autorizării sistemului informatic şi de comunicaţii propriu, pentru nivel strict secret de importanţă deosebită;

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

f) discuţii cu proprietarii, membrii consiliului director, funcţionarii de securitate, angajaţii, în vederea clarificării datelor rezultate din chestionar, după caz.

ART. 226

În cazul unui obiectiv industrial la al cărui management/acţionariat participă cetăţeni străini, cetăţeni români care au şi cetăţenia altui stat sau/şi persoane apatride, ORNISS, împreună cu ADS competentă, va evalua măsura în care interesul strain ar putea reprezenta o ameninţare la adresa protecţiei informaţiilor secrete de stat, care vor fi încredinţate acelui obiectiv industrial.

ART. 227

În indeplinirea sarcinilor şi obiectivelor ce le revin, pe linia protecţiei informaţiilor clasificate, ADS competente cooperează pe baza protocoalelor ce vor fi încheiate între ele cu avizul ORNISS.

ART. 228

În vederea desfăşurării procedurilor de avizare, obiectivul industrial are obligaţia de a permite accesul reprezentanţilor ADS în sediile, la echipamentele, operaţiunile şi la alte activităţi, respectiv de a prezenta documentele necesare şi de a furniza, la cerere, alte date şi informaţii.

ART. 229

(1) Dacă în urma verificării de securitate se constată că sunt îndeplinite cerinţele de securitate necesare asigurării protecţiei la nivelul de clasificare corespunzător informaţiilor vehiculate în cadrul contractului clasificat, ORNISS eliberează şi transmite obiectivului industrial autorizaţia sau certificatul de securitate industrială.

(2) Dacă se constată că obiectivul industrial nu îndeplineşte condiţiile de securitate necesare, ORNISS nu eliberează autorizaţia sau certificatul de securitate industrială şi informează obiectivul industrial în acest sens. ORNISS nu este obligat să prezinte motivele

refuzului. Refuzul eliberării autorizaţiei sau certificatului de securitate industrială va fi comunicat şi 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 securităţii, în luarea deciziei de eliberare a autorizaţiei 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 autorităţilor desemnate de securitate, ORNISS va elibera autorizaţia sau certificatul de securitate industrială ori, după caz, va comunica obiectivului industrial refuzul eliberării acestora.

ART. 231

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

ART. 232

Termenele pentru eliberarea autorizaţiei sau certificatului de securitate industrială sunt:

a) pentru autorizaţia 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 importanţă deosebită - 180 de zile lucrătoare.

ART. 233

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

(2) Dacă în perioada menţionată 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 situaţia în care ORNISS decide retragerea autorizaţiei sau certificatului de securitate industrială va înştiinţa contractantul, contractorul şi autoritatea desemnată de securitate competentă.

ART. 235

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

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

CAPITOLUL VIII
Protecţia surselor generatoare de informaţii - infosec

SECŢIUNEA 1
Dispoziţii generale

ART. 236

Modalităţile şi măsurile de protecţie a informaţiilor clasificate care se prezintă în format electronic sunt similare celor pe suport de hârtie.

ART. 237

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

- INFOSEC - ansamblul măsurilor şi structurilor de protecţie a informaţiilor clasificate care sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatice de comunicaţii şi al altor sisteme electronice, împotriva ameninţărilor şi a oricăror acţiuni care pot aduce atingere confidenţialităţii, integrităţii, disponibilităţii autenticităţii şi nerepudierii informaţiilor clasificate precum şi afectarea funcţionării sistemelor informatice, indiferent dacă acestea apar accidental sau intenţionat. Măsurile INFOSEC acoperă securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografică, precum şi depistarea şi prevenirea ameninţărilor la care sunt expuse informaţiile şi sistemele;

– informaţiile în format electronic - texte, date, imagini, sunete, înregistrate pe dispozitive de stocare sau pe suporturi magnetice, optice, electrice ori transmise sub formă de curenţi, tensiuni sau câmp electromagnetic, în eter sau în reţele de comunicaţii;

– sistemul de prelucrare automată a datelor - SPAD - ansamblul de elemente interdependente în care se includ: echipamentele de calcul, produsele software de bază şi aplicative, metodele, procedeele şi, dacă este cazul, personalul, organizate astfel încât să asigure îndeplinirea funcţiilor de stocare, prelucrare automată şi transmitere a informaţiilor în format electronic, şi care se află sub coordonarea şi controlul unei singure autorităţi. Un SPAD poate să cuprindă subsisteme, iar unele dintre acestea pot fi ele insele SPAD;

– componentele specifice de securitate ale unui SPAD, necesare asigurării unui nivel corespunzător de protecţie pentru informaţiile clasificate care urmează a fi stocate sau procesate într-un SPAD, sunt:

– funcţii şi caracteristici hardware/firmware/software;

– proceduri de operare şi moduri de operare;

– proceduri de evidenţă;
– controlul accesului;
– definirea zonei de operare a SPAD;
– definirea zonei de operare a posturilor de lucru/a terminalelor la distanţă;
– restricţii impuse de politica de management;
– structuri fizice şi dispozitive;
– mijloace de control pentru personal şi comunicaţii;
– reţele de transmisii de date - RTD - ansamblul de elemente interdependente în care se includ: echipamente, programe şi dispozitive de comunicaţie, tehnică de calcul hardware şi software, metode şi proceduri pentru transmisie şi recepţie de date şi controlul reţelei, precum şi, dacă este cazul, personalul aferent. Toate acestea sunt organizate astfel încât să asigure îndeplinirea funcţiilor de transmisie a informaţiilor 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 comunicaţii; mai multe RTD pot utiliza serviciile unuia şi aceluiaşi sistem de comunicaţii.

Caracteristicile de securitate ale unei RTD cuprind: caracteristicile de securitate ale sistemelor SPAD individuale conectate, împreună cu toate componentele şi facilitatile asociate retelei - facilităţi de comunicatii ale retelei, mecanisme şi proceduri de identificare şi etichetare, controlul accesului, programe şi proceduri de control şi revizie - necesare pentru a asigura un nivel corespunzător de protecţie pentru informaţiile clasificate, care sunt transmise prin intermediul RTD;

- RTD locală - reţea de transmisii de date care interconectează mai multe computere sau echipamente de reţea, situate în acelaşi perimetru;

– sistemul informatic şi de comunicaţii - SIC - ansamblu informatic prin intermediul căruia se stochează, se procesează şi se transmit informaţii în format electronic, alcătuit din cel puţin un SPAD, izolat sau conectat la o RTD. Poate avea o configuraţie complexă, formată din mai multe SPAD-uri şi/sau RTD-uri interconectate;

– securitatea SPAD, RTD şi SIC - aplicarea măsurilor de securitate la SPAD şi RTD - SIC cu scopul de a preveni sau împiedica extragerea sau modificarea informaţiilor clasificate stocate, procesate, transmise prin intermediul acestora - prin interceptare, alterare, distrugere, accesare neautorizată cu mijloace electronice, precum şi invalidarea de servicii sau funcţii, prin mijloace specifice;

– confidenţialitatea - asigurarea accesului la informaţii clasificate numai pe baza certificatului de securitate al persoanei, în acord cu nivelul de secretizare a informaţiei accesate şi a permisiunii rezultate din aplicarea principiului nevoii de a cunoaşte;

– integritatea - interdicţia modificării - prin ştergere sau adăugare - ori a distrugerii în mod neautorizat a informaţiilor clasificate;

– disponibilitatea asigurarea condiţiilor necesare regăsirii şi folosirii cu uşurinţă, ori de câte ori este nevoie, cu respectarea strictă a condiţiilor de confidenţialitate şi integritate a informaţiilor clasificate;

– autenticitatea - asigurarea posibilităţii de verificare a identităţii pe care un utilizator de SPAD sau RTD pretinde că o are;

– nerepudierea - măsura prin care se asigură faptul că, după emiterea/recepţionarea unei informaţii într-un sistem de comunicaţii securizat, expeditorul/destinatarul nu poate nega, în mod fals, că a expediat/primit informaţii;

– risc de securitate - probabilitatea ca o ameninţare sau o vulnerabilitate ale SPAD sau RTD - SIC să se materializeze în mod efectiv;

– managementul de risc - are ca scop identificarea, controlul şi minimizarea riscurilor de securitate şi este o activitate continuă de stabilire şi menţinere a unui nivel de securitate în domeniul tehnologiei informaţiei şi comunicaţiilor - TIC - într-o unitate, în sensul că, pornind de la analiza de risc, identifică şi evaluează ameninţările şi vulnerabilităţile şi propune aplicarea măsurilor adecvate de contracarare, proiectate la un preţ de cost corelat cu consecinţele care ar decurge din divulgarea, modificarea sau ştergerea informaţiilor care trebuie protejate;

– regula celor doi - obligativitatea colaborării a două persoane pentru îndeplinirea unei activităţi specifice;

– produs informatic de securitate - componenta de securitate care se incorporeaza într-un SPAD sau RTD - SIC şi care serveşte la sporirea sau asigurarea confidenţialităţii, integrităţii, disponibilităţii, autenticităţii şi nerepudierii informaţiilor stocate, procesate sau transmise;

– securitatea calculatoarelor - COMPUSEC - aplicarea la nivelul fiecărui calculator a facilităţilor de securitate hardware, software şi firmware, pentru a preveni divulgarea, manevrarea, modificarea sau ştergerea neautorizată a informaţiilor clasificate ori invalidarea neautorizată a unor funcţii;

– securitatea comunicaţiilor - COMSEC - aplicarea măsurilor de securitate în telecomunicaţii, cu scopul de a proteja mesajele dintr-un sistem de telecomunicaţii, care ar putea fi interceptate, studiate, analizate şi, prin reconstituire, pot conduce la dezvăluiri de informaţii clasificate.

COMSEC reprezintă ansamblul de proceduri, incluzând :

a) măsuri de securitate a transmisiilor;

b) măsuri de securitate împotriva radiaţiilor - TEMPEST;

c) măsuri de acoperire criptologică;

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

e) măsuri COMPUSEC;

- TEMPEST - ansamblul măsurilor de testare şi de realizare a securităţii împotriva scurgerii de informaţii, prin intermediul emisiilor electromagnetice parazite;

– evaluarea - examinarea detaliată, din punct de vedere tehnic şi funcţional, a aspectelor de securitate ale SPAD şi RTD - SIC sau a produselor de securitate, de către o autoritate abilitată în acest sens.

Prin procesul de evaluare se verifică:

a) prezenţa facilităţilor/funcţiilor de securitate cerute;

b) absenţa efectelor secundare compromiţătoare care ar putea decurge din implementarea facilităţilor de securitate;

c) funcţionalitatea globală a sistemului de securitate;

d) satisfacerea cerinţelor de securitate specifice pentru un SPAD şi RTD - SIC;

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

f) existenţa performanţelor de securitate ale produselor informatice de securitate instalate în SPAD sau RTD-SIC;

- certificarea - emiterea unui document de constatare, la care se ataşează unul de analiză, în care sunt prezentate modul în care a decurs evaluarea şi rezultatele acesteia, în documentul de constatare se menţionează măsurile în care SPAD şi RTD - SIC satisfac cerinţele de securitate, precum şi măsura în care produsele informatice de securitate răspund exigenţelor referitoare la protecţia informaţiilor clasificate în format electronic;

– acreditarea - etapa de acordare a autorizării şi aprobării unui SPAD sau RTD - SIC de a prelucra informaţii clasificate, în spaţiul/mediul operaţional propriu.

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

a) nota justificativă despre obiectivul acreditării sistemului, nivelul/nivelurile de clasificare a informaţiilor care urmează să fie procesate şi vehiculate; modul/modurile de operare protejată propuse;

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

c) o descriere detaliată a facilităţilor de securitate şi a procedurilor propuse, destinate SPAD sau RTD - SIC. Această descriere va reprezenta elementul esenţial pentru finalizarea procesului de acreditare;

d) planul de implementare şi întreţinere a caracteristicilor de securitate;

e) planul de desfăşurare a etapelor de testare, evaluare şi certificare a securităţii SPAD sau RTD - SIC;

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

- zona SPAD - reprezintă o zonă de lucru în care se gasesc şi operează unul sau mai multe calculatoare, unităţi periferice locale şi de stocare, mijloace de control şi echipament specific de reţea şi de comunicaţii. Zona SPAD nu include zona în care sunt amplasate terminale, echipamente periferice sau staţii de lucru la distanţă, chiar dacă aceste echipamente sunt conectate la echipamentul central de calcul din zona SPAD;

– zonă terminal/staţie de lucru la distanţă - reprezintă o zonă, separată de zona SPAD, în care se găsesc :

a) elemente de tehnică de calcul;

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

c) echipamente de comunicaţii;

- ameninţarea - posibilitatea de compromitere accidentală sau deliberată a securităţii SPAD sau RTD -SIC, prin pierderea confidenţialităţii, a integrităţii sau disponibilităţii

informaţiilor în format electronic sau prin afectarea funcţiilor care asigură autenticitatea şi nerepudierea informaţiilor;

– vulnerabilitatea - slăbiciune sau lipsă de control care ar putea permite sau facilita o manevră tehnică, procedurală sau operaţională, prin care se ameninţă o valoare sau ţintă specifică.

ART. 238

Abrevierile utilizate în prezentul capitol semnifică:

a) CSTIC - componenta de securitate pentru tehnologia informaţiei şi comunicaţiilor instituită în unităţile deţinătoare de informaţii clasificate;

b) TIC - tehnologia informaţiei şi comunicaţiilor;

c) CSS - cerinţele de securitate specifice.

ART. 239

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

a) stocate şi procesate în cadrul SPAD sau transmise prin intermediul RTD;

b) stocate şi transportate prin intermediul suporturilor de memorie, dispozitivelor electronice - cipuri de memorie, hârtie perforată sau alte suporturi specifice.

(2) Încărcarea informaţiilor pe mediile prevăzute în alin. (1) lit. b, precum şi interpretarea lor pentru a deveni inteligibile, se face cu ajutorul echipamentelor electronice specializate.

ART. 240

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

(2) În vederea autorizării SPAD şi RTD - SIC unităţile 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 informaţiei şi comunicaţiilor, personal instruit şi măsuri de protecţie a informaţiei, incluzând controlul accesului la sistemele şi serviciile informatice şi de comunicatii, pe baza principiului necesităţii de a cunoaşte şi al nivelului de secretizare atribuit.

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

ART. 241

(1) Aplicarea reglementărilor în vigoare referitoare la protecţia informaţiilor clasificate în format electronic funcţionează unitar la nivel naţional. Sistemul de emitere şi implementare a măsurilor de securitate adresate protecţiei informaţiilor clasificate care sunt stocate, procesate sau transmise de SPAD sau RTD - SIC, precum şi controlul modului de implementare a măsurilor de securitate se realizează de către o structură funcţională cu atribuţii de reglementare, control şi autorizare, care include:

a) o agenţie pentru acordarea acreditării de funcţionare în regim de securitate;

b) o agenţie care elaborează şi implementează metode, mijloace şi măsuri de securitate;

c) o agenţie responsabilă cu protecţia criptografică.

(2) Agenţiile menţionate la alin. (1) sunt subordonate instituţiei desemnate la nivel naţional, pentru protecţia informaţiilor clasificate, ORNISS.

(3) Măsurile de protecţie a informaţiilor clasificate în format electronic trebuie reactualizate permanent, prin depistare, documentare şi gestionare a ameninţărilor şi vulnerabilităţilor la adresa informaţiilor clasificate şi sistemelor care le prelucrează, stochează şi transmit.

ART. 242

Măsurile de securitate INFOSEC vor fi structurate după nivelul de clasificare al informaţiilor pe care le protejează şi în conformitate cu conţinutul acestora.

ART. 243

Conducatorul unităţii deţinătoare de informaţii clasificate răspunde de securitatea propriilor informaţii care sunt stocate, procesate sau transmise în SPAD sau RTD - SIC.

ART. 244

(1) În fiecare unitate care administrează SPAD şi RTD - SIC în care se stochează, se procesează sau se transmit informaţii clasificate, se va institui o componentă de securitate pentru tehnologia informaţiei şi a comunicaţiilor - CSTIC, în subordinea structurii/funcţionarului de securitate.

(2) În funcţie de volumul de activitate şi dacă cerinţele de securitate permit, atribuţiile CSTIC pot fi îndeplinite numai de către funcţionarul de securitate TIC sau pot fi preluate, în totalitate, de către structura/funcţionarul de securitate din unitate.

(3) CSTIC îndeplineşte atribuţii privind:

a) implementarea metodelor, mijloacelor şi măsurilor necesare protecţiei informaţiilor în format electronic;

b) exploatarea operaţonală a SPAD şi RTD - SIC în condiţii de securitate;

c) coordonarea cooperării dintre unitatea deţinătoare a SPAD sau RTD - SIC şi autoritatea care asigură acreditarea;

d) implementarea măsurilor de securitate şi protecţia criptografică ale SPAD sau RTD - SIC.

(4) CSTIC reprezintă punctul de contact al agenţiilor competente cu unităţile care deţin în administrare SPAD sau RTD - SIC şi, după caz, poate fi investită, temporar, de către aceste agenţii, cu unele dintre atribuţiile lor.

(5) Propunerile pe linie de securitate avansate de către CSTIC devin operaţionale numai după ce au fost aprobate de către conducerea unităţii care deţine în administrare respectivul SPAD sau RTD - SIC.

ART. 245

CSTIC se instituie la nivelul fiecărei SPAD şi RTD - SIC şi reprezintă persoana sau compartimentul cu responsabilitatea delegată de către agenţia de securitate pentru informatică şi comunicaţii de a implementa metodele, mijloacele şi măsurile de securitate şi de a exploata SPAD şi RTD - SIC în condiţii de securitate.

ART. 246

CSTIC este condusă de către funcţionarul de securitate TIC şi are în compunere administratorii de securitate şi, după caz, şi alti specialişti din SPAD sau RTD - SIC. Toata structura CSTIC face parte din personalul unităţii care administrează SPAD sau RTD - SIC.

ART. 247

Exercitarea atribuţiilor CSTIC trebuie să cuprindă întregul ciclu de viaţă al SPAD sau RTD - SIC, începând cu proiectarea, continuând cu elaborarea specificaţiilor, testarea instalării, acreditarea, testarea periodică în vederea reacreditării, exploatarea operaţională, modificarea şi încheind cu scoaterea din uz. În anumite situaţii, rolul CSTIC poate fi preluat de către alte componente ale unităţii, în decursul ciclului de viaţă.

ART. 248

CSTIC mijloceşte cooperarea dintre conducerea unităţii căreia îi aparţine SPAD sau RTD - SIC şi agenţia pentru acreditare de securitate, atunci când unitatea:

a) planifică dezvoltarea sau achiziţia de SPAD sau RTD;

b) propune schimbări ale unei configuraţii 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 securităţii SPAD sau RTD - SIC;

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

g) planifică sau propune intreprinderea oricărei alte activităţi referitoare la îmbunătăţirea securităţii SPAD sau RTD - SIC deja acreditate.

ART. 249

CSTIC, cu aprobarea autorităţii de acreditare de securitate, stabilesşte standardele şi procedurile de securitate care trebuie respectate de către furnizorii de echipamente, pe parcursul dezvoltării, instalarii şi testării SPAD şi RTD - SIC şi răspunde pentru justificarea, selecţia, implementarea şi controlul componentelor de securitate, care constituie parte a SPAD şi RTD - SIC.

ART. 250

CSTIC stabileşte, pentru structurile de securitate şi management ale SPAD şi RTD - SIC, încă de la înfiinţare, responsabilităţile pe care le vor exercita pe tot ciclul de viaţă al SPAD şi RTD - SIC respective.

ART. 251

Activitatea INFOSEC din SPAD şi RTD - SIC, desfăşurată de către CSTIC, trebuie condusă şi coordonată de persoane care deţin certificat de securitate corespunzător, cu pregătire de specialitate în domeniul sistemelor TIC precum şi al securităţii acestora,

obtinută în instituţii de învăţământ acreditate INFOSEC, sau care au lucrat în domeniu cel puţin 5 ani.

ART. 252

Protecţia SPAD şi RTD - SIC din compunerea sistemelor de armament şi de detecţie va fi definită în contextul general al sistemelor din care acestea fac parte şi va fi realizata prin aplicarea prevederilor prezentelor standarde.

SECŢIUNEA a 2-a
Structuri organizatorice cu atribuţii specifice în domeniul INFOSEC

A. Agenţia de acreditare de securitate

ART. 253

Agenţia de acreditare de securitate este subordonată instituţiei desemnate la nivel naţional pentru protecţia informaţiilor clasificate, are reprezentanţi delegaţi din cadrul ADS implicate, în funcţie de SPAD şi RTD - SIC care trebuie acreditate, şi îndeplineşte următoarele atribuţii principale:

a) asigură, la nivel naţional, acreditarea de securitate şi reacreditarea SPAD şi RTD - SIC care stochează, procesează sau transmit informaţii clasificate, în funcţie de nivelul de clasificare a acestora;

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

c) stabileşte criteriile de acreditare de securitate pentru SPAD şi RTD - SIC.

ART. 254

Agenţia de acreditare de securitate îşi exercită atribuţiile în domeniul INFOSEC în numele instituţiei desemnate la nivel naţional pentru protecţia informaţiilor clasificate şi are responsabilitatea de a impune standarde de securitate în acest domeniu.

B. Agenţia de securitate pentru informatică şi comunicaţii

ART. 255

Agenţia de securitate pentru informatică şi comunicaţii este structura subordonată instituţiei desemnate la nivel naţional pentru protecţia informaţiilor electronice clasificate, având reprezentanţi delegaţi din cadrul ADS implicate care acţionează la nivel naţional.

ART. 256

Agentia este responsabilă de conceperea şi implementarea mijloacelor, metodelor şi masurilor de protecţie a informaţiilor clasificate care sunt stocate, procesate sau transmise prin intermediul SPAD şi RTD - SIC şi are, în principal, următoarele atribuţii:

a) coordonează activităţile de protecţie a informaţiilor clasificate care sunt stocate, procesate sau transmise prin intermediul SPAD şi RTD - SIC;

b) elaborează şi promovează reglementări şi standarde specifice;

c) analizeaza cauzele incidentelor de securitate şi gestionează baza de date privind ameninţările şi vulnerabilitatile din sistemele de comunicaţie şi informatice, necesare pentru elaborarea managementul de risc;

d) semnalează agenţiei de acreditare de securitate incidentele de securitate în domeniu;

e) integrează măsurile privind protecţia fizică, de personal, a documentelor administrative, COMPUSEC, COMSEC, TEMPEST şi criptografică;

f) execută inspecţii periodice asupra SPAD şi RTD - SIC în vederea reacreditării;

g) supune certificării şi autorizării sistemele de securitate specifice SPAD şi RTD - SIC.

ART. 257

Pentru îndeplinirea atribuţiilor sale, agenţia de securitate pentru informatică şi comunicaţii cooperează cu agenţia de acreditare de securitate, cu agenţia de protecţie criptografică şi cu alte structuri cu atribuţii în domeniu.

C. Agenţia de protecţie criptografică

ART. 258

Agentia de protecţie criptografica se organizeaza la nivel naţional, este subordonata institutiei desemnate la nivel naţional pentru protectia informaţiilor clasificate şi are urmatoarele atribuţii principale:

a) asigură managementul materialelor şi echipamentelor criptografice;

b) realizează distribuirea materialelor şi echipamentelor criptografice;

c) raportează instituţiei desemnate la nivel naţional pentru protectia informaţiilor clasificate incidentele de securitate cu care s-a confruntat;

d) cooperează cu agenţia de acreditare de securitate, cu agenţia de concepere şi implementare a metodelor, mijloacelor şi măsurilor de securitate şi cu alte structuri cu atribuţii în domeniu.

SECŢIUNEA a 3-a
Măsuri, cerinţe şi moduri de operare

A. Măsuri şi cerinţe specifice INFOSEC

ART. 259

(1) Măsurile de protecţie a informaţiilor clasificate în format electronic se aplică sistemelor SPAD şi RTD - SIC care stochează, procesează sau transmit asemenea informaţii.

(2) Unităţile deţinătoare de informaţii clasificate au obligaţia de a stabili şi implementa un ansamblu de măsuri de securitate a sistemelor SPAD şi RTD - SIC - fizice, de personal, administrative, de tip TEMPEST şi criptografic.

ART. 260

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

B. Cerinţe de securitate specifice SPAD şi RTD - SIC

ART. 261

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

(2) CSS se elaborează pentru fiecare SPAD şi RTD - SIC care stochează, procesează sau transmite informaţii clasificate, sunt stabilite de către CSTIC şi aprobate de către agenţia de acreditare de securitate.

ART. 262

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

ART. 263

CSS au la bază standardele naţionale de protecţie, parametrii esenţiali ai mediului operaţional, nivelul minim de autorizare a personalului, nivelul de clasificare a informaţiilor gestionate şi modul de operare a sistemului care urmează să fie acreditat.

C. Moduri de operare

ART. 264

SPAD şi RTD - SIC care stochează, procesează sau transmit informaţii clasificate vor fi certificate şi 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 informaţiilor stocate, procesate sau transmise prin aceste sisteme. Necesitatea de a cunoaşte pentru aceste persoane se stabileşte cu privire la toate informaţiile stocate, procesate sau transmise în cadrul SPAD sau RTD - SIC.

(2) În acest mod de operare, principiul necesităţii de a cunoaşte nu impune o separare a informaţiilor în cadrul SPAD sau RTD, ca mijloc de securitate a SIC. Celelalte măsuri de protecţie prevăzute vor asigura îndeplinirea cerinţelor impuse de cel mai înalt nivel de clasificare a informaţiilor gestionate şi de toate categoriile de informaţii cu destinaţie 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 informaţiilor stocate, procesate sau transmise în cadrul SPAD sau RTD - SIC, iar accesul la informaţii se va face diferenţiat, conform principiului necesităţii de a cunoaşte.

(2) Pentru a asigura accesul diferenţiat la informaţii, conform principiului necesităţii de a cunoaşte, se instituie facilităţi de securitate care să asigure un acces selectiv la informaţii în cadrul SPAD sau RTD - SIC.

(3) Celelalte măsuri de protecţie vor satisface cerinţele pentru cel mai înalt nivel de clasificare şi pentru toate categoriile de informaţii cu destinaţie specială stocate, procesate, transmise în cadrul SPAD sau RTD - SIC.

(4) Toate informaţiile stocate, procesate sau vehiculate în cadrul unui SPAD sau RTD - SIC în acest mod de operare vor fi protejate ca informaţii cu destinaţie specială, având cel mai înalt nivel de clasificare care a fost constatat în mulţimea informaţiilor stocate, procesate sau vehiculate prin sistem.

ART. 267

(1) În modul de operare multi-nivel, accesul la informaţiile clasificate se face diferenţiat, potrivit principiului necesităţii de a cunoaşte, conform următoarelor reguli:

a) nu toate persoanele cu drept de acces la SPAD sau RTD - SIC au certificat de securitate pentru acces la informaţii 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 RTD - SIC au acces la toate informaţiile stocate, procesate sau transmise prin aceste sisteme.

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

D. Administratorii de securitate

ART. 268

(1) Securitatea SPAD a reţelei şi a obiectivului SIC se asigură prin funcţiile de administrator de securitate.

(2) Administratorii de securitate sunt:

a) administratorul de securitate al SPAD;

b) administratorul de securitate al reţelei;

c) administratorul de securitate al obiectivului SIC.

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

ART. 269

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

(2) La recomandarea autorităţii de acreditare de securitate, CSTIC poate desemna structuri de administrare ale SPAD care îndeplinesc aceleaşi atribuţii.

ART. 270

Administratorul de securitate al reţelei este desemnat de CSTIC pentru un SIC de mari dimensiuni sau în cazul interconectării mai multor SPAD şi îndeplineşte atribuţii privind managementul securităţii comunicaţiilor.

ART. 271

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

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

(3) Obiectivul SIC reprezintă un amplasament specific sau un grup de amplasamente în care funcţionează un SPAD şi/sau RTD. Responsabilitatile şi măsurile de securitate pentru fiecare zonă de amplasare a unui terminal/staţie de lucru care funcţionează la distanţă trebuie explicit determinate.

E. Utilizatorii şi vizitatorii

ART. 272

(1) Toţi utilizatorii de SPAD sau RTD - SIC poartă responsabilitatea în ce priveşte securitatea acestor sisteme - raportate, în principal, la drepturile acordate şi sunt îndrumaţi de către administratorii de securitate.

(2) Utilizatorii vor fi autorizaţi pentru clasa şi nivelul de secretizare a informaţiilor clasificate stocate, procesate sau transmise în SPAD sau RTD - SIC. La acordarea accesului la informaţii, individual, se va urmări respectarea principiului necesităţii de a cunoaşte.

(3) Informarea şi conştientizarea 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 şi sa îndeplinească principiul necesităţii de a cunoaşte, în situaţia 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 informaţiile clasificate.

SECŢIUNEA a 4-a
Componentele INFOSEC

A. Securitatea personalului

ART. 274

(1) Utilizatorii SPAD şi RTD - SIC sunt autorizaţi şi li se permite accesul la informaţii clasificate pe baza principiului necesităţii de a cunoaşte şi în funcţie de nivelul de clasificare a informaţiilor stocate, procesate sau transmise prin aceste sisteme.

(2) Unităţile deţinătoare de informaţii clasificate în format electronic au obligaţia de a institui măsuri speciale pentru instruirea şi supravegherea personalului, inclusiv a personalului de proiectare de sistem care are acces la SPAD şi RTD, în vederea prevenirii şi înlăturării vulnerabilităţilor faţă de accesarea neautorizată.

ART. 275

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

ART. 276

Procedurile de lucru ale personalului din SPAD şi RTD - SIC trebuie să asigure separarea între operaţiunile de programare şi cele de exploatare a sistemului sau reţelei. Este interzis, cu excepţia unor situaţii speciale, ca personalul să facă atât programarea, cât şi operarea sistemelor sau reţelelor şi trebuie instituite proceduri speciale pentru depistarea acestor situaţii.

ART. 277

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

ART. 278

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

B. Securitatea fizică

ART. 279

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

ART. 280

În zonele în care sunt amplasate sisteme SPAD şi terminale la distanţă - staţii de lucru, unde se procesează şi/sau pot fi accesate informaţii clasificate, se aplică următoarele măsuri generale de securitate:

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

b) zonele şi locurile în care securitatea SPAD sau RID - SIC sau a terminalelor la distanţă poate fi modificată nu trebuie să fie niciodată ocupate de un singur angajat autorizat;

c) persoanelor care solicită acces temporar sau cu intermitenţe 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. Vizitatorii vor fi însoţiţi permanent, pentru a avea garanţia că nu pot avea acces la informaţii clasificate şi nici la echipamentele utilizate.

ART. 281

În funcţie de riscul de securitate şi de nivelul de secretizare al informaţiilor stocate, procesate şi transmise, se impune cerinţa de aplicare a regulii de lucru cu două persoane şi în alte zone, ce vor fi stabilite în stadiul iniţial al proiectului şi prezentate în cadrul CSS.

ART. 282

Când un SPAD este exploatat în mod autonom, deconectat în mod permanent de alte SPAD, ţinând cont de condiţiile specifice, de alte măsuri de securitate, tehnice sau procedurale şi de rolul pe care îl are respectivul SPAD în funcţionarea de ansamblu a sistemului, agenţia de acreditare de securitate trebuie să stabilească măsuri specifice de protecţie, adaptate la structura acestui SPAD, conform nivelului de clasificare a informaţiilor gestionate.

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

ART. 283

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

ART. 284

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

D. Securitatea informaţiilor clasificate în format electronic

ART. 285

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

ART. 286

Modul în care este prezentată informaţia în clar, chiar dacă se utilizează codul prescurtat de transmisie sau reprezentarea binară ori alte forme de transmitere la distanţă, nu trebuie să influenţeze nivelul de clasificare acordat informaţiilor respective.

ART. 287

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

ART. 288

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

ART. 289

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

ART. 290

Mediile refolosibile de stocare a informaţiilor utilizate pentru înregistrarea informaţiilor clasificate îşi menţin cea mai înaltă clasificare pentru care au fost utilizate anterior, până când respectivelor informaţii li se reduce nivelul de clasificare sau sunt declasificate, moment în care mediile susmenţionate se reclasifică în mod corespunzător sau sunt distruse în conformitate cu prevederile procedurilor operaţionale de securitate.

E. Controlul şi evidenţa informaţiilor în format electronic

ART. 291

(1) Evidenţa automată a accesului la informaţiile clasificate în format electronic se ţine în registrele de acces şi trebuie realizată necondiţionat prin software.

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

(3) Perioada minimă de păstrare a registrelor de acces la informaţiile strict secrete de importanţă deosebită este de 10 ani, iar a registrelor de acces la informaţiile strict secrete şi secrete, de cel puţin 3 ani.

ART. 292

(1) Mediile de stocare care conţin informaţii clasificate utilizate în interiorul unei zone SPAD pot fi manipulate ca unic material clasificat, cu condiţia ca materialul să fie identificat, marcat cu nivelul său de clasificare şi 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) Evidenţele acestora vor fi menţinute 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/staţie de lucru la distanţă, se stabilesc proceduri adecvate de securitate, aprobate de către agenţia de acreditare de securitate. Procedurile trebuie să cuprindă şi instrucţiuni specifice privind evidenţa informaţiilor în format electronic.

F. Manipularea şi controlul mediilor de stocare a informaţiilor clasificate în format electronic

ART. 294

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

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

(3) Identificarea şi controalele trebuie să asigure următoarele cerinţe:

a) Pentru nivelul secret:

- un mijloc de identificare - număr de serie şi 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;

– evidenţele manuale sau tipărite la imprimantă, indicând conţinutul şi nivelul de secretizare a informaţiilor înregistrate pe mediile de stocare.

b) Pentru nivelul strict secret şi strict secret de importanţă deosebită, informaţiile detaliate asupra mediului de stocare, incluzând conţinutul şi nivelul de clasificare, se ţin într-un registru adecvat.

ART. 295

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

a) pentru nivelul secret - controalele punctuale ale prezentei fizice şi continutului mediilor de stocare se efectueaza periodic, verificandu-se dacă acele medii de stocare nu conţin informaţii cu un nivel de clasificare superior;

b) pentru nivelul strict secret - toate mediile de stocare se inventariaza periodic, controland punctual prezenta lor fizica şi conţinutul, pentru a verifica dacă pe acele medii nu sunt stocate informaţii cu un nivel de clasificare superior;

c) pentru nivelul strict secret de importanţa deosebită, toate mediile se verifica periodic, cel puţin anual şi se controlează punctual, în legătură cu prezenta fizica şi conţinutul lor.

G. Declasificarea şi distrugerea mediilor de stocare a informaţiilor în format electronic

ART. 296

Informaţiile clasificate înregistrate pe medii de stocare refolosibile se şterg doar în conformitate cu procedurile operaţionale de securitate.

ART. 297

(1) Când un mediu de stocare urmează sa 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 şi refolosirea mediilor de stocare care conţin informaţii strict secrete de importanţă deosebită, acestea putând fi numai distruse, în conformitate cu procedurile operaţionale de securitate.

ART. 298

Informaţiile clasificate în format electronic stocate pe un mediu de unică folosinţă - cartele, benzi perforate - trebuie distruse conform prevederilor procedurilor operaţionale de securitate.

SECŢIUNEA a 5-a
Reguli generale de securitate TIC

A. Securitatea comunicaţiilor

ART. 299

Toate mijloacele folosite pentru transmiterea electromagnetică a informaţiilor clasificate se supun instrucţiunilor de securitate a comunicaţiilor emise de către instituţia desemnată la nivel naţional pentru protecţia informaţiilor clasificate.

ART. 300

Într-un SPAD - SIC trebuie să se dispună mijloace de interzicere a accesului la informaţiile clasificate de la toate terminalele/staţiile de lucru la distanţă, 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 şi faţă de emisiile electromagnetice

ART. 301

Instalarea iniţială a SPAD sau RTD - SIC sau orice modificare majoră adusă acestora vor fi executate de persoane autorizate, în condiţiile prezentelor standarde. Lucrările vor fi permanent supravegheate de personal tehnic calificat, care are acces la informaţii 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 şi RTD - SIC vor fi instalate în conformitate cu reglementările specifice în vigoare, emise de către instituţia desemnată la nivel naţional

pentru protecţia informaţiilor clasificate, cu directivele şi standardele tehnice corespunzătoare.

ART. 303

Sistemele SPAD şi RTD - SIC care stochează, procesează sau transmit informaţii secrete de stat vor fi protejate corespunzător faţă de vulnerabilităţile de securitate cauzate de radiaţiile compromiţătoare - TEMPEST.

C. Securitatea în timpul procesării informaţiilor clasificate

ART. 304

Procesarea informaţiilor se realizează în conformitate cu procedurile operaţionale de securitate, prevăzute în prezentele standarde.

ART. 305

Transmiterea informaţiilor secrete de stat către instalaţii automate - a căror funcţionare nu necesită prezenţa unui operator uman - este interzisă, cu excepţia cazului când se aplică reglementări speciale aprobate de către autoritatea de acreditare de securitate, iar acestea au fost specificate în procedurile operaţionale de securitate.

ART. 306

În SPAD sau RTD-SIC care au utilizatori - existenţi sau potenţiali - fără certificate de securitate emise conform prezentelor standarde nu se pot stoca, procesa sau transmite informaţii strict secrete de importanţă deosebită.

D. Procedurile operaţionale de securitate

ART. 307

Procedurile operaţionale de securitate reprezintă descrierea implementării strategiei de securitate ce urmează să fie adoptată, a procedurilor operaţionale de urmat şi a responsabilităţilor personalului.

ART. 308

Procedurile operaţionale de securitate sunt elaborate de către agenţia de concepere şi implementare a metodelor, mijloacelor şi măsurilor de securitate, în colaborare cu CSTIC, precum şi cu agenţia de acreditare de securitate, care are atribuţii de coordonare, şi alte autorităţi cu atribuţii în domeniu. Agenţia de acreditare de securitate va aproba procedurile de operare înainte de a autoriza stocarea, procesarea sau transmiterea informaţiilor secrete de stat prin SPAD - RTD - SIC.

E. Protecţia produselor software şi managementul configuraţiei

ART. 309

CSTIC are obligaţia să efectueze controale periodice, prin care să stabilească dacă toate produsele software originale - sisteme de operare generale, subsisteme şi pachete soft - aflate în folosinţă, sunt protejate în condiţii conforme cu nivelul de clasificare al informaţiilor pe care acestea trebuie să le proceseze. Protecţia programelor - software de

aplicaţie se stabileşte pe baza evaluării nivelului de secretizare a acestora, ţinând cont de nivelul de clasificare a informaţiilor pe care urmeaza să le proceseze.

ART. 310

(1) Este interzisă utilizarea de software neautorizat de către agenţia de acreditare de securitate.

(2) Conservarea exemplarelor originale, a copiilor - backup sau off-site, precum şi salvările periodice ale datelor obţinute din procesare vor fi executate în conformitate cu prevederile procedurilor operaţionale de securitate.

ART. 311

(1) Versiunile software care sunt în uz trebuie să fie verificate la intervale regulate, pentru a garanta integritatea şi funcţionarea lor corectă.

(2) Versiunile noi sau modificate ale software-ului nu vor fi folosite pentru procesarea informaţiilor secrete de stat, până când procedurile de securitate ale acestora nu sunt testate şi aprobate conform CSS.

(3) Un software care îmbunătăţeşte posibilităţile sistemului şi care nu are nici o procedură de securitate nu poate fi folosit înainte de a fi verificat de către CSTIC.

F. Verificări pentru depistarea virusilor de calculator şi a software-ului nociv

ART. 312

Verificarea prezenţei virusilor şi software-ului nociv se face în conformitate cu cerinţele impuse de către agenţia de acreditare de securitate.

ART. 313

(1) Versiunile de software noi sau modificate - sisteme de operare, subsisteme, pachete de software şi software de aplicaţie - 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 viruşilor 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 reţea publică de comunicaţii.

G. Întreţinerea tehnică a SPAD sau RTD - SIC

ART. 314

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

(2) Personalul de întreţinere trebuie să deţină certificate de securitate de nivel corespunzător nivelului de secretizare a informaţiilor 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 operaţionale de securitate.

ART. 316

Cerinţele menţionate la art. 314 trebuie stipulate în CSS, iar procedurile de desfăşurare a activităţii respective trebuie stabilite în procedurile operaţionale de securitate. Nu se acceptă tipurile de întreţinere care constau în aplicarea unor proceduri de diagnosticare ce implică accesul de la distanţă la sistem, decât dacă activitatea respectivă se desfăşoară sub control strict şi numai cu aprobarea agenţiei de acreditare de securitate.

H. Achiziţii

ART. 317

Sistemele SPAD sau RTD - SIC, precum şi componentele lor hardware şi software sunt achiziţionate de la furnizori interni sau externi selectaţi dintre cei agreaţi de către agenţia de acreditare de securitate.

ART. 318

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

ART. 319

SPAD sau RTD - SIC care stochează, procesează sau transmit informaţii secrete de stat sau componentele lor de bază - sisteme de operare de scop general, produse de limitare a funcţionării pentru realizarea securităţii şi produse pentru comunicare în reţea - se pot achiziţiona numai dacă au fost evaluate şi certificate de către agenţia de acreditare de securitate.

ART. 320

Pentru SPAD şi RTD - SIC care stochează, procesează sau transmit informaţii secrete de serviciu, sistemele şi 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 ţine cont ca astfel de echipamente, odată utilizate în SPAD sau RTD - SIC ce procesează, stochează sau transmit informaţii clasificate, vor fi supuse măsurilor de protecţie 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 şi RTD - SIC

ART. 322

(1) Toate SPAD şi RTD - SIC, înainte de a fi utilizate pentru stocarea, procesarea sau transmiterea informaţiilor clasificate, trebuie acreditate de către agenţia de acreditare de securitate, pe baza datelor furnizate de către CSS, procedurilor operaţionale de securitate şi altor documentaţii relevante.

(2) Subsistemele SPAD şi RTD - SIC şi staţiile de lucru cu acces la distanţă sau terminalele vor fi acreditate ca parte integrantă a sistemelor SPAD şi RTD - SIC la care sunt conectate, în cazul în care un sistem SPAD sau RTD - SIC deserveşte atât NATO, cât şi organizaţiile/structurile interne ale ţării, acreditarea se va face de către autoritatea naţională de securitate, cu consultarea ADS şi a agenţiilor INFOSEC, potrivit competenţelor.

J. Evaluarea şi certificarea

ART. 323

În situaţiile ce privesc modul de operare de securitate multi-nivel, înainte de acreditarea propriu-zisă a SPAD sau RTD - SIC, hardware-ul, firmware-ul şi software-ul vor fi evaluate şi certificate de către agenţia de acreditare de securitate, în acest sens, instituţia desemnată la nivel naţional pentru protecţia informaţiilor clasificate va stabili criterii diferenţiate pentru fiecare nivel de secretizare a informaţiilor vehiculate de SPAD sau RTD - SIC.

ART. 324

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

ART. 325

Următoarele situaţii impun evaluarea şi certificarea de securitate în modul de operare de securitate multi-nivel:

a) pentru SPAD sau RTD - SIC care stochează, procesează sau transmite informaţii clasificate strict secret de importanţă deosebită;

b) pentru SPAD sau RTD - SIC care stochează, procesează sau transmite informaţii clasificate strict secret, în cazurile în care:

- SPAD sau RTD - SIC este interconectat cu un alt SPAD sau RTD - SIC - de exemplu, aparţinând altui CSTIC;

– SPAD sau RTD - SIC are un număr de utilizatori posibili care nu poate fi definit exact.

ART. 326

Procesele de evaluare şi certificare trebuie să se desfăşoare, conform principiilor şi instrucţiunilor aprobate, de către echipe de expertizare cu pregătire tehnică adecvată şi autorizate corespunzător. Aceste echipe vor fi compuse din experţi selecţionati de către agenţia de acreditare de securitate.

ART. 327

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

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

K. Verificări de rutină pentru menţinerea acreditării

ART. 328

Pentru toate SPAD şi RTD - SIC care stochează, procesează sau transmit informaţii secrete de stat, CSTIC stabileşte 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 agenţiei de acreditare de securitate trebuie să fie identificate cu claritate şi 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 funcţionarea corectă a dispozitivelor de securitate.

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

ART. 330

(1) Toate SPAD şi RTD - SIC care stochează, procesează sau transmit informaţii secrete de stat sunt inspectate şi reexaminate periodic de către agenţia de acreditare de securitate.

(2) Pentru SPAD sau RTD - SIC care stochează, procesează sau transmit informaţii strict secrete de importanţă deosebită, inspecţia se va face cel puţin 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 informaţiei, ce operează autonom sau ca parte a unei reţele, precum şi calculatoarele portabile cu discuri fixe sunt considerate medii de stocare a informaţiilor, în acelaşi sens ca şi celelalte medii amovibile de stocare a informaţiilor.

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

ART. 332

Echipamentelor prevăzute la art. 331 trebuie să li se acorde nivelul de protecţie pentru acces, manipulare, stocare şi transport, corespunzător cu cel mai înalt nivel de clasificare a informaţiilor 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 şi a hardware-ului, aflate în proprietate privată, pentru stocarea, procesarea şi transmiterea informaţiilor secrete de stat.

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

ART. 334

Este interzisă introducerea mediilor de stocare amovibile, a software-ului şi hardware-ului, aflate în proprietate privată, în zonele în care se stochează, se procesează sau se transmit informaţii clasificate, fără aprobarea conducătorului unităţii.

N. Utilizarea echipamentelor contractorilor sau a celor puse la dispoziţie de alte instituţii

ART. 335

Utilizarea într-un obiectiv a echipamentelor şi a software-ului contractanţilor, pentru stocarea, procesarea sau transmiterea informaţiilor clasificate este permisă numai cu avizul CSTIC şi aprobarea şefului unităţii.

ART. 336

Utilizarea într-un obiectiv a echipamentelor şi software-ului puse la dispoziţie de către alte institutii poate fi permisă, în acest caz echipamentele sunt evidenţiate în inventarul unităţii, în ambele situaţii, trebuie obţinut avizul CSTIC.

O. Marcarea informaţiilor cu destinaţie specială

ART. 337

Marcarea informaţiilor cu destinaţie specială se aplică, în mod obişnuit, informaţiilor clasificate care necesită o distribuţie limitată şi manipulare specială, suplimentar faţă de caracterul atribuit prin clasificarea de securitate.

CAPITOLUL IX
Contravenţii şi sancţiuni la normele privind protecţia informaţiilor clasificate

ART. 338

(1) Constituie contravenţii la normele privind protecţia informaţiilor clasificate următoarele fapte:

a) deţinerea fără drept, sustragerea, divulgarea, alterarea sau distrugerea neautorizată a informaţiilor secrete de stat;

b) neîndeplinirea măsurilor prevăzute în art. 18, 25-28, 29, 96-139 şi 140-181;

c) neîndeplinirea obligaţiilor 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) şi 185-190;

e) neîndeplinirea sau îndeplinirea defectuoasa a obligaţiilor prevăzute în art. 240 alin. (2) şi (3), art. 243 şi art. 248, precum şi nerespectarea regulilor prevăzute în art. 274-336.

(2) Contravenţiile prevăzute la alin. (1) se sancţionează astfel:

a) contravenţiile prevăzute la alin. (1) lit. a) se sancţionează cu amendă de la 500.000 lei la 50.000.000 lei în cazul faptelor de deţinere fără drept sau de alterare a informaţiilor clasificate şi cu amendă de la 10.000.000 lei la 100.000.000 lei, în cazul faptelor de sustragere, divulgare sau distrugere neautorizată a informaţiilor clasificate;

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

c) faptele prevăzute în alin. (1) lit. d) se sancţionează 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 sancţionează cu amendă de la 5.000.000 lei la 50.000.000 lei.

(3) Persoanele sau autorităţile care constată contravenţiile pot aplica, după caz, şi sancţiunea complementară, constând în confiscarea, în condiţiile legii, a bunurilor destinate, folosite sau rezultate din contravenţii.

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

ART. 339

(1) Contravenţiile şi sancţiunile prevăzute la art. 338 se constată şi se aplică, în limitele competenţelor ce le revin, de către persoane anume desemnate din Serviciul Român de Informaţii, Ministerul Apărării Naţionale, Ministerul de Interne, Ministerul Justiţiei, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Pază şi Serviciul de Telecomunicaţii Speciale.

(2) Pot să constate contravenţiile şi să aplice sancţiunile prevăzute la art. 338, în limitele competenţelor stabilite:

a) persoane anume desemnate din ORNISS;

b) conducătorii autorităţilor sau instituţiilor publice, agenţilor economici cu capital parţial sau integral de stat şi ai altor persoane juridice de drept public;

c) autorităţile sau persoanele prevăzute de reglementările generale referitoare la regimul juridic al contravenţiilor.

(3) Plângerile împotriva proceselor-verbale de constatare a contravenţiilor şi de aplicare a sancţiunilor se soluţioneaza potrivit reglementărilor generale privind regimul juridic al contravenţiilor.

CAPITOLUL X
Dispoziţii finale

ART. 340

Nomenclatura funcţiilor, condiţiile de studii şi vechime, precum şi salarizarea personalului cu atribuţii privind evidenţa, întocmirea, păstrarea, procesarea, multiplicarea,

manipularea, transportul, transmiterea şi distrugerea informaţiilor clasificate se stabilesc potrivit actelor normative în vigoare.

ART. 341

Conducătorii unităţilor care gestionează informaţii clasificate vor lua măsuri ca dispoziţiile prezentelor standarde să fie aduse la cunoştinţa tuturor salariaţilor şi vor intreprinde măsuri pentru:

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

b) nominalizarea personalului cu atribuţii şi funcţii privind gestionarea informaţiilor clasificate;

c) iniţierea demersurilor prevăzute de lege şi de prezentele standarde, pentru obţinerea abilitărilor privind accesul la informaţii clasificate.

ART. 342

La solicitarea persoanelor juridice din sfera de competenţă a Serviciului Român de Informaţii, R.A. Rasirom va evalua conformitatea şi va prezenta ORNISS propuneri de eliberare a certificatelor de acreditare a calităţii pentru sistemele şi echipamentele de protecţie fizică a informaţiilor clasificate.

ART. 343

(1) Prezentele standarde se interpretează şi se aplică în concordanţă cuNormele privind protecţia informaţiilor clasificate ale Organizaţiei Tratatului Atlanticului de Nord în România, aprobate prin Hotărârea Guvernului nr. 353 din 15 aprilie 2002.

(2) În eventualitatea unor neconcordanţe între cele două reglementări menţionate la alin (1), au prioritate Normele privind protecţia informaţiilor clasificate ale Organizaţiei Tratatului Atlanticului de Nord în România, aprobate prin Hotărârea Guvernului nr. 353 din 15 aprilie 2002.

ART. 344

Dispoziţiile prezentelor standarde referitoare la contravenţiile şi sancţiunile la normele privind protecţia informaţiilor clasificate se aplică după 60 de zile de la publicarea prezentei hotărâri.

ART. 345

Anexele nr. 1-32 fac parte integrantă din prezentele standarde naţionale de protecţie a informaţiilor clasificate.