Cuprins

STANDARD NAŢIONAL din 13 iunie 2002 (*actualizat*)
de protecţie a informaţiilor clasificate în România
(actualizat până la data de 24 martie 2005*)
EMITENT • GUVERNUL

---
*) Textul initial a fost publicat în MONITORUL OFICIAL nr. 485 din 5 iulie 2002. Aceasta este forma actualizata de S.C. "Centrul Teritorial de Calcul Electronic" S.A. Piatra Neamt până la data de 24 martie 2005, cu modificările şi completările aduse de: HOTĂRÂREA nr. 2.202 din 30 noiembrie 2004 (~/../../../Public/DetaliiDocumentAfis/57906) şi HOTĂRÂRE nr. 185 din 9 martie 2005 (~/../../../Public/DetaliiDocumentAfis/60231).

+ Capitolul 1 DISPOZITII GENERALE

+ Articolul 1

Standardele naţionale de protecţie a informaţiilor clasificate în România cuprind normele de aplicare a Legii nr. 182/2002 (~/../../../Public/DetaliiDocumentAfis/35209) privind protectia informaţiilor clasificate referitoare la:
a) clasificarile informaţiilor secrete de stat şi normele privind masurile minime de protecţie în cadrul fiecarei clase;
b) oblibaţiile şi raspunderile autorităţilor şi instituţiilor publice, ale agentilor economici şi ale altor persoane juridice de drept public sau privat privind protectia informaţiilor secrete de stat;
c) normele privind accesul la informaţiile clasificate, precum şi procedura verificărilor de securitate;
d) regulile generale privind evidenta, intocmirea, pastrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea informaţiilor secrete de stat;
e) regulile de identificare şi marcare, inscriptionarile şi menţiunile obligatorii pe documentele secrete de stat, în functie de nivelurile de secretizare, cerinţele de evidenta a numerelor de exemplare şi a destinatarilor, termenele şi regimul de pastrare, interdicţiile de reproducere şi circulatie;
f) condiţiile de fotografiere, filmare, cartografiere şi executare a unor lucrari de arte plastice în obiective sau locuri care prezinta importanţa deosebită pentru protectia informaţiilor secrete de stat;
g) regulile privitoare la accesul strainilor la informaţiile secrete de stat;
h) protectia informaţiilor clasificate care fac obiectul contractelor industriale secrete - securitatea industriala;
i) protectia surselor generatoare de informaţii - INFOSEC.

+ Articolul 2

(1) Prezentele standarde instituie sistemul naţional de protecţie a informaţiilor clasificate, în concordanta cu interesul naţional, cu criteriile şi recomandarile NATO şi sunt obligatorii pentru toate persoanele juridice sau fizice care gestioneaza astfel de informaţii.
(2) Echivalenta informaţiilor naţionale clasificate, pe niveluri de secretizare, cu informaţiile NATO clasificate este:
a) Strict secret de importanţa deosebită - NATO top secret
b) Strict secret - NATO secret
c) Secret - NATO confidential

d) Secret de serviciu - NATO restricted

+ Articolul 3

Termenii folositi în prezentele standarde au urmatorul înţeles:

- Autoritate Desemnata de Securitate - ADS - institutie abilitata prin lege sa stabileasca, pentru domeniul sau de activitate şi responsabilitate, structuri şi măsuri proprii privind coordonarea şi controlul activităţilor referitoare la protectia informaţiilor secrete de stat. Sunt autorităţi desemnate de securitate, potrivit legii: Ministerul Apararii Naţionale, Ministerul de Interne, Ministerul Justiţiei, Serviciul Roman de Informaţii, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Paza, Serviciul de Telecomunicatii Speciale;
- autorizatie de acces la informaţii clasificate - document eliberat cu avizul instituţiilor abilitate, de conducatorul persoanei juridice detinatoare de astfel de informaţii, prin care se confirma 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 cunoaste;
- autorizatie de securitate industriala - document eliberat de Oficiul Registrului Naţional al Informaţiilor Secrete de Stat - ORNISS - unui obiectiv industrial, prin care se atesta ca este abilitat sa participe la procedura de negociere a unui contract clasificat;
- autorizatie speciala - document eliberat de către ORNISS prin care se atesta verificarea şi acreditarea unei persoane de a desfăşura activităţi de fotografiere, filmare, cartografiere şi lucrari de arte plastice pe teritoriul României, în obiective, zone sau locuri care prezinta importanţa deosebită pentru protectia informaţiilor secrete de stat;
- aviz de securitate industriala - document eliberat de către ADS prin care se atesta ca obiectivul industrial contractant a implementat toate masurile de securitate necesare protectiei informaţiilor clasificate vehiculate în derularea contractului incheiat;
- certificat de securitate - document eliberat persoanei cu atribuţii nemijlocite în domeniul protectiei informaţiilor clasificate, respectiv functionarului de securitate sau salariatului din structura de securitate, care atesta verificarea şi acreditarea de a detine, de a avea acces şi de a lucra cu informaţii clasificate de un anumit nivel de secretizare;
- certificat de securitate industriala - document eliberat de ORNISS unui obiectiv industrial, prin care se atesta ca este abilitat sa deruleze activităţi industriale şi/sau de cercetare ce presupun accesul la informaţii clasificate;
- clasificarea informaţiilor - incadrarea informaţiilor intr-o clasa şi nivel de secretizare;
- contract clasificat - orice contract incheiat între părţi, în condiţiile legii, în cadrul caruia se cuprind şi se vehiculeaza informaţii clasificate;
- contractant - unitate industriala, comerciala, 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 informatiei clasificate de sub incidenţa reglementarilor 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 contine informaţii clasificate, în original sau copie, precum:

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

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

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

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

- functionar de securitate - persoana care indeplineste atribuţiile de protecţie a informaţiilor clasificate în cadrul autorităţilor, instituţiilor publice, agentilor 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 evidenta, accesare, procesare, multiplicare, manipulare, transport, transmitere, inventariere, pastrare, arhivare sau distrugere a informaţiilor clasificate;
- incident de securitate - orice actiune sau inactiune contrara reglementarilor de securitate a carei consecinţa a determinat sau este de natura sa determine compromiterea informaţiilor clasificate;
- indicator de interdictie text sau simbol care semnaleaza interzicerea accesului sau derularii unor activităţi în zone, obiective, sectoare sau locuri care prezinta importanţa deosebită pentru protectia informaţiilor clasificate;
- informatie clasificata compromisa - informatie clasificata care şi-a pierdut integritatea, a fost ratacita, pierduta ori accesata, total sau parţial, de persoane neautorizate;
- institutie cu atribuţii de coordonare a activităţii şi de control al masurilor privitoare la protectia informaţiilor clasificate sau institutie abilitata - Ministerul Apararii Naţionale, Ministerul de Interne, Ministerul Justiţiei, Serviciul Roman de Informaţii, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Paza, Serviciul de Telecomunicatii Speciale, potrivit competentelor stabilite prin lege;
- marcare - activitatea de inscriptionare a nivelului de secretizare a informatiei şi de semnalare a cerinţelor speciale de protecţie a acesteia;
- material clasificat - document sau produs prelucrat ori în curs de prelucrare, care necesita a fi protejat împotriva cunoasterii neautorizate;

- necesitatea de a cunoaste - principiul conform caruia accesul la informaţii clasificate se acordă în mod individual numai persoanelor care, pentru indeplinirea indatoririlor de serviciu, trebuie să lucreze cu astfel de informaţii sau să aibă acces la acestea;
- negocieri - activităţile circumscrise adjudecarii unui contract sau subcontract, de la notificarea intentiei de organizare a licitaţiei, până la incheierea acesteia;
- obiectiv industrial - unitate de cercetare sau cu activitate de productie, care desfăşoară activităţi stiintifice, tehnologice sau economice ce au legătură cu siguranţa sau cu apararea naţionala, ori prezinta importanţa deosebită pentru interesele economice şi tehnico-stiintifice ale României;
- obiectiv, sector sau loc de importanţa deosebită pentru protectia informaţiilor secrete de stat - incinta sau perimetru anume desemnat, în care sunt gestionate informaţii secrete de stat;
- parte contractantă - oricare dintre părţile care convin sa negocieze, sa incheie sau sa deruleze un contract clasificat;
- protectia surselor generatoare de informaţii - ansamblul masurilor destinate protectiei informaţiilor elaborate, stocate sau transmise prin sisteme ori retele de prelucrare automata a datelor şi/sau de comunicatii;
- securitate industriala - sistemul de norme şi măsuri care reglementeaza protectia informaţiilor clasificate în domeniul activităţilor contractuale;
- sistem de protecţie a informaţiilor clasificate - ansamblul de măsuri de natura juridica, procedurala, fizica, de protecţie a personalului şi a surselor generatoare de informaţii, destinate securitatii materialelor şi documentelor clasificate;
- structura de securitate - compartiment specializat în protectia informaţiilor clasificate, organizat în cadrul autorităţilor, instituţiilor publice, agentilor economici cu capital integral sau parţial de stat şi al altor persoane juridice de drept public sau privat;
- subcontractant - parte care îşi asuma executarea unei părţi a contractului clasificat sub coordonarea contractantului;
- trecerea la un alt nivel de clasificare sau de secretizare - schimbarea clasificarii, respectiv a nivelului de secretizare a informaţiilor secrete de stat;
- unitate detinatoare de informaţii clasificate sau unitate - autoritate sau institutie 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 detine informaţii clasificate;
- verificare de securitate - totalitatea masurilor intreprinse de autorităţile desemnate de securitate, conform competentelor, pentru stabilirea onestitatii şi profesionalismului persoanelor, în scopul avizarii eliberarii certificatului de securitate sau autorizatiei de acces la informaţii clasificate;
- zona de securitate - perimetru delimitat şi special amenajat unde sunt gestionate informaţii clasificate.

+ Capitolul 2 CLASIFICAREA ŞI DECLASIFICAREA INFORMATIILOR. MASURI MINIME DE PROTECTIE SPECIFICE CLASELOR ŞI NIVELURILOR DE SECRETIZARE

+ Secţiunea 1 Clasificarea informaţiilor

+ Articolul 4

(1) Potrivit legii, informaţiile sunt clasificate secrete de stat sau secrete de serviciu, în raport de importanţa pe care o au pentru securitatea naţionala şi de consecintele ce s-ar produce ca urmare a dezvaluirii sau diseminarii lor neautorizate.
(2) Informaţiile secrete de stat sunt informaţiile a caror divulgare poate prejudicia siguranţa naţionala şi apararea tarii şi care, în functie de importanţa valorilor protejate, se includ în urmatoarele niveluri de secretizare prevăzute de lege:
a) strict secret de importanţa deosebită;
b) strict secret;
c) secret.
(3) Informaţiile a caror divulgare este de natura sa determine prejudicii unei persoane juridice de drept public sau privat se clasifica secrete de serviciu.

+ Articolul 5

(1) Autorităţile publice care elaboreaza ori lucreaza cu informaţii secrete de stat au obligaţia sa intocmeasca un ghid pe baza caruia se va realiza clasificarea corecta şi uniforma a acestora.
(2) Ghidul prevăzut la alin. (1) se aproba personal şi în scris de către imputernicitii sau, după caz, funcţionarii superiori abilitati sa atribuie nivelurile de secretizare, conform legii.

+ Articolul 6

Autorităţile şi instituţiile publice intocmesc liste proprii cuprinzand categoriile de informaţii secrete de stat în domeniile lor de activitate, care se aproba şi se actualizeaza prin hotărâre a Guvernului.

+ Articolul 7

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

+ Articolul 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 indeplinirea atribuţiilor de serviciu, divulgarea lor putand prejudicia interesul unităţii.

+ Articolul 9

Unitatile care gestioneaza informaţii clasificate au obligaţia sa analizeze ori de cate 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.

+ Articolul 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.

+ Articolul 11

Seful ierarhic al emitentului are obligaţia sa verifice dacă informaţiile au fost clasificate corect şi sa ia măsuri în consecinţa, când constata ca au fost atribuite niveluri de secretizare necorespunzatoare.

+ Articolul 12

(1) Termenele de clasificare a informaţiilor secrete de stat vor fi stabilite de emitent, în functie de importanţa acestora şi de consecintele care s-ar produce ca urmare a dezvaluirii sau diseminarii lor neautorizate.

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

- 100 de ani pentru informaţiile clasificate strict secret de importanţa 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 motivatii temeinice, la solicitarea conducătorilor unităţilor detinatoare de informaţii clasificate sau, după caz, a imputernicitilor şi functionarilor superiori abilitati sa atribuie nivelurile de secretizare.

+ Articolul 13

Fiecare imputernicit ori functionar superior abilitat sa atribuie niveluri de secretizare va dispune verificarea periodica 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.

+ Articolul 14

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

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

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

+ Articolul 15

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

+ Articolul 16

Cazurile considerate supraevaluari ori subevaluari ale clasei sau nivelului de secretizare vor fi supuse atenţiei emitentului, iar dacă acesta decide sa reclasifice informaţiile va informa detinatorii.

+ Articolul 17

(1) Informaţiile vor fi clasificate numai în cazul în care se impune protectia acestora, iar nivelurile de secretizare şi termenele de clasificare subzista atât timp cat dezvaluirea sau diseminarea lor neautorizata ar putea prejudicia siguranţa naţionala, apararea tarii, 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.

+ Articolul 18

(1) În termen de 12 luni de la intrarea în vigoare a prezentei hotărâri, detinatorii de informaţii secrete de stat şi secrete de serviciu, stabilite astfel potrivit H.C.M. nr. 19 din 14 ianuarie 1972 (~/../../../Public/DetaliiDocumentAfis/298), vor prezenta persoanelor sau autorităţilor publice imputernicite sa atribuie niveluri de secretizare propuneri privind incadrarea 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

+ Articolul 19

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

+ Articolul 20

(1) Informaţiile se declasifica dacă:

a) termenul de clasificare a expirat;

b) dezvaluirea informaţiilor nu mai poate prejudicia siguranţa naţionala, apararea tarii, ordinea publică, ori interesele persoanelor de drept public sau privat detinatoare;

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

(2) Declasificarea sau trecerea la un alt nivel de secretizare a informaţiilor secrete de stat se realizează de imputernicitii şi funcţionarii superiori abilitati prin lege sa atribuie niveluri de secretizare, cu avizul prealabil al instituţiilor care coordonează activitatea şi controlul masurilor privitoare la protectia informaţiilor clasificate, potrivit competentelor materiale.

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

+ Articolul 21

Ori de cate 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 anumita data sau la producerea unui anumit eveniment.

+ Articolul 22
(1) La schimbarea clasei sau nivelului de secretizare atribuit initial unei informaţii, emitentul este obligat sa incunostinteze structura/functionarul de securitate, care va face menţiunile necesare în registrele de evidenta.
(2) Data şi noua clasa sau nivel de secretizare vor fi marcate pe document deasupra sau sub vechea inscriptie, care va fi anulata prin trasarea unei linii oblice.
(3) Emitentul informaţiilor declasificate ori trecute în alt nivel de clasificare se va asigura ca gestionarii acestora sunt anuntati la timp, în scris, despre acest lucru.
+ Articolul 23
(1) Informaţiile clasificate despre care s-a stabilit cu certitudine ca 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.
+ Articolul 24
Informaţiile secrete de serviciu se declasifica de conducătorii unităţilor care le-au emis, prin scoaterea de pe listele prevăzute la art. 8, care vor fi reanalizate ori de cate ori este necesar.
+ Secţiunea a 3-a Măsuri minime de protecţie a informaţiilor clasificate
+ Articolul 25
Masurile 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, functia şi numărul persoanelor care au sau pot avea acces la informaţii, potrivit certificatului de securitate şi autorizatiei de acces şi cu respectarea principiului necesităţii de a cunoaste;
d) amenintarile, riscurile şi vulnerabilitatile ce pot avea consecinte asupra informaţiilor clasificate.
+ Articolul 26
Transmiterea informaţiilor clasificate către alti utilizatori se va efectua numai dacă acestia deţin certificate de securitate sau autorizaţii de acces corespunzător nivelului de secretizare.
+ Articolul 27
Certificatele de securitate aparţinând persoanelor al caror comportament, atitudini sau manifestari pot crea premise de insecuritate pentru informaţiile secrete de stat vor fi imediat retrase, cu incunostintarea instituţiilor investite cu atribuţii de coordonare a activităţii şi de control al masurilor privitoare la protectia informaţiilor clasificate, potrivit competentelor.
+ Articolul 28
Conducătorii unităţilor şi persoanele care gestioneaza informaţii clasificate au obligaţia de a aduce la cunoştinţa instituţiilor cu atribuţii de coordonare şi control în domeniu orice indicii din care pot rezultă premise de insecuritate pentru astfel de informaţii.
+ Secţiunea a 4-a Structura/functionarul de securitate
+ Articolul 29
(1) Pentru implementarea masurilor de protecţie a informaţiilor clasificate, în unitatile detinatoare de astfel de informaţii se infiinteaza, în condiţiile legii, structuri de securitate cu atribuţii specifice.
(2) În situaţia în care unitatea detine un volum redus de informaţii clasificate, atribuţiile structurii de securitate vor fi indeplinite de functionarul de securitate.
(3) Structura de securitate se organizeaza şi se încadrează potrivit legii.
(4) Seful structurii de securitate, respectiv functionarul de securitate, este un adjunct al conducătorului persoanei juridice sau un membru al consiliului de administratie al unităţii.
+ Articolul 30
Seful structurii de securitate, respectiv functionarul de securitate, detine certificat de securitate corespunzător celui mai înalt nivel de clasificare a informaţiilor secrete de stat gestionate de unitate.
+ Articolul 31
(1) Structura/functionarul de securitate are urmatoarele atribuţii generale:
a) elaboreaza şi supune aprobării conducerii unităţii normele interne privind protectia informaţiilor clasificate, potrivit legii;
b) întocmeşte programul de prevenire a scurgerii de informaţii clasificate şi îl supune avizarii instituţiilor abilitate, iar după aprobare, acţionează pentru aplicarea acestuia;
c) coordonează activitatea de protecţie a informaţiilor clasificate, în toate componentele acesteia;
d) asigura relationarea cu institutia abilitata sa coordoneze activitatea şi sa controleze masurile privitoare la protectia informaţiilor clasificate, potrivit legii;
e) monitorizează activitatea de aplicare a normelor de protecţie a informaţiilor clasificate şi modul de respectare a acestora;
f) consiliaza conducerea unităţii în legătură cu toate aspectele privind securitatea informaţiilor clasificate;
g) informeaza conducerea unităţii despre vulnerabilitatile şi riscurile existente în sistemul de protecţie a informaţiilor clasificate şi propune măsuri pentru înlăturarea acestora;
h) acorda sprijin reprezentantilor autorizati ai instituţiilor abilitate, potrivit competentelor legale, pe linia verificării persoanelor pentru care se solicita accesul la informaţii clasificate;
i) organizeaza activităţi de pregatire specifică a persoanelor care au acces la informaţii clasificate;
j) asigura pastrarea şi organizeaza evidenta certificatelor de securitate şi autorizaţiilor de acces la informaţii clasificate;
k) actualizeaza permanent evidenta certificatelor de securitate şi a autorizaţiilor de acces;
l) întocmeşte şi actualizeaza listele informaţiilor clasificate elaborate sau pastrate de unitate, pe clase şi niveluri de secretizare;

m) prezinta conducătorului unităţii propuneri privind stabilirea obiectivelor, sectoarelor şi locurilor de importanţa deosebită pentru protectia informaţiilor clasificate din sfera de responsabilitate şi, după caz, solicita sprijinul instituţiilor abilitate;
n) efectueaza, cu aprobarea conducerii unităţii, controale privind modul de aplicare a masurilor 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 functionarului de securitate, se stabilesc prin fisa postului, aprobata de conducatorul unităţii.

+ Articolul 32

Persoanele care lucreaza în structura de securitate sau, după caz, functionarul de securitate vor fi incluse în programe permanente de pregatire organizate de instituţiile investite cu atribuţii de coordonare a activităţii şi de control al masurilor privitoare la protectia informaţiilor clasificate, potrivit legii.

+ Secţiunea a 5-a Accesul la informaţiile clasificate

+ Articolul 33

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

+ Articolul 34

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

+ Articolul 35

(1) Persoanele cărora le-au fost eliberate certificate de securitate sau autorizaţii de acces vor fi instruite, atât la acordarea acestora, cat şi periodic, cu privire la conţinutul reglementarilor privind protectia informaţiilor clasificate.
(2) Activităţile de instruire vor fi consemnate de structura/functionarul de securitate, sub semnatura, în fisa de pregatire individuala, prezentată la anexa nr. 2.
(3) Persoanele prevăzute la alin. (1) vor semna angajamentul de confidentialitate prevăzut la anexa nr. 3.

+ Articolul 36

(1) În cazuri excepţionale, determinate de situaţii de criza, calamitati sau evenimente imprevizibile, conducatorul unităţii poate acorda acces temporar la informaţii clasificate anumitor persoane care nu deţin certificat de securitate sau autorizatie de acces, cu condiţia asigurarii unui sistem corespunzător de evidenta.
(2) Persoanele care primesc dreptul de acces temporar la informaţii secrete de stat vor semna angajamentul de confidentialitate şi vor fi comunicate la ORNISS, în cel mai scurt timp posibil, pentru efectuarea verificărilor de securitate, potrivit procedurilor.

+ Articolul 37

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

+ Articolul 38

(1) Transmiterea informaţiilor clasificate între unităţi se va efectua cu aprobarea emitentului şi cu respectarea principiului necesităţii de a cunoaste.
(2) Predarea-primirea informaţiilor clasificate între unitatea detinatoare şi unitatea primitoare se face cu respectarea masurilor de protecţie prevăzute în prezentele standarde.

+ Articolul 39

Structura/functionarul de securitate al unităţii detinatoare se va asigura ca reprezentantul unităţii primitoare detine certificatul de securitate sau autorizatia de acces corespunzătoare nivelului de secretizare a informaţiilor clasificate ce fac obiectul predarii-primirii.

+ Capitolul 3 REGULI GENERALE PRIVIND EVIDENTA, INTOCMIREA, PASTRAREA, PROCESAREA, MULTIPLICAREA, MANIPULAREA, TRANSPORTUL, TRANSMITEREA ŞI DISTRUGEREA INFORMATIILOR CLASIFICATE

+ Articolul 40

(1) În unitatile detinatoare de informaţii clasificate se organizeaza compartimente speciale pentru evidenta, intocmirea, pastrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea acestora în condiţii de siguranţă.
(2) Activitatea compartimentelor speciale prevăzute la alin. (1) este coordonata de structura/functionarul de securitate.

+ Articolul 41

La redactarea documentelor ce conţin informaţii clasificate se vor respecta urmatoarele reguli:
a) menţionarea, în antet, a unităţii emitente, a numarului şi datei înregistrării, a clasei sau nivelului de secretizare, a numarului de exemplare şi, după caz, a destinatarului;
b) numerele de înregistrare se inscriu pe toate exemplarele documentului şi pe anexele acestora, fiind precedate de un zero (0) pentru documentele secrete, de doua zerouri (00) pentru cele strict secrete, de trei zerouri (000) pentru cele strict secrete de importanţa deosebită şi de litera "S" pentru secrete de serviciu;
c) la sfârşitul documentului se inscriu în clar, după caz, rangul, functia, numele şi prenumele conducătorului unităţii emitente, precum şi ale celui care îl întocmeşte, urmate de semnaturile acestora şi stampila unităţii;
d) înscrierea, pe fiecare pagina a documentului, a clasei sau nivelului de secretizare atribuit acestuia;
e) pe fiecare pagina a documentelor ce conţin informaţii clasificate se inscriu numărul curent al paginii, urmat de numărul total al acestora.

+ Articolul 42

(1) În situaţia în care documentul de baza este insotit de anexe, la sfârşitul textului se indica, pentru fiecare anexa, numărul de înregistrare, numărul de file al acesteia şi clasa sau nivelul de secretizare.
(2) Anexele se clasifica în functie 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 semneaza, dacă este cazul, de persoanele care au semnat documentul de baza.
(5) Aplicarea, pe documentele anexate, a stampilei unităţii emitente este obligatorie.

+ Articolul 43

(1) Când documentele ce conţin informaţii clasificate se semneaza de o singura persoana, datele privind rangul, functia, numele şi prenumele acesteia se inscriu sub text, în centrul paginii.
(2) Când semneaza doua sau mai multe persoane, rangul, functia, numele şi prenumele conducătorului unităţii se inscriu în partea stanga, iar ale celorlalţi semnatari în partea dreaptă, în ordinea rangurilor şi functiilor.

+ Articolul 44

Când documentele care conţin informaţii clasificate se emit în comun de doua sau mai multe unităţi, denumirile acestora se inscriu separat în antet, iar la sfârşit se semneaza de către conducătorii unităţilor respective, de la stanga la dreapta, aplicandu-se stampilele corespunzătoare.

+ Articolul 45

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

+ Articolul 46

(1) Toate documentele, indiferent de forma, care conţin informaţii clasificate au inscrise, pe fiecare pagina, nivelul de secretizare.
(2) Nivelul de secretizare se marcheaza prin stampilare, dactilografiere, tiparire sau ograf, astfel:
a) în partea dreaptă sus şi jos, pe exteriorul copertelor, pe pagina cu titlul şi pe prima pagina a documentului;
b) în partea de jos şi de sus, la mijlocul paginii, pe toate celelalte pagini ale documentului;
c) sub legenda, titlu sau scara de reprezentare şi în exterior - pe verso - atunci când acestea sunt pliate, pe toate schemele, diagramele, hartile, desenele şi alte asemenea documente.

+ Articolul 47

Portiunile 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.

+ Articolul 48

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

+ Articolul 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 aceleasi condiţii ca şi a celor în forma definitivă.

+ Articolul 50

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

+ Articolul 51

(1) Fotografiile, filmele, microfilmele şi negativele lor, rolele, bobinele sau containerele de pastrare a acestora se marcheaza vizibil cu o eticheta care indica numărul şi data înregistrării, precum şi clasa sau nivelul de secretizare.
(2) Microfilmele trebuie să aibă afisat la cele doua capete clasa sau nivelul de secretizare, iar la inceputul rolei, lista elementelor de continut.

+ Articolul 52

(1) Clasa sau nivelul de secretizare a informaţiilor înregistrate pe benzi audio se imprima verbal, atât la inceputul înregistrării, cat şi la sfârşitul acesteia.
(2) Marcarea clasei sau a nivelului de secretizare pe benzi video trebuie să asigure afisarea 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 inregistrarea benzilor, marcajul se aplică prin inserarea unui segment de banda la inceputul 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.

+ Articolul 53

Proiectiile de imagini trebuie să afiseze, la inceputul şi sfârşitul acestora, numărul şi data înregistrării, precum şi clasa sau nivelul de secretizare.

+ Articolul 54

(1) Rolele, bobinele sau containerele de pastrare a benzilor magnetice, inclusiv cele video, pe care au fost imprimate informaţii secrete de stat, vor avea inscris, 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 banda magnetica, atât la inceputul, cat şi la sfârşitul fiecarui pasaj, se va menţiona clasa sau nivelul de secretizare.

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

+ Articolul 55

În toate cazurile, ambalajele sau suportii în care se păstrează documente sau materiale ce conţin informaţii clasificate vor avea inscripţionat clasa sau nivelul de secretizare, numărul şi data înregistrării în evidente şi li se va atasa o lista cu denumirea acestora.

+ Articolul 56

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

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

+ Articolul 57

Numărul şi data initiala a înregistrării documentului clasificat trebuie pastrate, chiar dacă i se aduc amendamente, până când documentul respectiv va face obiectul reevaluarii clasei sau a nivelului de secretizare.

+ Articolul 58

Conducătorii unităţilor vor asigura masurile necesare de evidenta şi control al informaţiilor clasificate, astfel încât să se poată stabili, în orice moment, locul în care se afla aceste informaţii.

+ Articolul 59

(1) Evidenta materialelor şi documentelor care conţin informaţii clasificate se tine în registre speciale, intocmite 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 inscris în registrele de evidenta.

(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 evidenta a registrelor, condicilor, borderourilor şi a caietelor pentru insemnari clasificate, conform modelului din anexa nr. 7.

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

+ Articolul 60

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

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

(3) Inn registrele pentru evidenta 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.

+ Articolul 61

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

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

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

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

+ Articolul 62

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

(2) Evidenta documentelor strict secrete şi secrete poate fi operata în acelasi registru.

+ Articolul 63

Hartile, planurile topografice, asamblajele de harti şi alte asemenea documente se înregistrează în registrele pentru evidenta informaţiilor clasificate prevăzute în anexele nr. 4, 5 şi 6.

+ Articolul 64

Atribuirea aceluiasi numar de înregistrare unor documente cu continut diferit este interzisa.

+ Articolul 65

Registrele de evidenta vor fi completate de persoana desemnata care detine autorizatie sau certificat de securitate corespunzător.

+ Articolul 66

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

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

+ Articolul 67

(1) Documentelor care conţin informaţii clasificate rezultate în procesul de multiplicare li se atribuie numere din registrul de evidenta 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 inscriu obligatoriu pe toate exemplarele documentului.

+ Articolul 68

(1) Evidentierea operaţiunii de multiplicare se face prin marcare atât pe original, cat 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 pagina, 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 numeroteaza în ordine succesiva, chiar dacă operaţiunea se efectueaza de mai multe ori şi la date diferite.

+ Articolul 69

(1) Multiplicarea documentelor clasificate se face în baza aprobării conducătorului unităţii detinatoare, cu avizul structurii/functionarului de securitate, ambele inscrise pe cererea pentru copiere sau pe adresa de însoţire în care se menţionează necesitatea multiplicarii.
(2) Parchetele, instantele şi comisiile de cercetare pot multiplica documente care conţin informaţii clasificate numai în condiţiile prezentelor standarde.
(3) Extrasul dintr-un document care contine informaţii clasificate se face în baza cererii pentru copiere, cu aprobarea conducătorului unităţii, iar documentul rezultat va avea mentionat 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.

+ Articolul 70

(1) Dacă emitentul doreste să aibă control exclusiv asupra reproducerii, documentul va contine o indicatie vizibila cu urmatorul continut: "Reproducerea acestui document, totala sau parţială, este interzisa".
(2) Informaţiile clasificate inscrise pe documente cu regim restrictiv de reproducere care au menţiunea "Reproducerea interzisa" nu se multiplica.

+ Articolul 71

În cazul copierii unui document care contine informaţii clasificate se procedeaza astfel:
a) se stabileste numărul de exemplare în care va fi multiplicat;
b) se completeaza şi se aproba cererea pentru multiplicare, potrivit art. 69 alin. (1), după care aceasta se înregistrează în registrul de evidenta - anexa nr. 4 sau anexa nr. 5, după caz;
c) documentul original se preda operatorului pe bază de semnatura;
d) după verificarea exemplarelor rezultate, beneficiarul semneaza în registrul de evidenta a informaţiilor clasificate multiplicate, conform modelului din anexa nr. 9;
e) repartitia în vederea difuzarii exemplarelor copiate se consemneaza de către structura/functionarul de securitate pe spatele cererii pentru copiere;
f) cererea pentru copiere împreună cu exemplarele copiate se predau pe bază de semnatura structurii/functionarului de securitate în vederea difuzarii sau expedierii.

+ Articolul 72

(1) Când se dactilografiaza, se proceseaza la calculator sau se copiaza documente care conţin informaţii clasificate, în mai mult de doua exemplare, pe spatele exemplarului original sau al cererii pentru copiere se inscriu 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 executarii, avandu-se în vedere şi numărul de exemplare rezultat în urma dactilografierii sau procesarii la calculator.

+ Articolul 73

Documentele clasificate pot fi microfilmate sau stocate pe discuri optice ori pe suporti magnetici în urmatoarele 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 suportilor magnetici de stocare sa li se asigure aceeasi protecţie ca a documentului original;
c) toate microfilmele, discurile optice sau suportii magnetici de stocare să fie înregistrate intr-o evidenta specifică şi supuse, ca şi documentele originale, verificării anuale.

+ Articolul 74

(1) Difuzarea informaţiilor clasificate multiplicate se face obligatoriu cu avizul structurii/ functionarului de securitate.
(2) Informaţiile clasificate pot fi redifuzate de către destinatarul initial la alti destinatari, cu respectarea normelor din prezentele standarde.
(3) Emitentul este obligat sa indice clar toate restrictiile care trebuie respectate pentru difuzarea unei informaţii clasificate. Când se impun astfel de restrictii, destinatarii pot proceda la o redifuzare numai cu aprobarea scrisa a emitentului.

+ Articolul 75

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

+ Articolul 76

(1) Informaţiile clasificate iesite din termenul de clasificare se arhiveaza sau se distrug.
(2) Arhivarea sau distrugerea unui document clasificat se menţionează în registrul de evidenta principal, prin consemnarea cotei arhivistice de regasire sau, după caz, a numarului de înregistrare a procesului-verbal de distrugere.
(3) Distrugerea informaţiilor clasificate inlocuite 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 sa nu mai poata fi reconstituite.

+ Articolul 77
(1) Documentele de lucru, ciornele sau materialele acumulate sau create în procesul de elaborare a unui document, care conţin informaţii clasificate, de regula, 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 continute, arhivate şi protejate corespunzător clasei sau nivelului de secretizare a documentului final.
+ Articolul 78
(1) Informaţiile strict secrete de importanţa deosebită destinate distrugerii vor fi inapoiate unităţii emitente cu adresa de restituire.
(2) Fiecare asemenea informatie va fi trecuta pe un proces-verbal de distrugere, care va fi aprobat de conducerea unităţii şi semnat de seful structurii/functionarul de securitate şi de persoana care asista la distrugere, autorizata să aibă acces la informaţii strict secrete de importanţa deosebită.
(3) În situaţii de urgenta, protectia, inclusiv prin distrugere, a materialelor şi documentelor strict secrete de importanţa deosebită va avea intotdeauna prioritate faţă de alte documente sau materiale.
(4) Procesele-verbale de distrugere şi documentele de evidenta ale acestora vor fi arhivate şi pastrate cel puţin 10 ani.
+ Articolul 79
(1) Distrugerea informaţiilor strict secrete, secrete şi secrete de serviciu va fi evidentiata într-un proces-verbal semnat de doua persoane asistente autorizate să aibă acces la informaţii de acest nivel, avizat de structura/functionarul de securitate şi aprobat de conducatorul unităţii.
(2) Procesele-verbale de distrugere şi documentele de evidenta a informaţiilor strict secrete, secrete şi secrete de serviciu vor fi pastrate de compartimentul care a executat distrugerea, o perioadă de cel puţin trei ani, după care vor fi arhivate şi pastrate cel puţin 10 ani.
+ Articolul 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 intr-o formă de evidenta.
+ Articolul 81
(1) Documentele şi materialele ce conţin informaţii clasificate se transporta, pe teritoriul României, prin intermediul unităţii specializate a Serviciului Roman de Informaţii, potrivit normelor stabilite prin hotărâre a Guvernului.
(2) Documentele şi materialele care conţin informaţii clasificate se transporta în strainatate prin valiza diplomatica, de către curierii diplomatici selectionati şi pregatiti de Serviciul de Informaţii Externe.
(3) Este interzisa expedierea documentelor şi materialelor ce conţin informaţii clasificate prin S.N. "Posta Română" ori prin alte societăţi comerciale de transport.
+ Articolul 82
Conducătorii unităţilor detinatoare de informaţii clasificate vor desemna, din structura de securitate proprie, în condiţiile prezentelor standarde, cel puţin un delegat imputernicit pentru transportul şi executarea operaţiunilor de predare-primire a corespondentei clasificate, între aceasta şi unitatea specializata a Serviciului Roman de Informaţii.
+ Capitolul 4 PROTECTIA INFORMATIILOR SECRETE DE STAT
+ Secţiunea 1 Oblibaţiile şi raspunderile ce revin autorităţilor şi instituţiilor publice, agentilor economici şi altor persoane juridice pentru protectia informaţiilor secrete de stat
+ Articolul 83
Protectia informaţiilor secrete de stat reprezinta o obligaţie ce revine tuturor persoanelor autorizate care le emit, le gestioneaza sau care intră în posesia lor.
+ Articolul 84
(1) Conducătorii unităţilor detinatoare de informaţii secrete de stat sunt raspunzatori de aplicarea masurilor de protecţie a informaţiilor secrete de stat.
(2) Persoanele juridice de drept privat detinatoare de informaţii secrete de stat au obligaţia să respecte şi să aplice reglementarile în vigoare stabilite pentru autorităţile şi instituţiile publice, în domeniul lor de activitate.
+ Articolul 85
Până la înfiinţarea şi organizarea structurii de securitate sau, după caz, până la numirea functionarului de securitate, conducătorii unităţilor detinatoare de informaţii secrete de stat vor desemna o persoană care să indeplineasca temporar atribuţiile specifice protectiei informaţiilor clasificate, prin cumul de functii.
+ Articolul 86
(1) Conducatorul unităţii care gestioneaza informaţii secrete de stat este obligat:
a) să asigure organizarea activităţii structurii de securitate, respectiv a functionarului 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) sa notifice la ORNISS eliberarea certificatului de securitate sau autorizatiei de acces pentru fiecare angajat care lucreaza cu informaţii clasificate;
d) sa aprobe listele cu personalul verificat şi avizat pentru lucrul cu informaţiile secrete de stat şi evidenta deţinătorilor de certificate de securitate şi autorizaţii de acces şi să le comunice la ORNISS şi la instituţiile abilitate sa coordoneze activitatea şi controlul masurilor privitoare la protectia informaţiilor clasificate, potrivit legii;
e) sa intocmeasca lista informaţiilor secrete de stat şi a termenelor de mentinere în nivelurile de secretizare şi sa o supuna aprobării Guvernului, potrivit legii;

f) sa stabileasca obiectivele, sectoarele şi locurile din zona de competenţa care prezinta importanţa deosebită pentru protectia informaţiilor secrete de stat şi să le comunice Serviciului Roman de Informaţii pentru a fi supuse spre aprobare Guvernului;
g) să solicite asistenţa de specialitate instituţiilor abilitate sa coordoneze activitatea şi sa controleze masurile privitoare la protectia informaţiilor secrete de stat;
h) sa supuna avizarii instituţiilor abilitate programul propriu de prevenire a scurgerii de informaţii clasificate şi să asigure aplicarea acestuia;
i) sa elaboreze şi să aplice masurile procedurale de protecţie fizica şi de protecţie a personalului care are acces la informaţii clasificate;
j) sa intocmeasca ghidul pe baza caruia se va realiza incadrarea corecta şi uniforma în nivelurile de secretizare a informaţiilor secrete de stat, în stricta conformitate cu legea şi sa îl prezinte, spre aprobare, imputernicitilor şi functionarilor superiori abilitati prin lege sa atribuie nivelurile de secretizare;
k) să asigure aplicarea şi respectarea regulilor generale privind evidenta, intocmirea, pastrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea informaţiilor secrete de stat şi a interdictiilor de reproducere şi circulatie, în conformitate cu actele normative în vigoare;
l) sa comunice instituţiilor abilitate, potrivit competentelor, lista functiilor din subordine care necesita acces la informaţii secrete de stat;
m) la incheierea contractelor individuale de muncă, a contractelor de colaborare sau convenţiilor de orice natura sa precizeze oblibaţiile ce revin părţilor pentru protectia informaţiilor clasificate în interiorul şi în afara unităţii, în timpul programului şi după terminarea acestuia, precum şi la încetarea activităţii în unitatea respectiva;
n) să asigure includerea personalului structurii/functionarului de securitate în sistemul permanent de pregatire şi perfectionare, conform prezentelor standarde;
o) sa aprobe normele interne de aplicare a masurilor privind protectia informaţiilor clasificate, în toate componentele acesteia, şi sa controleze modul de respectare în cadrul unităţii;
p) să asigure fondurile necesare pentru implementarea masurilor privitoare la protectia informaţiilor clasificate, conform legii;
q) sa analizeze, ori de cate ori este necesar, dar cel puţin semestrial, modul în care structura/functionarul de securitate şi personalul autorizat asigura protectia informaţiilor clasificate;
r) să asigure inventarierea anuală a documentelor clasificate şi, pe baza acesteia, sa dispună măsuri în consecinţa, conform legii;
s) sa sesizeze instituţiile prevăzute la art. 25 din Legea nr. 182/2002 (~/../../../Public/DetaliiDocumentAfis/35209), conform competentelor, în legătură cu incidentele de securitate şi riscurile la adresa informaţiilor secrete de stat;
t) sa dispună efectuarea de cercetari şi, după caz, sa sesizeze organele de urmărire penala 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 (~/../../../Public/DetaliiDocumentAfis/35209).

+ Secţiunea a 2-a Protectia juridica

+ Articolul 87

Conducătorii unităţilor detinatoare de secrete de stat vor asigura condiţiile necesare pentru ca toate persoanele care gestioneaza astfel de informaţii sa cunoasca reglementarile în vigoare referitoare la protectia informaţiilor clasificate.

+ Articolul 88

(1) Conducătorii unităţilor detinatoare de informaţii secrete de stat au obligaţia de a instiinta, în scris, instituţiile prevăzute la art. 25 din Legea nr. 182/2002 (~/../../../Public/DetaliiDocumentAfis/35209), potrivit competentelor, prin cel mai operativ sistem de comunicare, despre compromiterea unor astfel de informaţii.
(2) Instiintarea prevăzută la alin. (1) se face în scopul obtinerii sprijinului necesar pentru recuperarea informaţiilor, evaluarea prejudiciilor, diminuarea şi înlăturarea consecintelor.
(3) Instiintarea 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 scurta prezentare a imprejurarilor în care a avut loc compromiterea, inclusiv data constatarii, 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, instiintarile preliminare vor fi completate pe măsura derularii cercetarilor.
(5) Documentele privind evaluarea prejudiciilor şi activităţile ce urmeaza a fi intreprinse ca urmare a compromiterii vor fi prezentate instituţiilor competente.

+ Articolul 89

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

+ Articolul 90

(1) Orice încălcare a reglementarilor de securitate va ti cercetata 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 prezinta suficienta incredere şi loialitate, astfel încât rezultatul compromiterii sa 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 savarsirii de infractiuni la protectia secretului de stat, unitatile detinatoare au obligaţia de a sesiza organele de urmărire penala şi de a pune la dispoziţia acestora datele şi materialele necesare probarii faptelor.
+ Articolul 91
(1) Structura/functionarul de securitate are obligaţia de a tine evidenta cazurilor de încălcare a reglementarilor de securitate, a documentelor de cercetare şi a masurilor de solutionare şi să le puna la dispoziţia autorităţilor desemnate de securitate, conform competentelor ce le revin.
(2) Documentele menţionate la alin. (1) se păstrează timp de cinci ani.
+ Articolul 92
Litigiile cu privire la calitatea de emitent ori detinator sau cele determinate de conţinutul informaţiilor secrete de stat, inclusiv drepturile patrimoniale ce revin emitentului din contractele de cesiune şi licenta, precum şi litigiile referitoare la nerespectarea dispoziţiilor legale privind dreptul de autor şi drepturile conexe, inventiile şi inovatiile, protectia modelelor industriale, combaterea concurentei neloiale şi a celor stipulate în tratatele, acordurile şi înţelegerile la care România este parte, sunt de competenţa instanţelor judecătorești.
+ Secţiunea a 3-a Protectia prin măsuri procedurale
+ Articolul 93
Toate unitatile care deţin informaţii secrete de stat au obligaţia sa stabileasca norme interne de lucru şi de ordine interioara destinate protectiei acestor informaţii, potrivit actelor normative în vigoare.
+ Articolul 94
(1) Masurile 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 sa coordoneze activitatea şi sa controleze masurile privitoare la protectia informaţiilor clasificate, potrivit legii.
(2) Sunt exceptate de obligativitatea prezentarii, spre avizare, a programului de prevenire a scurgerii de informaţii, mentionat la alin. (1), instituţiile prevăzute la art. 25 alin. (4) din Legea nr. 182/2002 (~/../../../Public/DetaliiDocumentAfis/35209).
+ Articolul 95
Angajamentele de confidentialitate intocmite potrivit reglementarilor în vigoare vor garanta ca informaţiile la care se acordă acces sunt protejate corespunzător.
+ Secţiunea a 4-a Protectia fizica
+ Articolul 96
Obiectivele, sectoarele şi locurile în care sunt gestionate informaţii secrete de stat trebuie protejate fizic împotriva accesului neautorizat.
+ Articolul 97
Masurile de protecţie fizica - gratii la ferestre, incuietori la uşi, paza la intrari, sisteme automate pentru supraveghere, control, acces, patrule de securitate, dispozitive de alarma, mijloace pentru detectarea observarii, ascultarii sau interceptarii - vor fi dimensionate în raport cu:
a) nivelul de secretizare a informaţiilor, volumul şi localizarea acestora;
b) tipul containerelor în care sunt depozitate informaţiile;
c) caracteristicile cladirii şi zonei de amplasare.
+ Articolul 98
Zonele în care sunt manipulate sau stocate informaţii secrete de stat trebuie organizate şi administrate în asa fel încât sa corespunda uneia din urmatoarele categorii:
a) zona de securitate clasa I, care presupune ca orice persoană aflata în interiorul acesteia are acces la informaţii secrete de stat, de nivel strict secret de importanţa deosebită şi strict secret, şi care necesita:
- 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 necesita:
- perimetru clar delimitat şi protejat, în care toate intrarile şi iesirile sunt supravegheate;
- controlul sistemului de intrare care să permită accesul neinsotit numai persoanelor verificate şi autorizate sa patrunda în aceasta zona;
- reguli de însoţire, supraveghere şi prevenire a accesului persoanelor neautorizate la informaţii clasificate.
+ Articolul 99
Incintele în care nu se lucreaza 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.
+ Articolul 100
În jurul zonelor de securitate clasa I sau clasa a II-a poate fi stabilita o zona administrativa, cu perimetru vizibil delimitat, în interiorul careia sa existe posibilitatea de control al personalului şi al vehiculelor.
+ Articolul 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 recunoastere individuala aplicat personalului.
(2) Unitatile detinatoare de informaţii secrete de stat vor institui un sistem propriu de control al vizitatorilor, destinat interzicerii accesului neautorizat al acestora în zonele de securitate.
+ Articolul 102
Permisul de acces nu va specifică, în clar, identitatea unităţii emitente sau locul în care deţinătorul are acces.

+ Articolul 103
Unitatile 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, genti şi alte tipuri de suporti în care s-ar putea transporta materiale şi informaţii secrete de stat.
+ Articolul 104
Personalul inclus în sistemul de paza şi aparare a obiectivelor, sectoarelor şi locurilor în care sunt gestionate informaţii secrete de stat trebuie să deţină autorizatie de acces corespunzător nivelului de secretizare a informaţiilor necesare indeplinirii atribuţiilor ce îi revin.
+ Articolul 105
Este interzis accesul cu aparate de fotografiat, filmat, înregistrat audio-video, de copiat din baze de date informatice sau de comunicare la distanta, în locurile în care se afla informaţii secrete de stat.
+ Articolul 106
Conducătorii unităţilor detinatoare de informaţii secrete de stat vor stabili reguli cu privire la circulatia şi ordinea interioara 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 cunoaste.
+ Articolul 107
Accesul pentru interventii tehnice, reparatii sau activităţi de deservire în locuri în care se lucreaza cu informaţii secrete de stat ori în care se păstrează, se prelucreaza sau se multiplica astfel de informaţii este permis numai angajatilor unităţii care deţin autorizaţii de acces, corespunzător celui mai înalt nivel de secretizare a informaţiilor pe care le-ar putea cunoaste.
+ Articolul 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 insemne sau echipamente specifice.
(2) În locurile şi sectoarele în care sunt gestionate informaţii secrete de stat, insemnele şi echipamentele distinctive se stabilesc prin regulamente de ordine interioara.
(3) Evidenta legitimatiilor, permiselor şi a altor insemne şi echipamente distinctive va fi ţinuta de structura/functionarul de securitate al unităţii.
+ Articolul 109
(1) Persoanele care pierd permisele de acces în unitate, insemnele sau echipamentele specifice sunt obligate sa anunte de îndată seful ierarhic.
(2) În situaţiile menţionate la alin. (1), conducatorul institutiei va dispune cercetarea imprejurarilor în care s-au produs şi va informa autoritatea desemnata de securitate competenţa.
(3) Structura/functionarul de securitate va lua masurile ce se impun pentru a preveni folosirea permiselor de acces, insemnelor sau echipamentelor specifice de către persoane neautorizate.
+ Articolul 110
Accesul fiecarui angajat al unităţii detinatoare de informaţii secrete de stat în zone de securitate clasa I sau clasa a II-a se realizează prin intrari anume stabilite, pe baza permisului de acces, semnat de conducatorul acesteia.
+ Articolul 111
(1) Permisele de acces vor fi individualizate prin aplicarea unor semne distinctive.
(2) Permisele de acces se vizeaza semestrial.
(3) La încetarea angajarii permisele de acces vor fi retrase şi anulate.
+ Articolul 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.
+ Articolul 113
Accesul persoanelor din afara unităţii în zona administrativa sau în zonele de securitate este permis numai dacă sunt insotite de persoane anume desemnate, cu bilet de intrare eliberat pe baza documentelor de legitimare de conducatorul unităţii.
+ Articolul 114
(1) Accesul angajatilor agentilor economici care efectueaza lucrari de constructii, reparatii şi întreţinere a cladirilor, instalaţiilor sau utilitatilor 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 reprezentantilor autorizati ai agentilor economici în cauza.
(2) Locurile în care se efectueaza lucrarile menţionate la alin. (1) se supraveghează de către persoane anume desemnate din unitatea beneficiara.
(3) Documentul de acces temporar are valabilitate pe durata executarii lucrărilor şi se vizeaza trimestrial, iar la terminarea activităţilor se restituie emitentului.
(4) Pierderea documentului de acces temporar va fi luata în evidenta structurii/functionarului de securitate care va dispune masurile necesare de prevenire a folosirii lui de către persoane neautorizate.
+ Articolul 115
Reprezentantii instituţiilor care, potrivit competentelor legale, au atribuţii de coordonare şi control pe linia protectiei informaţiilor clasificate au acces la obiectivele, sectoarele şi locurile în care sunt gestionate informaţii clasificate, pe baza legitimatiei de serviciu şi a delegatiei speciale, semnata de conducatorul autorităţii pe care o reprezinta.
+ Articolul 116
Persoanele aflate în practica de documentare, stagii de instruire sau schimb de experienta au acces numai în locurile stabilite de conducatorul unităţii, pe baza permiselor de acces eliberate în acest sens.
+ Articolul 117

Persoanele care solicită angajari, audiente, ori care prezinta reclamatii şi sesizari vor fi primite în afara zonelor administrative sau în locuri special amenajate, cu aprobarea conducătorului unităţii.
+ Articolul 118
În afara orelor de program şi în zilele nelucratoare, se vor organiza patrulari pe perimetrul unităţii, la intervale care vor fi stabilite prin instrucţiuni elaborate pe baza planului de paza şi aparare al obiectivului.
+ Articolul 119
(1) Sistemele de paza, supraveghere şi control-acces trebuie să asigure prevenirea patrunderii neautorizate în obiectivele, sectoarele şi locurile unde sunt gestionate informaţii clasificate.
(2) Timpul de reactie a personalului de paza şi aparare va fi testat periodic pentru a garanta interventia operativa în situaţii de urgenta.
+ Articolul 120
(1) Unitatile care gestioneaza informaţii secrete de stat vor întocmi planul de paza şi aparare a obiectivelor, sectoarelor şi locurilor care prezinta importanţa deosebită pentru protectia informaţiilor clasificate.
(2) Planul de paza şi aparare mentionat la alin. (1) va fi înregistrat potrivit celui mai înalt nivel de secretizare a informaţiilor protejate şi va cuprinde totalitatea masurilor de securitate luate pentru prevenirea accesului neautorizat la acestea.
(3) Planul de paza şi aparare 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 paza şi masurile de supraveghere a perimetrului protejat;
b) sistemul de control al accesului în zonele de securitate;
c) masurile de avertizare şi alarmare pentru situaţii de urgenta;
d) planul de evacuare a documentelor şi modul de actiune în caz de urgenta;
e) procedura de raportare, cercetare şi evidenta a incidentelor de securitate.
+ Articolul 121
Informaţiile secrete de stat se păstrează în containere speciale, astfel:
a) containere clasa A, autorizate la nivel naţional pentru pastrarea informaţiilor strict secrete de importanţa deosebită în zona de securitate clasa I;
b) containere clasa B, autorizate la nivel naţional pentru pastrarea informaţiilor strict secrete şi secrete în zone de securitate clasa I sau clasa a II-a.
+ Articolul 122
(1) Containerele din clasele A şi B vor fi construite astfel încât să asigure protectia împotriva patrunderii clandestine şi deteriorării sub orice formă a informaţiilor.
(2) Standardele în care trebuie să se incadreze containerele din clasele A şi B se stabilesc de ORNISS.
+ Articolul 123
(1) Încăperile de securitate sunt incaperile special amenajate în zone de securitate clasa I sau clasa a II-a, în care informaţiile secrete de stat pot fi pastrate pe rafturi deschise sau pot fi expuse pe harti, planse ori diagrame.
(2) Peretii, podelele, plafoanele, usile şi incuietorile incaperilor de securitate vor asigura protectia echivalenta clasei containerului de securitate aprobat pentru pastrarea informaţiilor clasificate potrivit nivelului de secretizare.
+ Articolul 124
(1) Ferestrele incaperilor de securitate dispuse la parter sau ultimul etaj vor fi protejate obligatoriu cu bare incastrate în beton sau asigurate antiefractie.
(2) În afara programului de lucru, usile incaperilor de securitate vor fi sigilate, iar sistemul de aerisire asigurat împotriva accesului neautorizat şi introducerii materialelor incendiare.
+ Articolul 125
În situaţii de urgenta, dacă informaţiile secrete de stat trebuie evacuate, se vor utiliza lazi metalice autorizate la nivel naţional din clasa corespunzătoare nivelului de secretizare a acestor informaţii.
+ Articolul 126
Incuietorile folosite la containerele şi incaperile de securitate în care sunt pastrate informaţii secrete de stat se impart în trei grupe, astfel:
a) grupa A - incuietori autorizate pentru containerele din clasa A;
b) grupa B - incuietori autorizate pentru containerele din clasa B;
c) grupa C - incuietori pentru mobilierul de birou.
+ Articolul 127
Standardele mecanismelor de inchidere, a sistemelor cu cifru şi incuietorilor, pe grupe de utilizare, se stabilesc de ORNISS.
+ Articolul 128
Cheile containerelor şi incaperilor de securitate nu vor fi scoase din zonele de securitate.
+ Articolul 129
(1) În afara orelor de program, cheile de la incaperile şi containerele de securitate vor fi pastrate în cutii sigilate, de către personalul care asigura paza şi apararea.
(2) Predarea şi primirea cheilor de la incaperile şi containerele de securitate se vor face, pe bază de semnatura, în condica special destinata - anexa nr. 11.
+ Articolul 130
(1) Pentru situaţiile de urgenta, un rand de chei suplimentare sau, după caz, o evidenta scrisa a combinatiilor incuietorilor, vor fi pastrate în plicuri mate sigilate, în containere separate, într-un compartiment stabilit de conducerea unităţii, sub control corespunzător.
(2) Evidenta fiecarei combinatii se va pastra în plic separat.

(3) Cheilor şi plicurilor cu combinatii trebuie să li se asigure acelasi nivel de protecţie ca şi informaţiilor la care permit accesul.
+ Articolul 131
Combinatiile incuietorilor de la incaperile şi containerele de securitate vor fi cunoscute de un numar restrans de persoane desemnate de conducerea unităţii.
+ Articolul 132
Cheile şi combinatiile incuietorilor vor fi schimbate:
a) ori de cate ori are loc o schimbare de personal;
b) de fiecare data când se constată că au intervenit situaţii de natura să le faca vulnerabile;
c) la intervale regulate, de preferinta o dată la şase luni, fără a se depăşi 12 luni.
+ Articolul 133
(1) Sistemele electronice de alarmare sau de supraveghere destinate protectiei informaţiilor secrete de stat vor fi prevăzute cu surse de alimentare de rezerva.
(2) Orice defectiune sau interventie neautorizata asupra sistemelor de alarma sau de supraveghere destinate protectiei informaţiilor secrete de stat trebuie să avertizeze personalul care le monitorizează.
(3) Dispozitivele de alarmare trebuie să între în functiune în cazul penetrarii peretilor, podelelor, tavanelor şi deschizaturilor, sau la miscari în interiorul incaperilor de securitate.
+ Articolul 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.
+ Articolul 135
Unitatile detinatoare de informaţii secrete de stat au obligaţia de a asigura protectia acestora împotriva ascultarilor neautorizate, pasive sau active.
+ Articolul 136
(1) Protectia împotriva ascultarii pasive a discutiilor confidentiale se realizează prin izolarea fonica a incaperilor.
(2) Protectia împotriva ascultarilor active, prin microfoane, radio-emitatori şi alte dispozitive implantate, se realizează pe baza inspecţiilor de securitate a incaperilor, accesoriilor, instalaţiilor, sistemelor de comunicatii, echipamentelor şi mobilierului de birou, realizate de unitatile specializate, potrivit competentelor legale.
+ Articolul 137
(1) Accesul în incaperile protejate împotriva ascultarilor 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 oricarei intrari neautorizate sau suspiciuni privind accesul persoanelor neautorizate şi după executarea lucrărilor de reparatii, întreţinere, zugravire sau redecorare.
(4) Nici un obiect nu va fi introdus în incaperile protejate împotriva ascultarii, fără a fi verificat în prealabil de către personalul specializat în depistarea dispozitivelor de ascultare.
+ Articolul 138
(1) În zonele în care se poarta discutii confidentiale 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 tehnica în zonele prevăzute în alin.(l) trebuie efectuate, în mod obligatoriu, inaintea începerii convorbirilor, pentru identificarea fizica a dispozitivelor de ascultare şi verificarea sistemelor telefonice, electrice sau de alta natura, care ar putea fi utilizate ca mediu de atac.
+ Articolul 139
(1) Echipamentele de comunicatii şi dotarile din birouri, în principal cele electrice şi electronice, trebuie verificate de specialisti ai autorităţilor desemnate de securitate competente, înainte de a fi folosite în zonele în care se lucreaza ori se discuta despre informaţii strict secrete sau strict secrete de importanţa 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 evidenta a tipului şi numerelor de inventar ale echipamentului şi mobilei mutate în/din interiorul incaperilor, care va fi gestionata ca material secret de stat.
+ Secţiunea a 5-a Protectia personalului
+ Articolul 140
(1) Unitatile detinatoare de informaţii secrete de stat au obligaţia de a asigura protectia personalului desemnat să asigure securitatea acestora ori care are acces la astfel de informaţii, potrivit prezentelor standarde.
(2) Masurile de protecţie a personalului au drept scop:
a) sa previna accesul persoanelor neautorizate la informaţii secrete de stat;
b) sa garanteze ca informaţiile secrete de stat sunt distribuite deţinătorilor de certificate de securitate/autorizaţii de acces, cu respectarea principiului necesităţii de a cunoaste;
c) să permită identificarea persoanelor care, prin actiunile sau inactiunile lor, pot pune în pericol securitatea informaţiilor secrete de stat şi sa previna accesul acestora la astfel de informaţii.
(3) Protectia personalului se realizează prin: selectionarea, verificarea, avizarea şi autorizarea accesului la informaţiile secrete de stat, revalidarea, controlul şi instruirea personalului, retragerea certificatului de securitate sau autorizatiei de acces.
+ Articolul 141
(1) Acordarea certificatului de securitate - anexa nr. 12 - şi autorizatiei de acces la informaţii clasificate - anexa nr. 13, potrivit nivelului de secretizare, este condiţionată de avizul autorităţii desemnate de securitate.
(2) În vederea eliberarii certificatului de securitate/autorizatiei de acces conducatorul unităţii solicita 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 mentionata 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 cauza, introduse în plic separat, sigilat.
(4) În functie de avizul comunicat de autoritatea desemnata, ORNISS va aproba eliberarea certificatului de securitate sau autorizatiei de acces şi va incunostinta oficial conducatorul unităţii.
(5) După obtinerea aprobării menţionate la alin. (4), conducatorul unităţii va notifica la ORNISS şi va elibera certificatul de securitate sau autorizatia de acces, conform art. 154.

+ Articolul 142

Certificatul de securitate sau autorizatia de acces se elibereaza numai în baza avizelor acordate de autoritatea desemnata de securitate în urma verificărilor efectuate asupra persoanei în cauza, cu acordul scris al acesteia.

+ Articolul 143

În cadrul procedurilor de avizare trebuie acordată atenţie speciala persoanelor care:
a) urmeaza să aibă acces la informaţii strict secrete şi strict secrete de importanţa deosebită;
b) ocupa functii ce presupun accesul permanent la un volum mare de informaţii secrete de stat;
c) pot fi vulnerabile la acţiuni ostile, ca urmare a importantei functiei în care vor fi numite, a mediului de relatii sau a locului de muncă anterior.

+ Articolul 144

(1) Oportunitatea avizarii va ti evaluata pe baza verificării şi investigarii biografiei celui în cauza.
(2) Când persoanele urmeaza sa indeplineasca functii 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.

+ Articolul 145

Unitatile care gestioneaza informaţii clasificate sunt obligate sa tina un registru de evidenta a certificatelor de securitate şi autorizaţiilor de acces la informaţii clasificate - anexa nr. 18.

+ Articolul 146

(1) Ori de cate ori apar indicii ca deţinătorul certificatului de securitate sau autorizatiei de acces nu mai indeplineste criteriile de compatibilitate privind accesul la informaţiile secrete de stat, verificările de securitate se reiau la solicitarea conducătorului unităţii adresata 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.

+ Articolul 147

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

+ Articolul 148

(1) Structura/functionarul de securitate are obligaţia sa puna la dispoziţia persoanei selectionate formularele tip corespunzătoare nivelului de acces pentru care se solicita eliberarea certificatului de securitate/autorizatiei de acces şi sa acorde asistenţa în vederea completarii acestora.
(2) În functie de nivelul de secretizare a informaţiilor pentru care se solicita avizul de securitate, termenele de prezentare a raspunsului de către instituţiile abilitate să efectueze verificările de securitate sunt:
a) pentru acces la informaţii strict secrete de importanţa deosebită - 90 de zile lucratoare;
b) pentru acces la informaţii strict secrete - 60 de zile lucratoare;
c) pentru acces la informaţii secrete - 30 de zile lucratoare.

+ Articolul 149

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

+ Articolul 150

(1) După primirea formularelor, institutia abilitata va efectua verificările în termenele prevăzute la art. 148 şi va comunică, în scris - anexa nr. 20, la ORNISS, avizul privind acordarea certificatului de securitate sau autorizatiei 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 protectiei informaţiilor secrete de stat, în luarea deciziei de acordare a avizului de securitate vor avea prioritate interesele de securitate.

+ Articolul 151

(1) În termen de 7 zile lucratoare de la primirea raspunsului de la autoritatea desemnata de securitate, ORNISS va decide asupra acordarii certificatului de securitate/autorizatiei de acces la informaţii secrete de stat şi va comunică 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 institutiei care a efectuat verificările.
(3) Dacă avizul este pozitiv, conducatorul unităţii solicitante va elibera certificatul de securitate sau autorizatia de acces persoanei în cauza, după notificarea prealabila la ORNISS - anexa nr. 22.

+ Articolul 152

(1) Verificarea în vederea avizarii pentru accesul la informaţii secrete de stat se efectueaza cu respectarea legislaţiei în vigoare privind responsabilitatile în domeniul protectiei unor asemenea informaţii, de către urmatoarele institutii:
a) Serviciul Roman de Informaţii, pentru:
- personalul propriu;

- personalul autorităţilor şi instituţiilor publice din zona de competenţa, potrivit legii;
- personalul agentilor economici cu capital integral sau parţial de stat şi al persoanelor juridice de drept public sau privat, altele decat cele date în competenţa instituţiilor menţionate la lit. b), c) şi d);
- personalul din cadrul Parchetului Naţional Anticoruptie.

b) Ministerul Apararii 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 strainatate;

c) Serviciul de Informaţii Externe, pentru:
- personalul militar sau civil propriu;
- personalul român al reprezentantelor diplomatice, misiunilor permanente, consulare, centrelor culturale, organismelor internationale şi altor reprezentante ale statului român în strainatate;
- cetatenii români aflati în strainatate în cadrul unor contracte, stagii de perfectionare, programe de cercetare sau în calitate de angajaţi la firme;

d) Ministerul Administraţiei şi Internelor, Serviciul de Protecţie şi Paza şi Serviciul de Telecomunicatii Speciale, pentru personalul propriu şi al persoanelor juridice a caror activitate o coordonează;

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

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

Litera a) a alin. (1) al art. 152 a fost completata cu o liniuţa de pct. 1 din HOTĂRÂREA nr. 2.202 din 30 noiembrie 2004 (~/../../../Public/DetaliiDocumentAfis/57906#?), publicată în MONITORUL OFICIAL nr. 1.225 din 20 decembrie 2004.

Litera d) a alin. (1) al art. 152 a fost modificata de pct. 2 din HOTĂRÂREA nr. 2.202 din 30 noiembrie 2004 (~/../../../Public/DetaliiDocumentAfis/57906#?), publicată în MONITORUL OFICIAL nr. 1.225 din 20 decembrie 2004.

Litera e) a alin. (1) al art. 152 a fost introdusa de pct. 3 din HOTĂRÂREA nr. 2.202 din 30 noiembrie 2004 (~/../../../Public/DetaliiDocumentAfis/57906#?), publicată în MONITORUL OFICIAL nr. 1.225 din 20 decembrie 2004.

+ Articolul 153

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

+ Articolul 154

Certificatul de securitate/autorizatia de acces se emite în doua exemplare originale, unul fiind pastrat de structura/functionarul de securitate, iar celalalt se trimite la ORNISS, care va informa institutia competenţa care a efectuat verificările.

+ Articolul 155

Valabilitatea certificatului de securitate/autorizatiei de acces eliberate unei persoane este de până la patru ani, în această perioadă verificările putand fi reluate oricand sunt indeplinite condiţiile prevăzute la art. 167.

+ Articolul 156

Pentru cadrele proprii, Ministerul Apararii Naţionale, Ministerul de Interne, Ministerul Justiţiei, Serviciul Roman de Informaţii, Serviciul de Informaţii Externe, Serviciul de Telecomunicatii Speciale şi Serviciul de Protecţie şi Paza vor elabora instrucţiuni interne privind verificarea, avizarea, eliberarea şi evidenta certificatelor de securitate/autorizaţiilor de acces.

+ Articolul 157

Decizia privind avizarea eliberarii certificatului de securitate/autorizatiei de acces va fi luata pe baza tuturor informaţiilor disponibile şi va avea în vedere:

a) loialitatea indiscutabila a persoanei;

b) caracterul, obiceiurile, relatiile şi discretia persoanei, care să ofere garantii asupra:
- corectitudinii în gestionarea informaţiilor secrete de stat;
- oportunitatii accesului neinsotit în compartimente, obiective, zone şi locuri de securitate în care se afla informaţii secrete de stat;
- respectarii reglementarilor privind protectia informaţiilor secrete de stat din domeniul sau de activitate.

+ Articolul 158

(1) Principalele criterii de evaluare a compatibilitatii în acordarea avizului pentru eliberarea certificatului de securitate/autorizatiei de acces vizeaza atât trasaturile de caracter, cat şi situaţiile sau imprejurarile din care pot rezultă riscuri şi vulnerabilitati de securitate.

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

+ Articolul 159

Urmatoarele situaţii imputabile atât solicitantului, cat şi sotului/sotiei sau concubinului/concubinei acestuia reprezinta elemente de incompatibilitate pentru acces la informaţii secrete de stat:

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

b) dacă a incercat, a sustinut, a participat, a cooperat sau a sprijinit acţiuni de spionaj, terorism ori persoane suspectate de a se incadra în această categorie sau de a fi membre ale unor organizaţii ori puteri straine inamice ordinii de drept din tara noastra;

c) dacă este sau a fost membru al unei organizaţii care a incercat, incearca sau sustine rasturnarea ordinii constitutionale prin mijloace violente, subversive sau alte forme ilegale;
d) dacă este sau a fost un sustinator al vreunei organizaţii prevăzute la lit. c), este sau a fost în relatii apropiate cu membrii unor astfel de organizaţii intr-o formă de natura sa ridice suspiciuni temeinice cu privire la increderea şi loialitatea persoanei.

+ Articolul 160

Constituie elemente de incompatibilitate pentru accesul solicitantului la informaţii secrete de stat oricare din urmatoarele situaţii:
a) dacă în mod deliberat a ascuns, a interpretat eronat sau a falsificat informaţii cu relevanta în planul sigurantei naţionale ori a mintit în completarea formularelor tip sau în cursul interviului de securitate;
b) are antecedente penale sau a fost sanctionat contraventional pentru fapte care indica tendinte infractionale;
c) are dificultati financiare serioase sau exista o discordanta semnificativa între nivelul sau de trai şi veniturile declarate;
d) consuma în mod excesiv bauturi alcoolice ori este dependent de alcool, droguri sau de alte substante interzise prin lege care produc dependenta;
e) are sau a avut comportamente imorale sau deviatii de comportament care pot genera riscul ca persoana să fie vulnerabila la santaj sau presiuni;
f) a demonstrat lipsa de loialitate, necinste, incorectitudine sau indiscretie;
g) a încălcat reglementarile privind protectia informaţiilor clasificate;
h) sufera sau a suferit de boli fizice sau psihice care îi pot cauza deficiente de discernamant confirmate prin investigatie medicală efectuata cu acordul persoanei solicitante;
i) poate fi supus la presiuni din partea rudelor sau persoanelor apropiate care ar putea genera vulnerabilitati exploatabile de către serviciile de informaţii ale caror interese sunt ostile României şi aliatilor săi.

+ Articolul 161

(1) Solicitarile pentru efectuarea verificărilor de securitate în vederea avizarii eliberarii certificatelor de securitate/autorizaţiilor de acces la informaţii secrete vor avea în vedere persoanele care:
a) în exercitarea atribuţiilor profesionale lucreaza cu date şi informaţii de nivel secret;
b) fac parte din personalul de execuţie sau administrativ şi, în virtutea acestui fapt, pot intră în contact cu date şi informaţii de acest nivel;
c) este de presupus ca vor lucra cu date şi informaţii de nivel secret, datorita functiei pe care o deţin;
d) se presupune că nu pot avansa profesional în functie, 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 baza, 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 institutiei abilitate să efectueze verificările de securitate poate avea o intrevedere cu aceasta.

+ Articolul 162

(1) Pentru eliberarea certificatelor de securitate/autorizaţiilor de acces la informaţii strict secrete se efectueaza verificări asupra persoanelor care:
a) în exercitarea atribuţiilor profesionale lucreaza cu date şi informaţii de nivel strict secret;
b) fac parte din personalul de execuţie sau administrativ şi, în virtutea acestui fapt, pot intră în contact cu date şi informaţii de acest nivel;
c) este de presupus ca vor lucra cu date şi informaţii de nivel strict secret, datorita functiei pe care o deţin;
d) se presupune că nu pot avansa profesional în functie, 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 baza 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) investigatii 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 verificata, dacă se considera ca ar putea clarifica aspecte rezultate din verificările efectuate.

+ Articolul 163

(1) Pentru eliberarea certificatelor de securitate/autorizaţiilor de acces la informaţii strict secrete de importanţa deosebită se efectueaza verificări asupra persoanelor care:
a) în exercitarea atribuţiilor profesionale lucreaza cu date şi informaţii de nivel strict secret de importanţa deosebită;
b) fac parte din personalul de execuţie sau administrativ şi, în virtutea acestui fapt, pot intră în contact cu informaţii de acest nivel.
(2) Avizarea accesului la informaţiile strict secrete de importanţa deosebită se va baza pe:
a) verificarea corectitudinii datelor menţionate în formularul de baza, formularul suplimentar şi formularul financiar, anexele nr. 15, 16 şi 17;
b) investigatii de cunoastere a conduitei şi antecedentelor la domiciliul actual şi cele anterioare, la locul de muncă actual şi la cele anterioare, precum şi la instituţiile de invatamant urmate, începând de la vârsta de 18 ani, investigatii care nu se vor limita la audierea persoanelor indicate de solicitantul avizului;
c) verificări ale mediului relational pentru a identifica existenta unor riscuri de securitate în cadrul acestuia;
d) un interviu cu persoana solicitanta, pentru a detalia aspectele rezultate din verificările efectuate;

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

+ Articolul 164

(1) Dacă în cursul verificărilor, pentru orice nivel, apar informaţii ce evidentiaza riscuri de securitate, se va realiza o verificare suplimentara, cu folosirea metodelor şi mijloacelor specifice instituţiilor cu atribuţii în domeniul sigurantei naţionale.

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

+ Articolul 165

În functie de nivelul de secretizare a informaţiilor secrete de stat la care se acordă accesul, investigatia de cunoastere a antecedentelor va avea în vedere, gradual, urmatoarele:

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

b) verificarea cazierului judiciar, în evidentele centrale şi locale ale politiei, în baza de date a Registrului Comerţului, precum şi în alte evidente;

c) stabilirea naţionalitatii persoanei şi cetateniei prezente şi anterioare;

d) confirmarea pregatirii în scolile, universităţile şi alte institutii de invatamant urmate de titular, de la implinirea varstei de 18 ani;

e) cunoasterea conduitei la locul de muncă actual şi la cele anterioare, cu referinţe obtinute din dosarele de angajare, aprecierile anuale asupra performantelor şi eficientei activităţii, ori furnizate de sefii instituţiilor, sefii de compartimente sau colegi;

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

g) cunoasterea comportarii pe timpul serviciului militar şi a modalitatii în care a fost trecut în rezerva;

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

i) solvabilitatea şi reputatia financiară a persoanei;

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

+ Articolul 166

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

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

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

+ Articolul 167

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

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

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

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

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

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

+ Articolul 168

La solicitarea revalidarii nu se elibereaza un nou certificat de securitate/autorizatie de acces, în urmatoarele situaţii:

a) în cazul în care se constata neconcordante între datele declarate în formularele tip şi cele reale;

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

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

+ Articolul 169

Pentru revalidarea accesului la informaţii secrete de stat se deruleaza aceleasi activităţi ca şi la acordarea avizului initial, verificările raportandu-se la perioada scursa de la eliberarea certificatului de securitate sau autorizatiei de acces anterioare.

+ Articolul 170

(1) Persoanele cărora li se elibereaza certificate de securitate/autorizaţii de acces vor fi instruite, obligatoriu, cu privire la protectia informaţiilor clasificate, inaintea începerii activităţii şi ori de cate ori este nevoie.

(2) Activitatea de pregatire se efectueaza planificat, în scopul prevenirii, contracararii şi eliminarii riscurilor şi amenintarilor la adresa securitatii informaţiilor clasificate.

(3) Pregătirea personalului se realizează diferentiat, potrivit nivelului de secretizare a informaţiilor la care certificatul de securitate sau autorizatia de acces permite accesul şi va fi înscrisă în fisa individuala de pregatire, care se păstrează la structura/functionarul de securitate.

(4) Toate persoanele incadrate în functii care presupun accesul la informaţii clasificate trebuie să fie instruite temeinic, atât în perioada premergatoare numirii în functie, cat şi la intervale prestabilite, asupra necesităţii şi modalitatilor de asigurare a protectiei acestor informaţii.
(5) După fiecare instruire, persoana care detine certificat de securitate sau autorizatie de acces va semna ca a luat act de conţinutul reglementarilor privind protectia informaţiilor secrete de stat.

+ Articolul 171

(1) Pregătirea personalului urmareste insusirea corecta a standardelor de securitate şi a modului de implementare eficienta a masurilor de protecţie a informaţiilor clasificate.
(2) Organizarea şi coordonarea activităţii de pregatire a structurilor/functionarilor de securitate sunt asigurate de autorităţile desemnate de securitate.

+ Articolul 172

(1) Planificarea şi organizarea activităţii de pregatire a personalului se realizează de către structura/functionarul de securitate.
(2) Autorităţile desemnate de securitate vor controla, potrivit competentelor, modul de realizare a activităţii de pregatire a personalului care acceseaza informaţii secrete de stat.

+ Articolul 173

(1) Pregătirea individuala a persoanelor care deţin certificate de securitate/autorizaţii de acces se realizează în raport cu atribuţiile profesionale.
(2) Toate persoanele care gestioneaza informaţii clasificate au obligaţia sa cunoasca reglementarile privind protectia informaţiilor clasificate şi procedurile interne de aplicare a masurilor de securitate specifice.

+ Articolul 174

(1) Pregătirea personalului se realizează sub forma de lectii, informari, prelegeri, simpozioane, schimb de experienta, seminarii, şedinţe cu caracter aplicativ şi se poate finaliza prin verificări sau certificari ale nivelului de cunoştinţe.
(2) Activităţile de pregatire vor fi organizate de structura/functionarul de securitate, conform tematicilor cuprinse în programele aprobate de conducerea unităţii.

+ Articolul 175

Certificatul de securitate sau autorizatia de acces îşi inceteaza valabilitatea şi se va retrage în urmatoarele cazuri:
a) la solicitarea ORNISS;
b) prin decizia conducătorului unităţii care a eliberat certificatul/autorizatia;
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.

+ Articolul 176

La retragerea certificatului de securitate sau autorizatiei 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.

+ Articolul 177

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

+ Secţiunea a 6-a Accesul cetatenilor straini, al cetatenilor români care au şi cetatenia 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 executa lucrari din această categorie

+ Articolul 178

Cetatenii straini, cetatenii români care au şi cetatenia altui stat, precum şi persoanele apatride pot avea acces la informaţii secrete de stat, cu respectarea principiului necesităţii de a cunoaste şi a convenţiilor, protocoalelor, contractelor şi altor înţelegeri incheiate în condiţiile legii.

+ Articolul 179

(1) Persoanele prevăzute la art. 178 vor fi verificate şi avizate conform prezentelor standarde, la solicitarea conducătorului unităţii în cadrul careia acestea urmeaza sa desfasoare activităţi care presupun accesul la informaţii secrete de stat.
(2) Conducatorul unităţii va elibera persoanelor respective o autorizatie de acces corespunzătoare nivelului de secretizare a informaţiilor la care urmeaza să aibă acces, valabila numai pentru perioada desfăşurării activităţilor comune, în baza acordului comunicat de ORNISS.

+ Articolul 180

(1) Persoanele prevăzute la art. 178 care desfăşoară activităţi de asistenţa tehnica, consultanţă, colaborare stiintifica ori specializare vor purta ecusoane distincte faţă de cele folosite de personalul propriu şi vor fi insotite permanent de persoane anume desemnate de conducerea unităţii respective.
(2) Conducatorul unităţii este obligat sa 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 gestioneaza informaţii secrete de stat.

+ Articolul 181

(1) Structura/functionarul de securitate are obligaţia de a instrui persoanele prevăzute la art. 178 în legătură cu regulile pe care trebuie să le respecte privind protectia informaţiilor secrete de stat.
(2) Autorizatia de acces se va elibera numai după insusirea reglementarilor privind protectia informaţiilor clasificate şi semnarea angajamentului de confidentialitate.

+ Articolul 182

Nerespectarea de către persoanele prevăzute la art. 178 a regulilor privind protectia informaţiilor clasificate va determina, obligatoriu, retragerea autorizatiei de acces.
+ Capitolul 5 CONDIŢIILE DE FOTOGRAFIERE, FILMARE, CARTOGRAFIERE ŞI EXECUTARE A UNOR LUCRARI DE ARTE PLASTICE IN OBIECTIVE SAU LOCURI CARE PREZINTA IMPORTANŢA DEOSEBITĂ PENTRU PROTECTIA INFORMATIILOR SECRETE DE STAT
+ Articolul 183
(1) Este interzisa fotografierea, filmarea, cartografierea sau executarea de lucrari de arte plastice pe teritoriul României, în obiective, zone sau locuri de importanţa deosebită pentru protectia informaţiilor secrete de stat, fără autorizatie speciala eliberata de către ORNISS, care va tine evidenta acestora, conform anexei nr. 23.
(2) Autorizatia speciala va fi eliberata de către ORNISS în baza avizului dat de ADS, precum şi de autorităţile sau instituţiile care au obiective, zone şi locuri de importanţa pentru protectia informaţiilor clasificate în arealul în care urmeaza să se desfăşoare activităţi de aceasta natură.
(3) Obiectivele şi mijloacele prevăzute la art. 17 din Legea nr. 182/2002 (~/../../../Public/DetaliiDocumentAfis/35209) pot fi filmate şi fotografiate de către personalul militar, pentru nevoile interne ale instituţiilor militare, pe baza aprobării scrise a ministrilor sau conducătorilor instituţiilor respective, pentru obiectivele, zonele sau locurile din competenţa lor.
+ Articolul 184
Trupele Ministerului Apararii Naţionale, Ministerului de Interne şi Serviciului Roman de Informaţii, aflate la instructie, în aplicaţii ori în interiorul obiectivelor prevăzute la art. 17 din Legea nr. 182/2002 (~/../../../Public/DetaliiDocumentAfis/35209), pot fi fotografiate sau filmate în scopuri educative şi de pregatire militara, cu aprobarea conducătorilor acestor institutii sau a imputernicitilor desemnaţi.
+ Articolul 185
Fotografierea, filmarea, cartografierea sau executarea de lucrari de arte plastice în zonele de securitate şi administrative ale unităţilor detinatoare de secrete de stat este permisa numai cu aprobarea scrisa a imputernicitilor abilitati sa atribuie niveluri de secretizare conform art. 19 din Legea 182/2002, potrivit competentelor materiale.
+ Articolul 186
(1) Cererea adresata ORNISS pentru eliberarea autorizatiei speciale de filmare, fotografiere, cartografiere sau de executare a lucrărilor de arte plastice va cuprinde, obligatoriu, menţionarea obiectului şi locului activităţii, aparatura folosita, perioada de timp în care urmeaza 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 lucratoare de la data primirii cererii. Pentru zborurile aerofotogrammetrice efectuate la scari de zbor mai mari de 1:20.000 în scopul realizării pe planuri topografice şi cadastrale, termenul este de 30 de zile lucratoare.
(3) Titularii autorizatiei speciale sunt obligati să se prezinte, inaintea începerii lucrărilor, la conducătorii instituţiilor unde acestea vor fi executate, pentru a se pune de acord cu privire la modalitatea de actiune şi verificarea aparaturii ce va fi folosita.

Alin. (2) al art. 186 a fost modificat pct. 1 al articolului unic din HOTĂRÂREA nr. 185 din 9 martie 2005 (~/../../../Public/DetaliiDocumentAfis/60231#?), publicată în MONITORUL OFICIAL nr. 247 din 24 martie 2005.
+ Articolul 187
Dacă solicitantul poseda autorizatie de nivel corespunzător obiectivului vizat, autorizatia speciala va fi eliberata în termen de 15 zile lucratoare de la data primirii solicitarii, cu respectarea principiului nevoii de a cunoaste.
+ Articolul 188
Obiectivele, zonele şi locurile în care fotografierea, filmarea, cartografierea sau executarea de lucrari de arte plastice se efectueaza numai cu autorizare vor fi marcate cu indicatoare de interdictie în acest sens, care vor fi instalate prin grija instituţiilor cărora le apartin, cu avizul de specialitate al organelor administraţiei publice locale.
+ Articolul 189
(1) Emiterea, detinerea sau folosirea de date şi documente geodezice, topo-fotogrammetrice şi cartografice, ce constituie secrete de stat, urmeaza, în privinta clasificarii, marcarii, inscriptionarii, procesarii, manipularii, evidentei, întocmirii, multiplicarii, transmiterii, pastrarii, transportului şi distrugerii acestora, regimul prevăzut de reglementarile în vigoare privitoare la protectia informaţiilor clasificate în România.
(2) Ministerele şi celelalte organe ale administraţiei publice centrale şi locale, care intocmesc 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.
+ Articolul 190.
(1) Activitatea de aerofotografiere cu camere fotogrammetrice digitale sau analogice a teritoriului României, la o scara de zbor mai mare de 1:20.000, se efectueaza pe baza autorizatiei speciale eliberate de ORNISS şi în prezenta reprezentantului Ministerului Apararii Naţionale.
(2) În vederea eliberarii autorizatiei menţionate la alin. (1), cererea adresata 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 prezenta reprezentantului Ministerului Apararii Naţionale, de către persoane juridice care indeplinesc condiţiile legale privind protectia informaţiilor clasificate.
(4) Materialele obtinute din activităţile de aerofotografiere prevăzute la alin. (1) se predau persoanelor juridice autorizate, pe bază de documente justificative, în prezenta reprezentantului Ministerului Apararii Naţionale.

(5) ORNISS tine evidenta autorizaţiilor speciale şi dispune retragerea acestora, la propunerea motivata 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 Apararii Naţionale, în termen de 30 de zile lucratoare de la primirea acestora.
(8) În termenul prevăzut la alin. (7) produsele finale rezultate în urma declasificarii se vor preda la ORNISS, prin grija reprezentantului Ministerului Apararii Naţionale, pentru a fi puse la dispoziţie beneficiarului.
(9) Se exceptează de la obligaţia indeplinirii procedurii prevăzute la alin. (1)-(8) activităţile de aerofotografiere, efectuate pe teritoriul României, la o scara de zbor mai mica sau egala cu 1:20.000.

Art. 190 a fost modificat prin pct. 2 al articolului unic din HOTĂRÂREA nr. 185 din 9 martie 2005 (~/../../../Public/DetaliiDocumentAfis/60231), publicată în MONITORUL OFICIAL nr. 247 din 24 martie 2005.

+ Capitolul 6 EXERCITAREA CONTROLULUI ASUPRA MASURILOR PRIVITOARE LA PROTECTIA INFORMATIILOR CLASIFICATE

+ Articolul 191

(1) Serviciul Roman de Informaţii, prin unitatea sa specializata, are competenţa generală de exercitare a controlului asupra modului de aplicare a masurilor de protecţie de către instituţiile publice şi unitatile detinatoare de informaţii clasificate.
(2) Activitatea de control în cadrul Ministerului Apararii Naţionale, Ministerului de Interne, Ministerului de Justiţie, Serviciului Roman de Informaţii, Serviciului de Informaţii Externe, Serviciului de Protecţie şi Paza şi Serviciului de Telecomunicatii Speciale se reglementeaza prin ordine ale conducătorilor acestor institutii, potrivit legii.
(3) Controlul privind masurile de protecţie a informaţiilor clasificate în cadrul Parlamentului, Administraţiei Prezidentiale, Guvernului şi Consiliului Suprem de Aparare a Tarii se organizeaza conform legii.
(4) Activitatea de control în cadrul reprezentantelor României în strainatate se reglementeaza şi se realizează de către Serviciul de Informaţii Externe.

+ Articolul 192

Controlul are ca scop:
a) evaluarea eficientei masurilor 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 vulnerabilitatilor existente în sistemul de protecţie a informaţiilor clasificate, care ar putea conduce la compromiterea acestor informaţii, în vederea luării masurilor de prevenire necesare;
c) luarea masurilor de remediere a deficientelor şi de perfectionare a cadrului organizatoric şi functional la nivelul structurii controlate;
d) constatarea cazurilor de nerespectare a normelor de protecţie a informaţiilor clasificate şi aplicarea sanctiunilor contraventionale sau, după caz, sesizarea organelor de urmărire penala, în situaţia în care fapta constituie infractiune;
e) informarea Consiliului Suprem de Aparare a Tarii şi Parlamentului cu privire la modul în care unitatile detinatoare de informaţii clasificate aplica reglementarile în materie.

+ Articolul 193

(1) Fiecare actiune de control se incheie printr-un document de constatare, întocmit de echipa/persoana care 1-a efectuat.
(2) În cazul în care controlul releva fapte şi disfunctionalitati de natura sa reprezinte riscuri majore de securitate pentru protectia informaţiilor clasificate va fi informat, de îndată, Consiliul Suprem de Aparare a Tarii, iar institutia controlata va dispune măsuri imediate de remediere a deficientelor constatate, va initia cercetarea administrativa şi, după caz, va aplica masurile sanctionatorii şi va sesiza organele de urmărire penala, în situaţia în care rezultă indicii ca s-ar fi produs infractiuni.

+ Articolul 194

În functie de obiectivele urmarite, controalele pot fi:
a) controale de fond, care urmaresc verificarea intregului sistem organizatoric, structural şi functional de protecţie a informaţiilor clasificate;
b) controale tematice, care vizeaza anumite domenii ale activităţii de protecţie a informaţiilor clasificate;
c) controale în situaţii de urgenta, care au ca scop verificarea unor aspecte punctuale, stabilite ca urmare a identificarii unui risc de securitate.

+ Articolul 195

În functie de modul în care sunt stabilite şi organizate, controalele pot fi:
a) planificate;
b) inopinate;
c) determinate de situaţii de urgenta.

+ Articolul 196

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

+ Articolul 197

Conducătorii unităţilor detinatoare de informaţii clasificate au obligaţia sa organizeze anual şi ori de cate ori este nevoie controale interne privind gestionarea acestora.
+ Capitolul 7 SECURITATEA INDUSTRIALA
+ Secţiunea 1 Dispozitii generale
+ Articolul 198
Prevederile prezentului capitol se vor aplica tuturor persoanelor juridice de drept public sau privat care desfăşoară ori solicita sa desfasoare 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
+ Articolul 199
În domeniul protectiei informaţiilor clasificate care fac obiectul activităţilor contractuale, ORNISS are urmatoarele atribuţii:
a) stabileste strategia de implementare unitara la nivel naţional a masurilor de protecţie a informaţiilor clasificate care fac obiectul activităţilor contractuale;
b) elibereaza autorizatia şi certificatul de securitate industriala, la cererea persoanelor juridice interesate;
c) gestioneaza, la nivel naţional, evidentele privind: persoanele juridice detinatoare de autorizaţii de securitate industriala; persoanele juridice detinatoare de certificate de securitate industriala; persoanele fizice care deţin certificate de securitate sau autorizaţii de acces eliberate în scopul negocierii sau executarii unui contract clasificat.
+ Articolul 200
În sfera lor de competenţa legala, autorităţile desemnate de securitate au urmatoarele atribuţii:
a) efectueaza verificările de securitate necesare acordarii avizului de securitate industriala, pe care îl transmite la ORNISS în vederea eliberarii autorizatiei sau, după caz, a certificatului de securitate industriala;
b) asigura asistenţa de specialitate obiectivelor industriale în vederea implementarii standardelor de securitate în domeniul protectiei informaţiilor clasificate vehiculate în cadrul activităţilor industriale;
c) desfăşoară activităţi de pregatire a personalului cu atribuţii pe linia protectiei informaţiilor clasificate, vehiculate în cadrul activităţilor industriale;
d) efectueaza verificări în situaţiile în care s-au semnalat încălcări ale reglementarilor de protecţie, distrugeri, disparitii, dezvaluiri neautorizate de informaţii clasificate, furnizate sau produse în cadrul unui contract clasificat;
e) se asigura ca fiecare obiectiv industrial, în cadrul caruia urmeaza să fie gestionate informaţii clasificate, a desemnat o structura/functionar de securitate în vederea exercitarii efective a atribuţiilor pe linia protectiei acestora, în cadrul contractelor clasificate;
f) monitorizează, în condiţiile legii, modul de asigurare a protectiei informaţiilor clasificate în procesul de negociere şi derulare a contractelor, iar în cazul în care constata factori de risc şi vulnerabilitati, informeaza imediat ORNISS şi propune masurile necesare;
g) avizeaza programele de prevenire a scurgerii informaţiilor clasificate din obiectivele industriale, anexele de securitate ale contractelor clasificate şi monitorizează respectarea prevederilor acestora;
h) efectueaza controale de securitate şi informeaza ORNISS asupra concluziilor rezultate;
i) verifica şi prezinta ORNISS propuneri de solutionare a sesizarilor, reclamatiilor şi observatiilor referitoare la modul de aplicare şi respectare a standardelor de protecţie în cadrul contractelor clasificate.
+ Secţiunea a 3-a Protectia informaţiilor clasificate care fac obiectul activităţilor contractuale
+ Articolul 201
(1) Clauzele şi procedurile de protecţie vor fi stipulate în anexa de securitate a fiecarui contract clasificat, care presupune acces la informaţii clasificate.
(2) Anexa de securitate prevăzută la alin. (1) va fi întocmită de partea contractantă detinatoare 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 desemnata de securitate competenţa.
+ Articolul 202
Partea contractantă detinatoare de informaţii clasificate ce vor fi utilizate în derularea unui contract este responsabila pentru clasificarea şi definirea tuturor componentelor acestuia, în conformitate cu normele în vigoare, sens în care poate solicita sprijin de la ADS, conform competentelor materiale stabilite prin lege.
+ Articolul 203
La clasificarea contractelor se vor aplica urmatoarele reguli generale:
a) în toate stadiile de planificare şi execuţie, contractul se clasifica pe niveluri corespunzătoare, în functie de conţinutul informaţiilor;
b) clasificarile 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 functie de nivelul cel mai înalt al informaţiilor, iar masurile 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 aproba de conducatorul persoanei juridice care a autorizat clasificarea initiala.
+ Articolul 204
În cazul în care apare necesitatea protejarii informaţiilor dintr-un contract care, anterior, nu a fost necesar a fi clasificat, contractorul are obligaţia declanşării procedurilor de clasificare şi protejare conform reglementarilor în vigoare.
+ Articolul 205

În cazul în care contractantul cedeaza unui subcontractant realizarea unei părţi din contractul clasificat, se va asigura ca acesta detine autorizatie sau certificat de securitate industriala şi este obligat sa instiinteze contractorul, iar la incheierea subcontractului sa prevada clauze şi proceduri de protecţie în conformitate cu prevederile prezentelor standarde.

+ Articolul 206

(1) În procesul de negociere a unui contract clasificat pot participa doar reprezentanti autorizati ai obiectivelor industriale care deţin autorizatie de securitate industriala eliberata de către ORNISS, care va tine evidenta acestora.

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

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

+ Articolul 207

(1) Invitatiile la licitatii sau prezentari de oferte, în cazul contractelor clasificate, trebuie să conţină o clauza prin care potentialul ofertant este obligat sa inapoieze documentele clasificate care i-au fost puse la dispoziţie, în cazul în care nu depune oferta până la data stabilita sau nu castiga competitia 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 sa pastreze confidentialitatea informaţiilor la care a avut acces.

+ Articolul 208

Contractorul păstrează evidenta tuturor participantilor la intalnirile de negociere, datele de identificare ale acestora şi angajamentele de confidentialitate, organizaţiile pe care le reprezinta, tipul şi scopul intalnirilor, precum şi informaţiile la care acestia au avut acces.

+ Articolul 209

Contractantii care intenţionează sa deruleze activităţi industriale cu subcontractanti sunt obligati să respecte procedurile prevăzute în acest capitol.

+ Articolul 210

Contractantul şi subcontractantii sunt obligati sa implementeze şi să respecte toate masurile de protecţie a informaţiilor clasificate puse la dispoziţie sau care au fost generate pe timpul derularii contractelor.

+ Articolul 211

Autorităţile desemnate de securitate vor verifica, potrivit competentelor, dacă obiectivul industrial indeplineste urmatoarele cerinţe:

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

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

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

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

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

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

g) nu utilizeaza în alte scopuri decat cele specifice contractului informaţiile clasificate la care are acces, fără permisiunea scrisa a emitentului;

h) inapoiaza toate informaţiile clasificate ce i-au fost încredinţate, precum şi pe cele generate pe timpul derularii contractului, cu excepţia cazului în care asemenea informaţii au fost distruse autorizat sau pastrarea lor a fost autorizata de către contractor pentru o perioadă de timp strict determinata;

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

+ Articolul 212

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

+ Articolul 213

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

a) ORNISS a emis certificatul de securitate industriala;

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

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

+ Secţiunea a 4-a Procedura de verificare, avizare şi certificare a obiectivelor industriale care negociaza şi deruleaza contracte clasificate

+ Articolul 214

Verificarea, avizarea şi eliberarea autorizatiei şi certificatului de securitate industriala reprezinta 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, incheiate cu detinatorii unor astfel de informaţii.

+ Articolul 215

(1) Pentru participarea la negocieri în vederea incheierii unui contract clasificat, conducatorul obiectivului industrial adreseaza ORNISS o cerere pentru eliberarea autorizatiei de securitate industriala - anexa nr. 24, la care anexeaza chestionarul de securitate industriala - anexa nr. 25.
(2) După obtinerea avizului de la autoritatea desemnata de securitate competenţa, ORNISS elibereaza autorizatia de securitate industriala - anexa nr. 28.
(3) Evidenta autorizaţiilor de securitate industriala eliberate potrivit alin. (2) se realizează conform anexei nr. 31.

+ Articolul 216

(1) Pentru derularea contractelor clasificate, ORNISS elibereaza obiectivelor industriale, certificate de securitate industriala - anexa nr. 29.
(2) Procedura de avizare a eliberarii certificatului de securitate industriala se realizează pe baza cererii pentru eliberarea certificatului de securitate industriala - anexa nr. 30, chestionarului de securitate - anexele nr. 26 şi 27 şi a copiei anexei de securitate mentionata la art. 201.
(3) ORNISS va tine evidenta certificatelor de securitate industriala potrivit anexei nr. 32.

+ Articolul 217

Activitatea de verificare în vederea eliberarii autorizatiei şi a certificatelor de securitate trebuie să asigure indeplinirea urmatoarelor obiective principale:
a) prevenirea accesului persoanelor neautorizate la informaţii clasificate;
b) garantarea ca informaţiile clasificate sunt distribuite pe baza existentei certificatului de securitate industriala şi a principiului necesităţii de a cunoaste;
c) identificarea persoanelor care, prin actiunile lor, pot pune în pericol protectia informaţiilor clasificate şi interzicerea accesului acestora la astfel de informaţii;
d) garantarea faptului ca obiectivele industriale au capacitatea de a proteja informaţiile clasificate în procesul de negociere, respectiv de derulare a contractului.

+ Articolul 218

(1) Pentru a i se elibera autorizatia şi certificatul de securitate, obiectivul industrial trebuie să indeplineasca urmatoarele cerinţe:
a) sa posede program de prevenire a scurgerii de informaţii clasificate, avizat conform reglementarilor în vigoare;
b) să fie stabil din punct de vedere economic;
c) sa nu fi înregistrat o greseala de management cu implicatii grave asupra stării de securitate a informaţiilor clasificate pe care le gestioneaza;
d) sa fi respectat oblibaţiile 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) Neindeplinirea cerințelor menţionate la alin. (1), precum şi furnizarea intentionata a unor informaţii inexacte în completarea chestionarului sau în documentele prezentate în vederea certificării constituie elemente de incompatibilitate în procesul de eliberare a autorizatiei sau certificatului de securitate industriala.

+ Articolul 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 afla în procedura reorganizarii judiciare sau a falimentului;
c) este implicat într-un litigiu care îi afectează stabilitatea economica;
d) nu îşi indeplineste oblibaţiile financiare către stat;
e) nu şi-a indeplinit la timp, în mod sistematic, oblibaţiile financiare către persoane fizice sau juridice.

+ Articolul 220

(1) Un obiectiv industrial nu corespunde din punct de vedere al protectiei informaţiilor clasificate dacă se constată că prezinta riscuri de securitate.
(2) Sunt considerate riscuri de securitate:
a) derularea unor activităţi ce contravin intereselor de siguranţă naţionala sau angajamentelor pe care România şi le-a asumat în cadrul acordurilor bilaterale sau multinationale;
b) relatiile cu persoane fizice sau juridice straine 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.

+ Articolul 221

(1) Pentru eliberarea autorizatiei sau certificatului de securitate industriala, solicitantul va transmite la ORNISS urmatoarele documente:
a) cererea de eliberare a autorizatiei, respectiv a certificatului de securitate industriala;
b) chestionarul de securitate completat, introdus într-un plic separat, sigilat.
(2) Pentru eliberarea certificatului de securitate industriala, solicitantul va atasa şi o copie a anexei de securitate.

+ Articolul 222

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

+ Articolul 223

Avizul de securitate eliberat de autoritatea desemnata de securitate competenţa trebuie să garanteze ca:
a) agentul economic nu prezinta riscuri de securitate;
b) sunt aplicate în mod corespunzător masurile de securitate fizica, prevăzute de reglementarile 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, miscari, grupari de persoane straine sau autohtone care au adoptat sau adopta o politica de sprijinire sau aprobare a comiterii de acte de sabotaj, subversive sau teroriste.

+ Articolul 224

Verificările de securitate se realizează astfel:
a) verificarea de securitate de nivel I - pentru eliberarea avizului necesar autorizatiei de securitate industriala;
b) verificarea de securitate de nivel II - pentru eliberarea avizului necesar certificatului de securitate industriala de nivel secret;
c) verificarea de securitate de nivel III - pentru eliberarea avizului necesar certificatului de securitate industriala de nivel strict secret;
d) verificarea de securitate de nivel IV - pentru eliberarea avizului necesar certificatului de securitate industriala de nivel strict secret de importanţa deosebită.

+ Articolul 225

În cadrul verificării de securitate se desfăşoară urmatoarele activităţi:
(1) Pentru verificările de securitate de nivel I:
a) verificarea corectitudinii datelor consemnate în chestionarul de securitate industriala, 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 fiecarei persoane cu putere de decizie - asociaţi/actionari, administratori, persoanele din comitetul director şi structura de securitate - ori executiva implicata în negocierea contractului clasificat;
d) verificarea datelor minime referitoare la bonitatea şi stabilitatea economica a obiectivului industrial - domeniu şi obiect de activitate, statut juridic, actionari, garantii bancare.
(2) Pentru verificările de securitate de nivel II:
a) verificarea corectitudinii datelor consemnate în chestionarul de securitate industriala - anexa nr. 26;
b) evaluarea statutului de securitate a fiecarei persoane cu putere de decizie - asociaţi/actionari, administratori, persoanele din comitetul director şi structura de securitate - ori executiva implicata în derularea contractului clasificat;
c) verificarea unor date minime referitoare la bonitatea şi stabilitatea economica a obiectivului industrial - domeniu şi obiect de activitate, statut juridic, actionari, garantii bancare;
d) verificarea modului de implementare şi de aplicare a normelor şi masurilor de securitate fizica, 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 industriala - anexa nr. 27;
b) evaluarea statutului de securitate a fiecarei persoane cu putere de decizie - asociaţi/actionari, administratori, persoanele din comitetul director şi structura de securitate - ori executiva implicata în derularea contractului clasificat, precum şi a celor desemnate sa participe la activităţile de negociere a acestuia;
c) verificarea datelor referitoare la bonitatea şi stabilitatea economica a agentului economic - domeniu şi obiect de activitate, statut juridic, actionari, garantii bancare - incluzând şi aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;
d) verificarea existentei autorizarii sistemului informatic şi de comunicatii propriu, pentru nivelul strict secret;
e) verificarea modului de implementare şi de aplicare a normelor şi masurilor de securitate fizica, de securitate a personalului şi a documentelor, prevăzute pentru nivelul strict secret;
f) discutii cu proprietarii, membrii consiliului director, funcţionarii de securitate, angajatii, în vederea clarificarii datelor rezultate din chestionar, după caz.
(4) Pentru verificarea de securitate de nivel IV:
a) verificarea corectitudinii datelor consemnate în chestionarul de securitate industriala - anexa nr. 27;
b) evaluarea statutului de securitate a fiecarei persoane cu putere de decizie - asociaţi/actionari, administratori, persoanele din comitetul director şi structura de securitate - ori executiva implicata în derularea contractului clasificat;
c) verificarea informaţiilor detaliate referitoare la bonitatea şi stabilitatea economica a agentului economic - domeniu şi obiect de activitate, statut juridic, actionari, garantii bancare - incluzând şi aspecte referitoare la sucursale, filiale, firme la care este asociat, date financiare;
d) verificarea existentei autorizarii sistemului informatic şi de comunicatii propriu, pentru nivel strict secret de importanţa deosebită;
e) verificarea modului de implementare şi de aplicare a normelor şi masurilor de securitate fizica, de securitate a personalului şi a documentelor, prevăzute pentru nivelul strict secret de importanţa deosebită;
f) discutii cu proprietarii, membrii consiliului director, funcţionarii de securitate, angajatii, în vederea clarificarii datelor rezultate din chestionar, după caz.

+ Articolul 226

În cazul unui obiectiv industrial la al cărui management/actionariat participa cetăţeni straini, cetăţeni români care au şi cetatenia altui stat sau/şi persoane apatride, ORNISS, împreună cu ADS competenţa, va evalua măsura în care interesul strain ar putea reprezenta o amenintare la adresa protectiei informaţiilor secrete de stat, care vor fi încredinţate acelui obiectiv industrial.

+ Articolul 227

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

+ Articolul 228

În vederea desfăşurării procedurilor de avizare, obiectivul industrial are obligaţia de a permite accesul reprezentantilor 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.
+ Articolul 229
(1) Dacă în urma verificării de securitate se constată că sunt indeplinite cerinţele de securitate necesare asigurarii protectiei la nivelul de clasificare corespunzător informaţiilor vehiculate în cadrul contractului clasificat, ORNISS elibereaza şi transmite obiectivului industrial autorizatia sau certificatul de securitate industriala.
(2) Dacă se constată că obiectivul industrial nu indeplineste condiţiile de securitate necesare, ORNISS nu elibereaza autorizatia sau certificatul de securitate industriala şi informeaza obiectivul industrial în acest sens. ORNISS nu este obligat să prezinte motivele refuzului. Refuzul eliberarii autorizatiei sau certificatului de securitate industriala 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 securitatii, în luarea deciziei de eliberare a autorizatiei sau certificatului de securitate industriala vor avea prioritate interesele de securitate.
+ Articolul 230
În termen de 7 zile lucratoare de la primirea avizului de securitate din partea autorităţilor desemnate de securitate, ORNISS va elibera autorizatia sau certificatul de securitate industriala ori, după caz, va comunică obiectivului industrial refuzul eliberarii acestora.
+ Articolul 231
Obiectivul industrial are obligaţia de a comunică ORNISS toate modificările survenite privind datele de securitate incluse în chestionarul completat, pe întreaga durata de valabilitate a autorizatiei sau certificatului de securitate industriala.
+ Articolul 232
Termenele pentru eliberarea autorizatiei sau certificatului de securitate industriala sunt:
a) pentru autorizatia de securitate industriala - 60 de zile lucratoare;
b) pentru certificat de securitate industriala de nivel secret - 90 de zile lucratoare;
c) pentru certificat de securitate industriala de nivel strict secret - 120 de zile lucratoare;
d) pentru certificat de securitate industriala de nivel strict secret de importanţa deosebită - 180 de zile lucratoare.
+ Articolul 233
(1) Autorizatia de securitate are valabilitate până la incheierea contractului sau până la retragerea de la negocieri.
(2) Dacă în perioada mentionata la alin. (1) contractul clasificat care a facut obiectul negocierilor este adjudecat, contractantul este obligat să solicite la ORNISS eliberarea certificatului de securitate industriala.
(3) Termenul de valabilitate al certificatului de securitate industriala este determinat de perioada derularii contractului clasificat, dar nu mai mult de 3 ani, după care contractantul este obligat să solicite revalidarea acestuia.
+ Articolul 234
În situaţia în care ORNISS decide retragerea autorizatiei sau certificatului de securitate industriala va instiinta contractantul, contractorul şi autoritatea desemnata de securitate competenţa.
+ Articolul 235
Autorizatia sau certificatul de securitate industriala se retrage de ORNISS în urmatoarele cazuri:
a) la solicitarea obiectivului industrial;
b) la propunerea motivata a autorităţii desemnate de securitate competente;
c) la expirarea termenului de valabilitate;
d) la încetarea contractului;
e) la schimbarea nivelului de certificare acordat initial.
+ Capitolul 8 PROTECTIA SURSELOR GENERATOARE DE INFORMATII - INFOSEC
+ Secţiunea 1 Dispozitii generale
+ Articolul 236
Modalitatile şi masurile de protecţie a informaţiilor clasificate care se prezinta în format electronic sunt similare celor pe suport de hartie.
+ Articolul 237
Termenii specifici, folositi în prezentul capitol, cu aplicabilitate în domeniul INFOSEC, se definesc după cum urmeaza:
- INFOSEC - ansamblul masurilor şi structurilor de protecţie a informaţiilor clasificate care sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatice de comunicatii şi al altor sisteme electronice, împotriva amenintarilor şi a oricăror acţiuni care pot aduce atingere confidentialitatii, integritatii, disponibilităţii autenticităţii şi nerepudierii informaţiilor clasificate precum şi afectarea funcţionarii sistemelor informatice, indiferent dacă acestea apar accidental sau intentionat. Masurile INFOSEC acopera securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografica, precum şi depistarea şi prevenirea amenintarilor 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 forma de curenti, tensiuni sau camp electromagnetic, în eter sau în retele de comunicatii;
- sistemul de prelucrare automata a datelor - SPAD - ansamblul de elemente interdependente în care se includ: echipamentele de calcul, produsele software de baza şi aplicative, metodele, procedeele şi, dacă este cazul, personalul, organizate astfel încât să asigure indeplinirea functiilor de stocare, prelucrare automata şi

transmitere a informaţiilor în format electronic, şi care se afla 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 asigurarii unui nivel corespunzător de protecţie pentru informaţiile clasificate care urmeaza a fi stocate sau procesate într-un SPAD, sunt:
- functii şi caracteristici hardware/firmware/software;
- proceduri de operare şi moduri de operare;
- proceduri de evidenta;
- controlul accesului;
- definirea zonei de operare a SPAD;
- definirea zonei de operare a posturilor de lucru/a terminalelor la distanta;
- restrictii impuse de politica de management;
- structuri fizice şi dispozitive;
- mijloace de control pentru personal şi comunicatii;
- retele de transmisii de date - RTD - ansamblul de elemente interdependente în care se includ: echipamente, programe şi dispozitive de comunicatie, tehnica de calcul hardware şi software, metode şi proceduri pentru transmisie şi receptie de date şi controlul retelei, precum şi, dacă este cazul, personalul aferent. Toate acestea sunt organizate astfel încât să asigure indeplinirea functiilor de transmisie a informaţiilor în format electronic între doua sau mai multe SPAD sau să permită interconectarea cu alte RTD-uri. O RTD poate utiliza serviciile unuia sau mai multor sisteme de comunicatii; mai multe RTD pot utiliza serviciile unuia şi aceluiasi sistem de comunicatii.
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 locala - retea de transmisii de date care interconecteaza mai multe computere sau echipamente de retea, situate în acelasi perimetru;
- sistemul informatic şi de comunicatii - SIC - ansamblu informatic prin intermediul caruia se stocheaza, se proceseaza şi se transmit informaţii în format electronic, alcătuit din cel puţin un SPAD, izolat sau conectat la o RTD. Poate avea o configuratie complexa, formata din mai multe SPAD-uri şi/sau RTD-uri interconectate;
- securitatea SPAD, RTD şi SIC - aplicarea masurilor 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 neautorizata cu mijloace electronice, precum şi invalidarea de servicii sau functii, prin mijloace specifice;
- confidentialitatea - asigurarea accesului la informaţii clasificate numai pe baza certificatului de securitate al persoanei, în acord cu nivelul de secretizare a informatiei accesate şi a permisiunii rezultate din aplicarea principiului nevoii de a cunoaste;
- integritatea - interdictia modificarii - prin stergere sau adaugare - ori a distrugerii în mod neautorizat a informaţiilor clasificate;
- disponibilitatea asigurarea condiţiilor necesare regasirii şi folosirii cu usurinta, ori de cate ori este nevoie, cu respectarea stricta a condiţiilor de confidentialitate şi integritate a informaţiilor clasificate;
- autenticitatea - asigurarea posibilităţii de verificare a identităţii pe care un utilizator de SPAD sau RTD pretinde ca o are;
- nerepudierea - măsura prin care se asigura faptul ca, după emiterea/receptionarea unei informaţii într-un sistem de comunicatii securizat, expeditorul/destinatarul nu poate nega, în mod fals, ca a expediat/primit informaţii;
- risc de securitate - probabilitatea ca o amenintare 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 continua de stabilire şi mentinere a unui nivel de securitate în domeniul tehnologiei informatiei şi comunicatiilor - TIC - intr-o unitate, în sensul că, pornind de la analiza de risc, identifica şi evalueaza amenintarile şi vulnerabilitatile şi propune aplicarea masurilor adecvate de contracarare, proiectate la un pret de cost corelat cu consecintele care ar decurge din divulgarea, modificarea sau stergerea informaţiilor care trebuie protejate;
- regula celor doi - obligativitatea colaborarii a doua persoane pentru indeplinirea unei activităţi specifice;
- produs informatic de securitate - componenta de securitate care se incorporeaza într-un SPAD sau RTD - SIC şi care serveste la sporirea sau asigurarea confidentialitatii, integritatii, disponibilităţii, autenticităţii şi nerepudierii informaţiilor stocate, procesate sau transmise;
- securitatea calculatoarelor - COMPUSEC - aplicarea la nivelul fiecarui calculator a facilitatilor de securitate hardware, software şi firmware, pentru a preveni divulgarea, manevrarea, modificarea sau stergerea neautorizata a informaţiilor clasificate ori invalidarea neautorizata a unor functii;
- securitatea comunicatiilor - COMSEC - aplicarea masurilor de securitate în telecomunicatii, cu scopul de a proteja mesajele dintr-un sistem de telecomunicatii, care ar putea fi interceptate, studiate, analizate şi, prin reconstituire, pot conduce la dezvaluiri de informaţii clasificate.
COMSEC reprezinta ansamblul de proceduri, incluzând :
a) măsuri de securitate a transmisiilor;
b) măsuri de securitate împotriva radiatiilor - TEMPEST;
c) măsuri de acoperire criptologica;
d) măsuri de securitate fizica, procedurala, de personal şi a documentelor;

e) măsuri COMPUSEC;
- TEMPEST - ansamblul masurilor de testare şi de realizare a securitatii împotriva scurgerii de informaţii, prin intermediul emisiilor electromagnetice parazite;
- evaluarea - examinarea detaliata, din punct de vedere tehnic şi functional, a aspectelor de securitate ale SPAD şi RTD - SIC sau a produselor de securitate, de către o autoritate abilitata în acest sens.
Prin procesul de evaluare se verifica:
a) prezenta facilitatilor/functiilor de securitate cerute;
b) absenta efectelor secundare compromitatoare care ar putea decurge din implementarea facilitatilor de securitate;
c) functionalitatea globală a sistemului de securitate;
d) satisfacerea cerinţelor de securitate specifice pentru un SPAD şi RTD - SIC;
e) stabilirea nivelului de incredere al SPAD sau RTD - SIC ori al produselor informatice de securitate implementate;
f) existenta performantelor de securitate ale produselor informatice de securitate instalate în SPAD sau RTD-SIC;
- certificarea - emiterea unui document de constatare, la care se ataseaza unul de analiza, în care sunt prezentate modul în care a decurs evaluarea şi rezultatele acesteia, în documentul de constatare se menţionează masurile în care SPAD şi RTD - SIC satisfac cerinţele de securitate, precum şi măsura în care produsele informatice de securitate raspund exigentelor referitoare la protectia informaţiilor clasificate în format electronic;
- acreditarea - etapa de acordare a autorizarii şi aprobării unui SPAD sau RTD - SIC de a prelucra informaţii clasificate, în spatiul/mediul operational 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 urmatoarele:
a) nota justificativa despre obiectivul acreditarii sistemului, nivelul/nivelurile de clasificare a informaţiilor care urmeaza să fie procesate şi vehiculate; modul/modurile de operare protejata propuse;
b) nota justificativa despre managementul riscurilor - modul de tratare, gestionare şi rezolvare a riscurilor - în care se specifică pericolele şi punctele vulnerabile, precum şi masurile adecvate de contracarare a acestora;
c) o descriere detaliata a facilitatilor de securitate şi a procedurilor propuse, destinate SPAD sau RTD - SIC. Aceasta descriere va reprezenta elementul esential 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 securitatii SPAD sau RTD - SIC;
f) certificatul şi, acolo unde este necesar, elemente de acreditare suplimentare;
- zona SPAD - reprezinta o zona de lucru în care se gasesc şi opereaza unul sau mai multe calculatoare, unităţi periferice locale şi de stocare, mijloace de control şi echipament specific de retea şi de comunicatii. Zona SPAD nu include zona în care sunt amplasate terminale, echipamente periferice sau statii de lucru la distanta, chiar dacă aceste echipamente sunt conectate la echipamentul central de calcul din zona SPAD;
- zona terminal/statie de lucru la distanta - reprezinta o zona, separata de zona SPAD, în care se gasesc :
a) elemente de tehnica de calcul;
b) echipamentele periferice locale, terminale sau statii de lucru la distanta, conectate la echipamentele din zona SPAD;
c) echipamente de comunicatii;
- amenintarea - posibilitatea de compromitere accidentala sau deliberata a securitatii SPAD sau RTD -SIC, prin pierderea confidentialitatii, a integritatii sau disponibilităţii informaţiilor în format electronic sau prin afectarea functiilor care asigura autenticitatea şi nerepudierea informaţiilor;
- vulnerabilitatea - slabiciune sau lipsa de control care ar putea permite sau facilita o manevră tehnica, procedurala sau operationala, prin care se ameninta o valoare sau ţinta specifică.

+ Articolul 238

Abrevierile utilizate în prezentul capitol semnifica:
a) CSTIC - componenta de securitate pentru tehnologia informatiei şi comunicatiilor instituita în unitatile detinatoare de informaţii clasificate;
b) TIC - tehnologia informatiei şi comunicatiilor;
c) CSS - cerinţele de securitate specifice.

+ Articolul 239

(1) Informaţiile care se prezinta 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, hartie perforata 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.

+ Articolul 240

(1) Sistemele SPAD şi RTD - SIC au dreptul sa stocheze, sa proceseze sau sa transmita informaţii clasificate, numai dacă sunt autorizate potrivit prezentei hotărâri.
(2) În vederea autorizarii SPAD şi RTD - SIC unitatile vor întocmi, cu aprobarea organelor lor de conducere, strategia proprie de securitate, în baza careia vor implementa sisteme proprii de securitate, care vor include utilizarea de produse specifice tehnologiei informatiei şi comunicatiilor, personal instruit şi măsuri de protecţie a informatiei, incluzând controlul accesului la sistemele şi serviciile informatice şi de comunicatii, pe baza principiului necesităţii de a cunoaste şi al nivelului de secretizare atribuit.

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

+ Articolul 241

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

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

b) o agentie care elaboreaza şi implementeaza metode, mijloace şi măsuri de securitate;

c) o agentie responsabila cu protectia criptografica.

(2) Agentiile menţionate la alin. (1) sunt subordonate institutiei desemnate la nivel naţional, pentru protectia informaţiilor clasificate, ORNISS.

(3) Masurile de protecţie a informaţiilor clasificate în format electronic trebuie reactualizate permanent, prin depistare, documentare şi gestionare a amenintarilor şi vulnerabilitatilor la adresa informaţiilor clasificate şi sistemelor care le prelucreaza, stocheaza şi transmit.

+ Articolul 242

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

+ Articolul 243

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

+ Articolul 244

(1) În fiecare unitate care administreaza SPAD şi RTD - SIC în care se stocheaza, se proceseaza sau se transmit informaţii clasificate, se va institui o componenta de securitate pentru tehnologia informatiei şi a comunicatiilor - CSTIC, în subordinea structurii/functionarului de securitate.

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

(3) CSTIC indeplineste atribuţii privind:

a) implementarea metodelor, mijloacelor şi masurilor necesare protectiei informaţiilor în format electronic;

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

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

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

(4) CSTIC reprezinta punctul de contact al agentiilor competente cu unitatile care deţin în administrare SPAD sau RTD - SIC şi, după caz, poate fi investita, temporar, de către aceste agentii, cu unele dintre atribuţiile lor.

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

+ Articolul 245

CSTIC se instituie la nivelul fiecarei SPAD şi RTD - SIC şi reprezinta persoana sau compartimentul cu responsabilitatea delegata de către agentia de securitate pentru informatica şi comunicatii de a implementa metodele, mijloacele şi masurile de securitate şi de a exploata SPAD şi RTD - SIC în condiţii de securitate.

+ Articolul 246

CSTIC este condusa de către functionarul de securitate TIC şi are în compunere administratorii de securitate şi, după caz, şi alti specialisti din SPAD sau RTD - SIC. Toata structura CSTIC face parte din personalul unităţii care administreaza SPAD sau RTD - SIC.

+ Articolul 247

Exercitarea atribuţiilor CSTIC trebuie să cuprindă intregul ciclu de viaţa al SPAD sau RTD - SIC, începând cu proiectarea, continuand cu elaborarea specificatiilor, testarea instalarii, acreditarea, testarea periodica în vederea reacreditarii, exploatarea operationala, modificarea şi incheind cu scoaterea din uz. în anumite situaţii, rolul CSTIC poate fi preluat de către alte componente ale unităţii, în decursul ciclului de viaţa.

+ Articolul 248

CSTIC mijloceste cooperarea dintre conducerea unităţii careia îi aparţine SPAD sau RTD - SIC şi agentia pentru acreditare de securitate, atunci când unitatea:

a) planifica dezvoltarea sau achizitia de SPAD sau RTD;

b) propune schimbari ale unei configuratii de sistem existente;

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

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

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

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

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

+ Articolul 249

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

+ Articolul 250
CSTIC stabileste, pentru structurile de securitate şi management ale SPAD şi RTD - SIC, inca de la înfiinţare, responsabilitatile pe care le vor exercita pe tot ciclul de viaţa al SPAD şi RTD - SIC respective.
+ Articolul 251
Activitatea INFOSEC din SPAD şi RTD - SIC, desfăşurată de către CSTIC, trebuie condusa şi coordonata de persoane care deţin certificat de securitate corespunzător, cu pregatire de specialitate în domeniul sistemelor TIC precum şi al securitatii acestora, obtinuta în institutii de invatamant acreditate INFOSEC, sau care au lucrat în domeniu cel puţin 5 ani.
+ Articolul 252
Protectia SPAD şi RTD - SIC din compunerea sistemelor de armament şi de detectie va fi definita 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. Agentia de acreditare de securitate
+ Articolul 253
Agentia de acreditare de securitate este subordonata institutiei desemnate la nivel naţional pentru protectia informaţiilor clasificate, are reprezentanti delegaţi din cadrul ADS implicate, în functie de SPAD şi RTD - SIC care trebuie acreditate, şi indeplineste urmatoarele atribuţii principale:
a) asigura, la nivel naţional, acreditarea de securitate şi reacreditarea SPAD şi RTD - SIC care stocheaza, proceseaza sau transmit informaţii clasificate, în functie de nivelul de clasificare a acestora;
b) asigura evaluarea şi certificarea sistemelor SPAD şi RTD - SIC sau a unor elemente componente ale acestora;
c) stabileste criteriile de acreditare de securitate pentru SPAD şi RTD - SIC.
+ Articolul 254
Agentia de acreditare de securitate îşi exercită atribuţiile în domeniul INFOSEC în numele institutiei desemnate la nivel naţional pentru protectia informaţiilor clasificate şi are responsabilitatea de a impune standarde de securitate în acest domeniu.
B. Agentia de securitate pentru informatica şi comunicatii
+ Articolul 255
Agentia de securitate pentru informatica şi comunicatii este structura subordonata institutiei desemnate la nivel naţional pentru protectia informaţiilor electronice clasificate, având reprezentanti delegaţi din cadrul ADS implicate care acţionează la nivel naţional.
+ Articolul 256
Agentia este responsabila 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, urmatoarele atribuţii:
a) coordonează activităţile de protecţie a informaţiilor clasificate care sunt stocate, procesate sau transmise prin intermediul SPAD şi RTD - SIC;
b) elaboreaza şi promovează reglementari şi standarde specifice;
c) analizeaza cauzele incidentelor de securitate şi gestioneaza baza de date privind amenintarile şi vulnerabilitatile din sistemele de comunicatie şi informatice, necesare pentru elaborarea managementul de risc;
d) semnaleaza agentiei de acreditare de securitate incidentele de securitate în domeniu;
e) integreaza masurile privind protectia fizica, de personal, a documentelor administrative, COMPUSEC, COMSEC, TEMPEST şi criptografica;
f) executa inspecţii periodice asupra SPAD şi RTD - SIC în vederea reacreditarii;
g) supune certificării şi autorizarii sistemele de securitate specifice SPAD şi RTD - SIC.
+ Articolul 257
Pentru indeplinirea atribuţiilor sale, agentia de securitate pentru informatica şi comunicatii coopereaza cu agentia de acreditare de securitate, cu agentia de protecţie criptografica şi cu alte structuri cu atribuţii în domeniu.
C. Agentia de protecţie criptografica
+ Articolul 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) asigura managementul materialelor şi echipamentelor criptografice;
b) realizează distribuirea materialelor şi echipamentelor criptografice;
c) raporteaza institutiei desemnate la nivel naţional pentru protectia informaţiilor clasificate incidentele de securitate cu care s-a confruntat;
d) coopereaza cu agentia de acreditare de securitate, cu agentia de concepere şi implementare a metodelor, mijloacelor şi masurilor 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
+ Articolul 259
(1) Masurile de protecţie a informaţiilor clasificate în format electronic se aplică sistemelor SPAD şi RTD - SIC care stocheaza, proceseaza sau transmit asemenea informaţii.
(2) Unitatile detinatoare 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.
+ Articolul 260

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

B. Cerinţe de securitate specifice SPAD şi RTD - SIC

+ Articolul 261

(1) Cerinţele de securitate specifice - CSS se constituie într-un document incheiat între agentia 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 elaboreaza pentru fiecare SPAD şi RTD - SIC care stocheaza, proceseaza sau transmite informaţii clasificate, sunt stabilite de către CSTIC şi aprobate de către agentia de acreditare de securitate.

+ Articolul 262

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

+ Articolul 263

CSS au la baza standardele naţionale de protecţie, parametrii esentiali ai mediului operational, nivelul minim de autorizare a personalului, nivelul de clasificare a informaţiilor gestionate şi modul de operare a sistemului care urmeaza să fie acreditat.

C. Moduri de operare

+ Articolul 264

SPAD şi RTD - SIC care stocheaza, proceseaza sau transmit informaţii clasificate vor fi certificate şi acreditate sa opereze, pe anumite perioade de timp, în unul din urmatoarele moduri de operare:

a) dedicat;

b) de nivel înalt;

c) mulţi-nivel.

+ Articolul 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 cunoaste pentru aceste persoane se stabileste 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 cunoaste nu impune o separare a informaţiilor în cadrul SPAD sau RTD, ca mijloc de securitate a SIC. Celelalte măsuri de protecţie prevăzute vor asigura indeplinirea cerinţelor impuse de cel mai înalt nivel de clasificare a informaţiilor gestionate şi de toate categoriile de informaţii cu destinatie speciala stocate, procesate sau transmise în cadrul SPAD sau RTD.

+ Articolul 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 diferentiat, conform principiului necesităţii de a cunoaste.

(2) Pentru a asigura accesul diferentiat la informaţii, conform principiului necesităţii de a cunoaste, 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 destinatie speciala 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 destinatie speciala, având cel mai înalt nivel de clasificare care a fost constatat în multimea informaţiilor stocate, procesate sau vehiculate prin sistem.

+ Articolul 267

(1) În modul de operare mulţi-nivel, accesul la informaţiile clasificate se face diferentiat, potrivit principiului necesităţii de a cunoaste, conform urmatoarelor reguli:

a) nu toate persoanele cu drept de acces la SPAD sau RTD - SIC au certificat de securitate pentru acces la 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

+ Articolul 268

(1) Securitatea SPAD a retelei şi a obiectivului SIC se asigura prin functiile de administrator de securitate.

(2) Administratorii de securitate sunt:

a) administratorul de securitate al SPAD;

b) administratorul de securitate al retelei;

c) administratorul de securitate al obiectivului SIC.

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

+ Articolul 269

(1) CSTIC desemneaza un administrator de securitate al SPAD responsabil cu supervizarea dezvoltării, implementarii şi administrarii masurilor de securitate dintr-un SPAD, inclusiv participarea la elaborarea procedurilor operationale de securitate.

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

+ Articolul 270
Administratorul de securitate al retelei este desemnat de CSTIC pentru un SIC de mari dimensiuni sau în cazul interconectarii mai multor SPAD şi indeplineste atribuţii privind managementul securitatii comunicatiilor.
+ Articolul 271
(1) Administratorul de securitate al obiectivului SIC este desemnat de CSTIC sau de autoritatea de securitate competenţa şi raspunde de asigurarea implementarii şi menţinerea masurilor de securitate aplicabile obiectivului SIC respectiv.
(2) Responsabilitatile unui administrator de securitate al obiectivului SIC pot fi indeplinite de către structura/functionarul de securitate al unităţii, ca parte a indatoririlor sale profesionale.
(3) Obiectivul SIC reprezinta un amplasament specific sau un grup de amplasamente în care funcţionează un SPAD şi/sau RTD. Responsabilitatile şi masurile de securitate pentru fiecare zona de amplasare a unui terminal/statie de lucru care funcţionează la distanta trebuie explicit determinate.
E. Utilizatorii şi vizitatorii
+ Articolul 272
(1) Toţi utilizatorii de SPAD sau RTD - SIC poarta responsabilitatea în ce priveste securitatea acestor sisteme - raportate, în principal, la drepturile acordate şi sunt indrumati de către administratorii de securitate.
(2) Utilizatorii vor fi autorizati 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 cunoaste.
(3) Informarea şi constientizarea utilizatorilor asupra indatoririlor lor de securitate trebuie să asigure o eficacitate sporita a sistemului de securitate.
+ Articolul 273
Vizitatorii trebuie să aibă autorizare de securitate de nivel corespunzător şi sa indeplinească principiul necesităţii de a cunoaste, în situaţia în care accesul unui vizitator fără autorizare de securitate este considerat necesar, vor fi luate măsuri de securitate suplimentare pentru ca acesta sa nu poata avea acces la informaţiile clasificate.
+ Secţiunea a 4-a Componentele INFOSEC
A. Securitatea personalului
+ Articolul 274
(1) Utilizatorii SPAD şi RTD - SIC sunt autorizati şi li se permite accesul la informaţii clasificate pe baza principiului necesităţii de a cunoaste şi în functie de nivelul de clasificare a informaţiilor stocate, procesate sau transmise prin aceste sisteme.
(2) Unitatile detinatoare 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 inlaturarii vulnerabilitatilor faţă de accesarea neautorizata.
+ Articolul 275
În proiectarea SPAD şi RTD - SIC trebuie să se aiba în vedere ca atribuirea sarcinilor şi raspunderilor personalului să se faca în asa fel încât sa nu existe o persoană care să aibă cunoştinţa sau acces la toate programele şi cheile de securitate - parole, mijloace de identificare personala.
+ Articolul 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 retelei. Este interzis, cu excepţia unor situaţii speciale, ca personalul sa faca atât programarea, cat şi operarea sistemelor sau retelelor şi trebuie instituite proceduri speciale pentru depistarea acestor situaţii.
+ Articolul 277
Pentru orice fel de modificare aplicata 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 aplicata.
+ Articolul 278
Pentru a asigura implementarea corecta a masurilor de securitate, personalul SPAD şi RTD - SIC şi personalul care raspunde de securitatea acestora trebuie să fie instruit şi informat astfel încât să îşi cunoasca reciproc atribuţiile.
B. Securitatea fizica
+ Articolul 279
Zonele în care sunt amplasate SPAD şi/sau RTD - SIC şi cele cu terminale la distanta, în care sunt prezentate, stocate, procesate sau transmise informaţii clasificate ori în care este posibil accesul potenţial la astfel de informaţii, se declara zone de securitate clasa I sau clasa II ale obiectivului şi se supun masurilor de protecţie fizica stabilite prin prezentele standarde.
+ Articolul 280
În zonele în care sunt amplasate sisteme SPAD şi terminale la distanta - statii de lucru, unde se proceseaza şi/sau pot fi accesate informaţii clasificate, se aplică urmatoarele 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 distanta poate fi modificata nu trebuie să fie niciodata ocupate de un singur angajat autorizat;
c) persoanelor care solicită acces temporar sau cu intermitente 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 garantia că nu pot avea acces la informaţii clasificate şi nici la echipamentele utilizate.

+ Articolul 281
În functie 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 doua persoane şi în alte zone, ce vor fi stabilite în stadiul initial al proiectului şi prezentate în cadrul CSS.
+ Articolul 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 functionarea de ansamblu a sistemului, agentia de acreditare de securitate trebuie să stabileasca 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
+ Articolul 283
Toate informaţiile şi materialele care privesc accesul la un SPAD sau RTD - SIC sunt controlate şi protejate prin reglementari corespunzătoare nivelului de clasificare cel mai înalt şi specificului informaţiilor la care respectivul SPAD sau RTD - SIC permite accesul.
+ Articolul 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
+ Articolul 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 distanta.
+ Articolul 286
Modul în care este prezentată informatia în clar, chiar dacă se utilizeaza codul prescurtat de transmisie sau reprezentarea binara ori alte forme de transmitere la distanta, nu trebuie să influenteze nivelul de clasificare acordat informaţiilor respective.
+ Articolul 287
Când informaţiile sunt transferate între diverse SPAD sau RTD - SIC, ele trebuie să fie protejate atât în timpul transferului, cat şi la nivelul sistemelor informatice ale beneficiarului, corespunzător cu nivelul de clasificare al informaţiilor transmise.
+ Articolul 288
Toate mediile de stocare a informaţiilor se păstrează intr-o modalitate care să corespunda celui mai înalt nivel de clasificare a informaţiilor stocate sau suportilor, fiind protejate permanent.
+ Articolul 289
Copierea informaţiilor clasificate situate pe medii de stocare specifice TIC se executa în conformitate cu prevederile din procedurile operationale de securitate.
+ Articolul 290
Mediile refolosibile de stocare a informaţiilor utilizate pentru inregistrarea informaţiilor clasificate îşi mentin 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 susmentionate se reclasifica în mod corespunzător sau sunt distruse în conformitate cu prevederile procedurilor operationale de securitate.
E. Controlul şi evidenta informaţiilor în format electronic
+ Articolul 291
(1) Evidenta automata a accesului la informaţiile clasificate în format electronic se tine în registrele de acces şi trebuie realizata neconditionat prin software.
(2) Registrele de acces se păstrează pe o perioadă stabilita de comun acord între agentia de acreditare de securitate şi CSTIC.
(3) Perioada minima de pastrare a registrelor de acces la informaţiile strict secrete de importanţa deosebită este de 10 ani, iar a registrelor de acces la informaţiile strict secrete şi secrete, de cel puţin 3 ani.
+ Articolul 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 sau de clasificare şi controlat în interiorul zonei SPAD, până în momentul în care este distrus, redus la o copie de arhiva sau pus într-un dosar permanent.
(2) Evidentele acestora vor fi mentinute în cadrul zonei SPAD până când sunt supuse controlului sau distruse, conform prezentelor standarde.
+ Articolul 293
În cazul în care un mediu de stocare este generat într-un SPAD sau RTD - SIC, iar apoi este transmis intr-o zona cu terminal/statie de lucru la distanta, se stabilesc proceduri adecvate de securitate, aprobate de către agentia de acreditare de securitate. Procedurile trebuie să cuprindă şi instrucţiuni specifice privind evidenta informaţiilor în format electronic.
F. Manipularea şi controlul mediilor de stocare a informaţiilor clasificate în format electronic
+ Articolul 294
(1) Toate mediile de stocare secrete de stat se identifica 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 urmatoarele cerinţe:
a) Pentru nivelul secret:

- un mijloc de identificare - numar de serie şi marcajul nivelului de clasificare - pentru fiecare astfel de mediu, în mod separat;
- proceduri bine definite pentru emiterea, primirea, retragerea, distrugerea sau pastrarea mediilor de stocare;
- evidentele manuale sau tiparite la imprimanta, indicand conţinutul şi nivelul de secretizare a informaţiilor înregistrate pe mediile de stocare.
b) Pentru nivelul strict secret şi strict secret de importanţa deosebită, informaţiile detaliate asupra mediului de stocare, incluzând conţinutul şi nivelul de clasificare, se ţin într-un registru adecvat.
+ Articolul 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 indeplinirea urmatoarelor 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
+ Articolul 296
Informaţiile clasificate înregistrate pe medii de stocare refolosibile se sterg doar în conformitate cu procedurile operationale de securitate.
+ Articolul 297
(1) Când un mediu de stocare urmeaza sa iasa din uz, trebuie să fie declasificat suprimandu-se orice marcaje de clasificare, ulterior putand fi utilizat ca mediu de stocare nesecret. Dacă acesta nu poate fi declasificat, trebuie distrus printr-o procedură aprobata.
(2) Sunt interzise declasificarea şi refolosirea mediilor de stocare care conţin informaţii strict secrete de importanţa deosebită, acestea putand fi numai distruse, în conformitate cu procedurile operationale de securitate.
+ Articolul 298
Informaţiile clasificate în format electronic stocate pe un mediu de unica folosinţă - cartele, benzi perforate - trebuie distruse conform prevederilor procedurilor operationale de securitate.
+ Secţiunea a 5-a Reguli generale de securitate TIC
A. Securitatea comunicatiilor
+ Articolul 299
Toate mijloacele folosite pentru transmiterea electromagnetica a informaţiilor clasificate se supun instructiunilor de securitate a comunicatiilor emise de către institutia desemnata la nivel naţional pentru protectia informaţiilor clasificate.
+ Articolul 300
Intr-un SPAD - SIC trebuie să se dispună mijloace de interzicere a accesului la informaţiile clasificate de la toate terminalele/statiile de lucru la distanta, atunci când se solicita acest lucru, prin deconectare fizica sau prin proceduri software speciale, aprobate de către autoritatea de acreditare de securitate.
B. Securitatea la instalare şi faţă de emisiile electromagnetice
+ Articolul 301
Instalarea initiala a SPAD sau RTD - SIC sau orice modificare majoră adusa acestora vor fi executate de persoane autorizate, în condiţiile prezentelor standarde. Lucrarile 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.
+ Articolul 302
Toate echipamentele SPAD şi RTD - SIC vor fi instalate în conformitate cu reglementarile specifice în vigoare, emise de către institutia desemnata la nivel naţional pentru protectia informaţiilor clasificate, cu directivele şi standardele tehnice corespunzătoare.
+ Articolul 303
Sistemele SPAD şi RTD - SIC care stocheaza, proceseaza sau transmit informaţii secrete de stat vor fi protejate corespunzător faţă de vulnerabilitatile de securitate cauzate de radiatiile compromitatoare - TEMPEST.
C. Securitatea în timpul procesarii informaţiilor clasificate
+ Articolul 304
Procesarea informaţiilor se realizează în conformitate cu procedurile operationale de securitate, prevăzute în prezentele standarde.
+ Articolul 305
Transmiterea informaţiilor secrete de stat către instalaţii automate - a caror functionare nu necesita prezenta unui operator uman - este interzisa, cu excepţia cazului când se aplică reglementari speciale aprobate de către autoritatea de acreditare de securitate, iar acestea au fost specificate în procedurile operationale de securitate.
+ Articolul 306
În SPAD sau RTD-SIC care au utilizatori - existenti sau potentiali - fără certificate de securitate emise conform prezentelor standarde nu se pot stoca, procesa sau transmite informaţii strict secrete de importanţa deosebită.
D. Procedurile operationale de securitate
+ Articolul 307

Procedurile operationale de securitate reprezinta descrierea implementarii strategiei de securitate ce urmeaza să fie adoptata, a procedurilor operationale de urmat şi a responsabilitatilor personalului.
+ Articolul 308
Procedurile operationale de securitate sunt elaborate de către agentia de concepere şi implementare a metodelor, mijloacelor şi masurilor de securitate, în colaborare cu CSTIC, precum şi cu agentia de acreditare de securitate, care are atribuţii de coordonare, şi alte autorităţi cu atribuţii în domeniu. Agentia 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. Protectia produselor software şi managementul configuratiei
+ Articolul 309
CSTIC are obligaţia să efectueze controale periodice, prin care să stabileasca 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. Protectia programelor - software de aplicatie se stabileste pe baza evaluării nivelului de secretizare a acestora, ţinând cont de nivelul de clasificare a informaţiilor pe care urmeaza să le proceseze.
+ Articolul 310
(1) Este interzisa utilizarea de software neautorizat de către agentia de acreditare de securitate.
(2) Conservarea exemplarelor originale, a copiilor - backup sau off-site, precum şi salvarile periodice ale datelor obtinute din procesare vor fi executate în conformitate cu prevederile procedurilor operationale de securitate.
+ Articolul 311
(1) Versiunile software care sunt în uz trebuie să fie verificate la intervale regulate, pentru a garanta integritatea şi functionarea lor corecta.
(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 imbunatateste posibilitatile 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
+ Articolul 312
Verificarea prezentei virusilor şi software-ului nociv se face în conformitate cu cerinţele impuse de către agentia de acreditare de securitate.
+ Articolul 313
(1) Versiunile de software noi sau modificate - sisteme de operare, subsisteme, pachete de software şi software de aplicatie - stocate pe diferite medii care se introduc intr-o unitate, trebuie verificate obligatoriu pe sisteme de calcul izolate, în vederea depistarii software-ului nociv sau a virusilor de calculator, înainte de a fi folosite în SPAD sau RTD - SIC. Periodic se va proceda la verificarea software-ului instalat.
(2) Verificările trebuie tacute mai frecvent dacă SPAD sau RTD - SIC sunt conectate la alt SPAD sau RTD -SIC sau la o retea publică de comunicatii.
G. Întreţinerea tehnica a SPAD sau RTD - SIC
+ Articolul 314
(1) În contractele de întreţinere a SPAD şi RTD - SIC care stocheaza, proceseaza sau transmit informaţii secrete de stat, se vor specifică cerinţele care trebuie indeplinite 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.
+ Articolul 315
Scoaterea echipamentelor sau a componentelor hardware din zona SPAD sau RTD - SIC se executa în conformitate cu prevederile procedurilor operationale de securitate.
+ Articolul 316
Cerinţele menţionate la art. 314 trebuie stipulate în CSS, iar procedurile de desfăşurare a activităţii respective trebuie stabilite în procedurile operationale de securitate. Nu se accepta tipurile de întreţinere care constau în aplicarea unor proceduri de diagnosticare ce implica accesul de la distanta la sistem, decat dacă activitatea respectiva se desfăşoară sub control strict şi numai cu aprobarea agentiei de acreditare de securitate.
H. Achizitii
+ Articolul 317
Sistemele SPAD sau RTD - SIC, precum şi componentele lor hardware şi software sunt achiziţionate de la furnizori interni sau externi selectati dintre cei agreati de către agentia de acreditare de securitate.
+ Articolul 318
Componentele sistemelor de securitate implementate în SPAD sau RTD - SIC trebuie acreditate pe baza unei documentaţii tehnice amanuntite privind proiectarea, realizarea şi modul de distribuire al acestora.
+ Articolul 319
SPAD sau RTD - SIC care stocheaza, proceseaza sau transmit informaţii secrete de stat sau componentele lor de baza - sisteme de operare de scop general, produse de limitare a funcţionarii pentru realizarea securitatii şi produse pentru comunicare în retea - se pot achizitiona numai dacă au fost evaluate şi certificate de către agentia de acreditare de securitate.
+ Articolul 320
Pentru SPAD şi RTD - SIC care stocheaza, proceseaza sau transmit informaţii secrete de serviciu, sistemele şi componentele lor de baza vor respecta, pe cat posibil, criteriile prevăzute de prezentele standarde.
+ Articolul 321

La inchirierea unor componente hardware sau software, în special a unor medii de stocare, se va tine cont ca astfel de echipamente, odata utilizate în SPAD sau RTD - SIC ce proceseaza, stocheaza sau transmit informaţii clasificate, vor fi supuse masurilor de protecţie reglementate prin prezentele standarde. O dată clasificate, componentele respective nu vor putea fi scoase din zonele SPAD sau RTD - SIC decat după declasificare.
I. Acreditarea SPAD şi RTD - SIC
+ Articolul 322
(1) Toate SPAD şi RTD - SIC, înainte de a fi utilizate pentru stocarea, procesarea sau transmiterea informaţiilor clasificate, trebuie acreditate de către agentia de acreditare de securitate, pe baza datelor furnizate de către CSS, procedurilor operationale de securitate şi altor documentaţii relevante.
(2) Subsistemele SPAD şi RTD - SIC şi statiile de lucru cu acces la distanta 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, cat şi organizaţiile/structurile interne ale tarii, acreditarea se va face de către autoritatea naţionala de securitate, cu consultarea ADS şi a agentiilor INFOSEC, potrivit competentelor.
J. Evaluarea şi certificarea
+ Articolul 323
În situaţiile ce privesc modul de operare de securitate mulţi-nivel, înainte de acreditarea propriu-zisa a SPAD sau RTD - SIC, hardware-ul, firmware-ul şi software-ul vor fi evaluate şi certificate de către agentia de acreditare de securitate, în acest sens, institutia desemnata la nivel naţional pentru protectia informaţiilor clasificate va stabili criterii diferentiate pentru fiecare nivel de secretizare a informaţiilor vehiculate de SPAD sau RTD - SIC.
+ Articolul 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.
+ Articolul 325
Urmatoarele situaţii impun evaluarea şi certificarea de securitate în modul de operare de securitate mulţi-nivel:
a) pentru SPAD sau RTD - SIC care stocheaza, proceseaza sau transmite informaţii clasificate strict secret de importanţa deosebită;
b) pentru SPAD sau RTD - SIC care stocheaza, proceseaza 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 numar de utilizatori posibili care nu poate fi definit exact.
+ Articolul 326
Procesele de evaluare şi certificare trebuie să se desfăşoare, conform principiilor şi instructiunilor aprobate, de către echipe de expertizare cu pregatire tehnica adecvata şi autorizate corespunzător. Aceste echipe vor fi compuse din experti selectionati de către agentia de acreditare de securitate.
+ Articolul 327
(1) În procesele de evaluare şi certificare se va stabili în ce măsura un SPAD sau RTD - SIC indeplineste condiţiile de securitate specificate prin CSS, avandu-se în vedere ca, după incheierea 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 inceapa din stadiul de definire a SPAD sau RTD - SIC şi continua pe parcursul fazelor de dezvoltare.
K. Verificări de rutina pentru menţinerea acreditarii
+ Articolul 328
Pentru toate SPAD şi RTD - SIC care stocheaza, proceseaza sau transmit informaţii secrete de stat, CSTIC stabileste proceduri de control prin care să se poată stabili dacă schimbările intervenite în SIC sunt de natura a le compromite securitatea.
+ Articolul 329
(1) Modificările care implica reacreditarea sau pentru care se solicita aprobarea anterioara a agentiei 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 functionarea corecta a dispozitivelor de securitate.
(3) Menţinerea acreditarii SPAD sau RTD - SIC trebuie să depinda de satisfacerea criteriilor de verificare.
+ Articolul 330
(1) Toate SPAD şi RTD - SIC care stocheaza, proceseaza sau transmit informaţii secrete de stat sunt inspectate şi reexaminate periodic de către agentia de acreditare de securitate.
(2) Pentru SPAD sau RTD - SIC care stocheaza, proceseaza sau transmit informaţii strict secrete de importanţa deosebită, inspecţia se va face cel puţin o dată pe an.
L. Securitatea microcalculatoarelor sau a calculatoarelor personale
+ Articolul 331
(1) Microcalculatoarele sau calculatoarele personale care au discuri fixe sau alte medii nevolatile de stocare a informatiei, ce opereaza autonom sau ca parte a unei retele, precum şi calculatoarele portabile cu discuri fixe sunt considerate medii de stocare a informaţiilor, în acelasi sens ca şi celelalte medii amovibile de stocare a informaţiilor.
(2) În măsura în care acestea stocheaza informaţii clasificate trebuie supuse prezentelor standarde.
+ Articolul 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 vreodata 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

+ Articolul 333

(1) Este interzisa 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 reglementarile interne ale unităţii.

+ Articolul 334

Este interzisa introducerea mediilor de stocare amovibile, a software-ului şi hardware-ului, aflate în proprietate privată, în zonele în care se stocheaza, se proceseaza sau se transmit informaţii clasificate, fără aprobarea conducătorului unităţii.

N. Utilizarea echipamentelor contractorilor sau a celor puse la dispoziţie de alte institutii

+ Articolul 335

Utilizarea într-un obiectiv a echipamentelor şi a software-ului contractantilor, pentru stocarea, procesarea sau transmiterea informaţiilor clasificate este permisa numai cu avizul CSTIC şi aprobarea sefului unităţii.

+ Articolul 336

Utilizarea într-un obiectiv a echipamentelor şi software-ului puse la dispoziţie de către alte institutii poate fi permisa, în acest caz echipamentele sunt evidentiate în inventarul unităţii, în ambele situaţii, trebuie obţinut avizul CSTIC.

O. Marcarea informaţiilor cu destinatie speciala

+ Articolul 337

Marcarea informaţiilor cu destinatie speciala se aplică, în mod obisnuit, informaţiilor clasificate care necesita o distribuţie limitata şi manipulare speciala, suplimentar faţă de caracterul atribuit prin clasificarea de securitate.

+ Capitolul 9 CONTRAVENTII ŞI SANCTIUNI LA NORMELE PRIVIND PROTECTIA INFORMATIILOR CLASIFICATE

+ Articolul 338

(1) Constituie contraventii la normele privind protectia informaţiilor clasificate urmatoarele fapte:

a) detinerea fără drept, sustragerea, divulgarea, alterarea sau distrugerea neautorizata a informaţiilor secrete de stat;

b) neindeplinirea masurilor prevăzute în art. 18, 25-28, 29, 96-139 şi 140-181;

c) neindeplinirea 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) neindeplinirea sau indeplinirea 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) Contraventiile prevăzute la alin. (1) se sancţionează astfel:

a) contraventiile prevăzute la alin. (1) lit. a) se sancţionează cu amendă de la 500.000 lei la 50.000.000 lei în cazul faptelor de detinere 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 neautorizata 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 constata contraventiile pot aplica, după caz, şi sancţiunea complementara, constand în confiscarea, în condiţiile legii, a bunurilor destinate, folosite sau rezultate din contraventii.

(4) Dispozitiile reglementarilor generale referitoare la regimul juridic al contraventiilor se aplică în mod corespunzător.

+ Articolul 339

(1) Contraventiile şi sanctiunile prevăzute la art. 338 se constata şi se aplică, în limitele competentelor ce le revin, de către persoane anume desemnate din Serviciul Roman de Informaţii, Ministerul Apararii Naţionale, Ministerul de Interne, Ministerul Justiţiei, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Paza şi Serviciul de Telecomunicatii Speciale.

(2) Pot să constate contraventiile şi să aplice sanctiunile prevăzute la art. 338, în limitele competentelor stabilite:

a) persoane anume desemnate din ORNISS;

b) conducătorii autorităţilor sau instituţiilor publice, agentilor economici cu capital parţial sau integral de stat şi ai altor persoane juridice de drept public;

c) autorităţile sau persoanele prevăzute de reglementarile generale referitoare la regimul juridic al contraventiilor.

(3) Plangerile împotriva proceselor-verbale de constatare a contraventiilor şi de aplicare a sanctiunilor se solutioneaza potrivit reglementarilor generale privind regimul juridic al contraventiilor.

+ Capitolul 10 DISPOZITII FINALE

+ Articolul 340

Nomenclatura functiilor, condiţiile de studii şi vechime, precum şi salarizarea personalului cu atribuţii privind evidenta, intocmirea, pastrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea informaţiilor clasificate se stabilesc potrivit actelor normative în vigoare.

+ Articolul 341

Conducătorii unităţilor care gestioneaza informaţii clasificate vor lua măsuri ca dispozitiile prezentelor standarde să fie aduse la cunoştinţa tuturor salariatilor şi vor intreprinde măsuri pentru:

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

b) nominalizarea personalului cu atribuţii şi functii privind gestionarea informaţiilor clasificate;
c) iniţierea demersurilor prevăzute de lege şi de prezentele standarde, pentru obtinerea abilitarilor privind accesul la informaţii clasificate.

+ Articolul 342

La solicitarea persoanelor juridice din sfera de competenţa a Serviciului Roman 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 fizica a informaţiilor clasificate.

+ Articolul 343

(1) Prezentele standarde se interpreteaza şi se aplică în concordanta cu Normele privind protectia informaţiilor clasificate ale Organizaţiei Tratatului Atlanticului de Nord în România, aprobate prin Hotărârea Guvernului nr. 353 din 15 aprilie 2002 (~/../../../Public/DetaliiDocumentAfis/35977).
(2) În eventualitatea unor neconcordante între cele doua reglementari menţionate la alin (1), au prioritate Normele privind protectia informaţiilor clasificate ale Organizaţiei Tratatului Atlanticului de Nord în România, aprobate prin Hotărârea Guvernului nr. 353 din 15 aprilie 2002 (~/../../../Public/DetaliiDocumentAfis/35977).

+ Articolul 344

Dispozitiile prezentelor standarde referitoare la contraventiile şi sanctiunile la normele privind protectia informaţiilor clasificate se aplică după 60 de zile de la publicarea prezentei hotărâri.

+ Articolul 345

Anexele nr. 1-32 fac parte integrantă din prezentele standarde naţionale de protecţie a informaţiilor clasificate.

+ Anexa 1

FISA DE CONSULTARE
a documentului "Strict secret de importanţa deosebită"
nr. ..... din ..... privind .....

Nr. crt.	Numele, prenumele şi functia celor care au luat cunoştinţa de conţinutul documentului	Numărul şi seria certificatului	Data şi ora primirii	Semnatura celui care a primit	Cine a aprobat documentul	Data şi ora	Numele, prenumele şi semnatura	Obs.

+ Anexa 2

UNITATEA .....
Compartimentul .....
Nr. ..... din .....

FISA DE PREGATIRE INDIVIDUALA

NUME:
PRENUME:
FUNCTIA:
COMPARTIMENTUL:

Nr. crt.	Tema pregatirii	Forma de pregatire	Locul	Perioada	Semnatura titularului	Obs.

+ Anexa 3

ANGAJAMENT DE CONFIDENTIALITATE*)

Subsemnatul ..... nascut în localitatea ..... la data de ....., fiul (fiica) lui ..... şi a ..... angajat al ..... în functia de ....., cu domiciliul în localitatea ....., strada ....., nr. ....., bl. ....., sc. ....., et. ....., ap. .... judeţul/sectorul ....., posesor al certificatului/autorizatiei seria ....., nr. ...., declar că am luat cunoştinţa de dispozitiile legale cu privire la protectia informaţiilor clasificate şi ma angajez sa pastrez cu strictete secretul de stat şi de serviciu, sa respect intocmai normele legale cu privire la evidenta, manipularea şi pastrarea informaţiilor, datelor şi documentelor secrete de stat şi de serviciu ce mi-au fost încredinţate, inclusiv după încetarea activităţilor care presupun accesul la aceste informaţii.
Sunt constient ca în cazul în care voi încalcă prevederile normative privind protectia informaţiilor clasificate voi raspunde, potrivit legii, administrativ, disciplinar, material, civil ori penal, în raport cu gravitatea faptei.
Data .....
Semnatura
.....
DAT IN PREZENTA

(numele şi prenumele functionarului de securitate)
Semnatura
---

*) Pentru persoanele care au acces la informaţii secrete de stat şi de serviciu.

+ Anexa 4

ROMÂNIA
(UNITATEA)
.....
Compartimentul .....

REGISTRUL DE EVIDENTA
al informaţiilor strict secrete de importanţa deosebită

INTRARE

Nr. de inreg.	Data inreg. anul	luna	ziua	Nr. şi data tului expeditor	De la cine documentul	Conţinutul pe scurt documentului	Nr. al exemplarului	Nr. ex.	Nr. file/ anexe	Nr. file anexe	Cui i s-a repartizat documentul

IESIRE

Data expedierii anul	luna	ziua	Destinatarul documentului sau nr. procesului-verbal de distrugere	Nr. ex.	Nr. file/ anexe	Nr. file anexe	Nr. dosarului de expediere	şi fila unde a fost clasat documentul	Obs

+ Anexa 5

ROMÂNIA
(UNITATEA)
.....
Compartimentul .....

REGISTRUL DE EVIDENTA
al informaţiilor strict secrete şi secrete

INTRARE

Nr. de inreg.	Data inreg. anul	luna	ziua	Nr. şi data documentului	De la pro- cine	Nr. de ex.	Nivelul fi. de secretizare	Conţinutul pe scurt documentului	Nr. anexe	Nr. file anexe	Cui i s-a repartizat documentul

IESIRE

Data expedierii anul	luna	ziua	Nivelul de secretizare	Destinatarul documentului sau nr. procesului-verbal de distrugere	Nr. ex.	Nr. file/ anexe	Nr. file anexe	Nr. dosarului de expediere	şi fila unde a fost clasat documentul	Obs

+ Anexa 6

ROMÂNIA
(UNITATEA)
.....
Compartimentul .....

REGISTRUL DE EVIDENTA
al informaţiilor secrete de serviciu

INTRARE

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

IESIRE

Data expedierii			Destinatar	Nr. ex.	Nr. file anexe	Nr. file anexe	Nr. borderoului de expediere	Nr. dosarului și fila unde a fost clasat documentul (nr. procesului-verbal de distrugere	Obs.
anul	luna	ziua							

+ Anexa 7

REGISTRU UNIC
de evidenta a registrelor, condicilor, borderourilor
și a caietelor pentru insemnari clasificate

Nr. crt.	Nr. fișe	Denumirea materialelor distribuite	Numele, prenumele și semnătura celui care a primit materialul	Seria certificatului de securitate	Data distrib. numărul nr. procesului-verbal de distrugere	Ziua	Luna	Anul	Semnatura celui care a primit materialul	Nr. dosarului unde a fost clasat	O b s

+ Anexa 8

ROMÂNIA
(UNITATEA)
.....
Compartimentul .....

CONDICA DE PREDARE - PRIMIRE
a documentelor clasificate

Nr. crt.	Compunerea documentului	Numele, prenumele și semnătura celui care a primit documentul	Semnătura celui care a predat documentul	Data predării primirii	Nr. de înreg.	Denumire document (nivelul de secretizare)	Clasificatului de securitate ale documentului	Nr. dosare, mape sau file	Ex.	Nr. de pagini	Tura de zi	Tura de noapte	O b s

+ Anexa 9

ROMÂNIA
(UNITATEA)
.....
Compartimentul .....

REGISTRUL
de evidenta a informațiilor clasificate multiplicate

INTRARE

Nr. de înreg.	Data inreg.	Compartimentul care a solicitat copierea	Numele și prenumele celui care a predat	Numărul de exemplare tipărite	Data și semnatura celui care a primit	Nivelul documentului	Nr. de file/ex.	Nr. anexe	

	docu- mentul	ginal şi al cererii de copiere		mentului	copiat		

IESIRE

Documentul copiat			Forma de copiere	Data, numele şi prenumele persoanei care a primit	Obs.
Nr. exemplare	Total file copiate		originalul şi copiile		

+ Anexa 10

ANTET CLASIFICAREA
(institutia / agentul economic) (după completare, în functie de
Nr. --------- din -------- nivelul maxim de clasificare
a informaţiilor pe care
le cuprinde)
APROB
(functia, numele şi prenumele conducătorului
institutiei/agentului economic, semnatura
şi stampila)

PROGRAMUL DE PREVENIRE A SCURGERII DE INFORMATII CLASIFICATE DETINUTE DE
(unitatea care îl întocmeşte)

+ Capitolul 1 BAZA LEGALA

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

+ Capitolul 2

1. GENERALITATI

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

2. OBIECTIVE

Vor fi prezentate obiectivele urmarite prin masurile prezentate în program.
Vor fi vizate urmatoarele obiective minimale:
- apararea informaţiilor clasificate împotriva acţiunilor de compromitere, sabotaj, sustragere, distrugere neautorizata sau alterare;
- prevenirea accesului neautorizat la astfel de informaţii, a cunoasterii şi diseminarii lor ilegale;
- înlăturarea riscurilor şi vulnerabilitatilor ce pot pune în pericol protectia informaţiilor clasificate;
- asigurarea cadrului procedural necesar protectiei informaţiilor clasificate.

3. PRINCIPII

Se precizeaza principiile care stau la baza masurilor de prevenire a scurgerii de informaţii.
Masurile de prevenire a scurgerii de informaţii se bazeaza pe:
- autorizarea accesului la informaţiile clasificate absolut necesare indeplinirii atribuţiilor de serviciu (principiul "nevoii de a cunoaste");
- asigurarea aplicarii masurilor de protecţie, în mod diferentiat, pe zone de securitate şi în functie de nivelurile de acces la informaţii clasificate;
- accesul la informaţii clasificate este permis numai în baza verificărilor şi abilitarilor legale;
- aplicarea, în mod obligatoriu şi unitar, a masurilor de protecţie atât în locurile în care se depozitează informaţiile clasificate şi în cazul sistemelor informatice care stocheaza, prelucreaza sau transmit informaţii de acest fel, cat şi al persoanelor care au acces la acestea şi utilizatorilor retelelor respective;
- raspunderea personala privind aplicarea masurilor de protecţie stipulate prin programul de prevenire a scurgerii de informaţii clasificate.

+ Capitolul 3

1. ELEMENTE GENERALE PRIVIND INFORMATIILE CLASIFICATE DETINUTE DE INSTITUTIA/AGENTUL ECONOMIC

Se vor face precizări privind clasele şi nivelurile de secretizare a informaţiilor clasificate deţinute de institutia/agentul economic (în cazul celor primite de la alti emitenti se va menţiona baza juridica a detinerii, respectiv tipul contractului şi dacă s-au asumat obligaţii de protejare a secretului prin incheierea de acorduri între părţi).

2. LISTA INFORMATIILOR CLASIFICATE, APROBATE PRIN HOTĂRÂRE A GUVERNULUI (DOCUMENTE, DATE, OBIECTE SAU ACTIVITĂŢI, INDIFERENT DE SUPORT SAU FORMA), PE CLASE ŞI NIVELURI DE SECRETIZARE, DETINUTE DE UNITATEA IN CAUZA

Instituţiile/agentii economici vor întocmi lista cuprinzand categoriile informaţiilor clasificate, pe care le deţin, pe clase şi niveluri de secretizare.
Lista va fi actualizata ori de cate ori situaţia o impune (clasificarea sau declasificarea unor informaţii).

3. LOCURI UNDE SE CONCENTREAZA, DE REGULA ORI TEMPORAR, DATE, INFORMATII, DOCUMENTE CLASIFICATE SAU SE DESFASOARA ASTFEL DE ACTIVITĂŢI (CONFORM ANEXEI Nr. 10/A)
Vor fi menţionate:
- spatiile destinate pastrarii documentelor clasificate;
- spatiul destinat sistemului/retelelor informatice de procesare automata a datelor care preia, prelucreaza, stocheaza şi transmite date şi informaţii clasificate;
- alte locuri unde se gestioneaza sau se manipuleaza asemenea date, informaţii şi documente clasificate sau se desfăşoară astfel de activităţi.

+ Capitolul 4

1. LISTA FUNCTIILOR CARE NECESITA ACCES LA INFORMATII CLASIFICATE
Vor fi precizate functiile care necesita accesarea informaţiilor clasificate, pe clase şi niveluri de secretizare, cu respectarea stricta a principiului "nevoii de a cunoaste".
2. PREZENTAREA PERSOANEI/STRUCTURII DESEMNATE SA INDEPLINEASCA ATRIBUŢII PE LINIA PROTECTIEI ACTIVITĂŢILOR, DATELOR, INFORMATIILOR ŞI DOCUMENTELOR CLASIFICATE
2.1. Pentru fiecare persoana în parte se vor preciza:
- numele şi prenumele;
- datele de identificare (prenumele parintilor, nume anterioare, data şi locul nasterii, profesia şi locul de muncă, domiciliul, telefonul);
2.2. Atribuţiile şi competentele privind asigurarea protectiei informaţiilor clasificate.
Nominalizarea se va face de către conducatorul institutiei/agentului economic respectiv, situaţia fiind prezentată pe niveluri de acces, care va fi acordat numai în urma obtinerii abilitarii.
3. PREZENTAREA PERSOANELOR CARE AU SAU URMEAZA SA AIBA ACCES LA INFORMATII CLASIFICATE, PE NIVELURI DE SECRETIZARE
Va fi întocmită lista cu persoanele care au sau urmeaza să aibă acces la informaţii clasificate, nominalizate de către conducatorul institutiei/agentului economic (inclusiv cele care lucreaza în sistemul informatic şi de telecomunicatii, destinat preluării, prelucrarii, stocarii şi transmiterii de informaţii clasificate)*)
Va fi întocmită, de asemenea, lista cu persoanele cărora li se acordă acces temporar la informaţii clasificate din cadrul sau din afara institutiei/agentului economic (inclusiv cele aparţinând firmelor prestatoare de servicii pentru întreţinerea sau instalarea programelor, care vor fi avizate corespunzător nivelului maxim de secretizare a informaţiilor din sistemele informatice şi de telecomunicatii)**).
Accesul la informaţii clasificate va fi permis numai după obtinerea abilitarii.
Pentru fiecare persoana nominalizata vor fi precizate:
- numele, prenumele şi datele de identificare (prenumele parintilor, nume anterioare, data şi locul nasterii, profesia şi locul de muncă, domiciliul, telefonul);
- informaţiile clasificate care îi sunt absolut necesare indeplinirii atribuţiilor de serviciu, cu precizarea clasei şi nivelului de secretizare a acestuia.

---
*) Numărul persoanelor nominalizate în lista respectiva va fi cel mult egal cu cel al functiilor ce necesita acces la informaţiile clasificate.
**) Listele respective vor fi actualizate, cu indeplinirea procedurilor legale de avizare, în raport de necesităţi (extinderea sau limitarea accesului unor persoane la informaţii clasificate, în functie de modificarea atribuţiilor de serviciu).

+ Capitolul 5

1. MASURI DE PROTECTIE FIZICA A CLADIRILOR, SPATIILOR/LOCURILOR UNDE SE PASTREAZA SAU SE CONCENTREAZA INFORMATII CLASIFICATE ORI SE DESFASOARA ASTFEL DE ACTIVITĂŢI (CONFORM ANEXEI Nr. 10/B)
Vor fi stipulate măsuri vizand:
- securitatea cladirilor;
- controlul intrarilor şi iesirilor;
- paza;
- containerele şi incaperile de securitate;
- incuietorile;
- controlul cheilor şi combinatiilor;
- dispozitivele de detectare a intrusilor;
- protectia fizica a copiatoarelor şi dispozitivelor telefax;
- planurile de urgenta.
2. MASURI PROCEDURALE DE PROTECTIE A DATELOR, INFORMATIILOR, DOCUMENTELOR ORI A ACTIVITĂŢILOR CLASIFICATE
Vor fi prezentate:
- reguli de evidenta, procesare, manipulare, accesare, multiplicare, transmitere, pastrare şi stocare a datelor, informaţiilor şi documentelor clasificate indiferent de suport (aprobate de conducerea institutiei/agentului economic);
- reguli de acces pentru personalul propriu;
- reguli de acces pentru personalul/persoanele din afara institutiei/agentului economic, inclusiv pentru straini sau reprezentanti mass-media.

+ Capitolul 6 PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ŞI DE TELECOMUNICATII DESTINAT PRELUARII, PRELUCRARII, STOCARII ŞI TRANSMITERII DE DATE

ŞI INFORMATII CLASIFICATE
Vor fi prezentate echipamentele de comunicatii şi birotica (telefoane, fax, telex, copiatoare) prin care vor fi transmise/prelucrate informaţii clasificate.
Vor fi prezentate, de asemenea, echipamentul informatic existent, calculatoarele conectate la Internet, sistemele de protecţie utilizate şi firma prestatoare de servicii pentru întreţinerea sau instalarea programelor (conform anexei nr. 10/C).
În situaţia în care unele dintre aceste echipamente nu sunt protejate corespunzător, se va face precizarea ca folosirea acestora pentru prelucrarea informaţiilor clasificate este interzisa.
+ Capitolul 7 MASURI DE PROTECTIE IMPOTRIVA OBSERVARII ŞI ASCULTARII*)
---
*) Zonele în care se elaboreaza şi/sau se discuta informaţii clasificate secret de stat trebuie protejate împotriva observarii şi ascultarii pasive şi/sau active. Responsabilitatea inlaturarii riscurilor privind observarea şi ascultarea revine institutiei/agentului economic, care elaboreaza sau, după caz, gestioneaza informaţii clasificate (conform anexei nr. 10/D).
+ Capitolul 8
1. CONTROALE, ACTIVITĂŢI DE ANALIZA ŞI EVALUARE A MODULUI IN CARE SE RESPECTA PREVEDERILE LEGALE REFERITOARE LA PROTECTIA INFORMATIILOR CLASIFICATE
Vor fi prezentate tematica şi periodicitatea controalelor (inopinate, periodice), cine le executa, documentele ce se intocmesc şi sanctiunile ce se vor aplica în cazurile de încălcare a reglementarilor privind protectia informaţiilor clasificate.
Se va întocmi planificarea activităţilor de evaluare şi analiza a stării de protecţie a informaţiilor clasificate şi se va prevedea ca anual, după incheierea operaţiunii de inventariere a suportilor de informaţii clasificate să se analizeze şi să se evalueze modul în care au fost respectate prevederile programului, prevazandu-se şi masurile care se impun şi termenele de remediere a unor nereguli constatate.
2. SOLUTIONAREA CAZURILOR DE INCALCARE A REGLEMENTARILOR PRIVIND PROTECTIA INFORMATIILOR CLASIFICATE (CONFORM ANEXEI Nr. 10/E)
Se vor face referiri la:
- masurile ce vor fi luate în cazul constatarii încălcării reglementarilor privind protectia informaţiilor clasificate;
- evidenta incalcarilor reglementarilor de securitate;
- comunicarea compromiterilor;
- scoaterea din evidenta a documentelor clasificate pierdute sau distruse.
+ Capitolul 9 MASURI DE INSTRUIRE ŞI EDUCATIE PROTECTIVA A PERSOANELOR CARE AU ATRIBUŢII PE LINIA PROTECTIEI INFORMATIILOR CLASIFICATE ŞI A CELOR CARE AU ACCES LA ASTFEL DE INFORMATII (CONFORM ANEXEI Nr. 10/F)*)
Se vor preciza:
- situaţii care impun asemenea măsuri;
- responsabilităţii;
- mijloace şi metode de instruire şi pregatire contrainformativa.
Întocmit
(numele, prenumele şi semnatura
functionarului de securitate)
Raspunderea pentru intocmirea, avizarea şi aplicarea programului de prevenire a scurgerii de informaţii clasificate revine conducătorului unităţii detinatoare.
Programul de prevenire a scurgerii de informaţii clasificate se actualizeaza, anual sau ori de cate ori se impune (identificarea unor noi riscuri şi vulnerabilitati, aparitia unor noi situaţii sau acte normative), modificările efectuate aducandu-se de fiecare data la cunoştinţa institutiei abilitate, unde se transmite sub forma de completare pentru a fi avizat.
Se întocmeşte în 2 exemplare (un exemplar la beneficiar şi unul la institutia abilitata).
---
*) Planul specific de pregatire a personalului este elaborat la inceputul fiecarui an. în conţinutul acestuia vor fi menţionate responsabilitatile, termenele, mijloacele şi metodele de instruire şi educatie proiectiva. Functionarul sau structura de securitate va tine evidenta instruirilor/activităţilor de educatie proiectiva şi va asigura pregătirea tuturor persoanelor avizate pentru acces la informaţii clasificate, care nu au participat la insiruirile organizate.
+ Anexa 10/A
LOCURI UNDE SE CONCENTREAZA, DE REGULA ORI TEMPORAR,
DATE, INFORMATII ŞI DOCUMENTE CLASIFICATE SAU
SE DESFASOARA ASTFEL DE ACTIVITĂŢI
De la caz la caz, pentru fiecare zona administrativa, zona de securitate sau incinta în care se desfăşoară activităţi, se lucreaza cu / se gestioneaza informaţii clasificate vor fi menţionate masurile de securitate protectiva existente şi garantiile pe care le prezinta în protectia informaţiilor şi activităţilor clasificate. De asemenea, se vor menţiona sarcinile şi atribuţiile ce trebuie indeplinite conform Regulamentului de organizare şi functionare interna.
Masurile de protecţie fizica a incaperilor şi locurilor unde se păstrează sau se manipuleaza informaţii clasificate sau se desfăşoară astfel de activităţi se vor organiza şi implementa în functie de zonele de securitate. Accesul în zonele de securitate şi incaperile în care se deruleaza activităţi ori se lucreaza cu informaţii clasificate va fi permis exclusiv persoanelor abilitate, potrivit nivelurilor de clasificare, cu respectarea principiului "nevoii de a cunoaste".

Zonele în care sunt manipulate sau stocate informaţii clasificate trebuie organizate şi administrate în asa fel încât sa corespunda uneia dintre urmatoarele categorii:
a) Zona de securitate clasa I, care presupune ca orice persoană aflata în interiorul acesteia are acces la informaţii secrete de stat, de nivelul "strict secret" şi "strict secret de importanţa deosebită".
O asemenea zona necesita:
- un perimetru clar definit 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 nivelului de securitate 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.
O asemenea zona necesita:
- perimetru clar definit şi protejat, în care toate intrarile şi iesirile sunt supravegheate;
- controlul sistemului de intrare, pentru a permite accesul neinsotit numai persoanelor verificate şi autorizate sa patrunda în aceasta zona. Pentru toate celelalte persoane trebuie să existe reguli de însoţire, supraveghere şi prevenire a accesului neautorizat la informaţii clasificate sau în sectoare în care sunt manipulate şi stocate astfel de informaţii.
Incintele în care nu se lucreaza zilnic 24 de ore vor fi inspectate după orele de program, pentru a verifica dacă informaţiile clasificate sunt asigurate în mod corespunzător.
c) Zona administrativa
În jurul zonelor de securitate clasa I sau clasa a II-a poate fi stabilita o zona administrativa cu perimetru vizibil definit, în interiorul careia sa existe posibilitatea de control al personalului şi vehiculelor, în zona administrativa sunt permise manipularea şi pastrarea numai a informaţiilor secrete de serviciu.
+ Anexa 10/B
MASURI DE PROTECTIE FIZICA A CLADIRILOR,
SPATIILOR/LOCURILOR UNDE SE PASTREAZA SAU SE
CONCENTREAZA DATE, INFORMATII ŞI DOCUMENTE
CLASIFICATE ORI SE DESFASOARA ASTFEL DE ACTIVITĂŢI
Securitatea cladirilor
Cladirile, spatiile/locurile în care se afla informaţii clasificate trebuie protejate împotriva accesului neautorizat. Masurile de protecţie (grilaje la ferestre, incuietori la uşi, paza la intrari, sisteme automate pentru controlul accesului, controale şi patrule de securitate, sisteme de alarma sau pentru detectarea intrusilor etc.) vor fi dimensionate în raport cu:
a) clasa de securitate a informaţiilor, suportul, volumul şi modul de depozitare a acestora în cladire;
b) calitatea containerelor în care sunt depozitate informaţiile clasificate;
c) locul de dispunere a spatiilor /locurilor unde se păstrează sau se concentreaza date, informaţii şi documente clasificate ori se desfăşoară astfel de activităţi;
d) caracteristicile cladirii.
Controlul intrarilor şi iesirilor
Intrarile în zonele de securitate clasa I şi clasa a II-a vor fi controlate prin permis de intrare sau printr-un sistem special de recunoastere personala aplicat personalului permanent. În mod obligatoriu se va institui un sistem de control al vizitatorilor pentru prevenirea accesului neautorizat la informaţiile clasificate.
Se recomanda ca permisul de intrare sa nu arate, în clar, identitatea organizaţiei emitente sau locul în care deţinătorul are acces. Controlul intrarilor şi iesirilor poate fi insotit de un sistem de identificare automata, care trebuie considerat suplimentar, fără a presupune o inlocuire totala a pazei.
Dacă se apreciaza necesar, la intrarea sau la ieşirea din zonele de securitate clasa I sau clasa a II-a, se vor efectua controale pentru depistarea şi/sau prevenirea tranzitarii fără drept a informaţiilor şi materialelor clasificate.
Paza
Folosirea paznicilor pentru asigurarea zonelor de securitate şi a informaţiilor clasificate se va face numai după ce au fost verificaţi, li s-a acordat abilitarea de securitate corespunzătoare zonei şi li s-a efectuat pregătirea de specialitate. Vor fi precizate inclusiv măsuri de control şi supraveghere corespunzătoare a paznicilor.
Patrularile în zonele de securitate clasa I şi clasa a II-a se vor realiza în afara orelor de program şi în zilele nelucratoare, la intervale care vor fi stabilite în functie de amenintarea locala, pentru a exista garantia ca informaţiile clasificate sunt protejate în mod corespunzător.
Pentru eficientizarea sistemelor de paza, în special în zonele de securitate unde, în interesul securitatii, paznicii nu pot avea intrare directa, trebuie asigurate măsuri menite sa previna accesul neautorizat şi sa detecteze eventualele încercări de patrundere fără drept în aceste perimetre, prin folosirea unor modalităţi adecvate (televiziune cu circuit inchis, sisteme de alarma sau pentru inspectare vizuala). De la caz la caz, astfel de modalităţi pot fi folosite şi ca substitute ale patrulelor.
Containere şi încăperi de securitate
Containerele folosite pentru pastrarea informaţiilor clasificate se impart în trei clase:
- clasa A: containere aprobate la nivel naţional pentru depozitarea informaţiilor strict secrete de importanţa deosebită în zone de securitate clasa I sau clasa a II-a;
- clasa B: containere aprobate la nivel naţional pentru pastrarea informaţiilor strict secrete şi secrete în zone de securitate clasa I sau clasa a II-a;
- clasa C: mobilier de birou adecvat numai pentru pastrarea informaţiilor secrete de serviciu.
Incaperile de securitate sunt construite (amenajate) în zone de securitate clasa I sau clasa a II-a, unde informaţiile clasificate secret de stat sunt pastrate pe rafturi deschise sau sunt expuse pe harti, diagrame etc.

Peretii, podelele, plafoanele, usile şi incuietorile acestor încăperi vor oferi o protecţie echivalenta clasei containerului de securitate aprobat pentru pastrarea informaţiilor clasificate respective.
Incuietori
Incuietorile folosite la containerele şi incaperile de securitate în care sunt pastrate informaţii clasificate se impart în trei grupe astfel:
- grupa A: incuietori aprobate la nivel naţional pentru containerele din clasa A;
- grupa B: incuietori aprobate la nivel naţional pentru containerele din clasa B;
- grupa C: incuietori indicate numai pentru mobilierul de birou adecvat numai pentru pastrarea informaţiilor secrete de serviciu (pentru clasa C).
Controlul cheilor şi combinatiilor
Cheile containerelor şi incaperilor de securitate nu trebuie scoase din cladirea sau zona de securitate în care se afla documentele clasificate.
Combinatiile incuietorilor (containerelor de securitate) vor fi cunoscute numai de persoanele abilitate.
Pentru cazurile de urgenta, un rand de chei suplimentare (o evidenta scrisa a fiecarei combinatii) vor fi pastrate în plicuri mate sigilate într-un compartiment stabilit de conducerea institutiei/agentului economic, sub control corespunzător, în containere separate. Evidenta fiecarei combinatii trebuie păstrată în plic separat. Cheilor şi plicurilor trebuie să li se asigure protecţie la nivelul de securitate a informaţiilor clasificate la care acestea permit accesul.
Cunoasterea combinatiilor incuietorilor de la containerele de securitate va fi restransa la un numar minim de persoane. Cheile şi combinatiile vor fi schimbate:
a) ori de cate ori are loc o schimbare de personal;
b) de fiecare data când se constată că a avut loc un compromis de natura să le faca vulnerabile;
c) la intervale regulate, de preferinta o dată la şase luni (fără a se depăşi 12 luni).
Dispozitive de detectare a intrusilor
Când se folosesc sisteme de alarma, televiziune cu circuit inchis sau alte dispozitive destinate supravegherii zonelor de securitate sau protectiei informaţiilor clasificate, sursa de alimentare trebuie să aibă atât conectare permanenta, cat şi de rezerva (eventual, o baterie reincarcabila). Orice defectare sau interventie neautorizata asupra acestor sisteme trebuie să declanseze o alarma sau un alt sistem de avertizare pentru personalul care monitorizează instalatia respectiva.
Protectia fizica a copiatoarelor şi dispozitivelor telefax
Copiatoarele şi dispozitivele telefax trebuie protejate fizic, în măsura în care este necesar să se garanteze folosirea lor numai de către persoanele autorizate.
Planuri de urgenta
Fiecare autoritate şi institutie/agent economic vor pregati planuri pentru protejarea informaţiilor clasificate în cazuri de urgenta, care să prevada inclusiv evacuarea şi distrugerea acestora atunci când este cazul.
Protectia, evacuarea şi/sau distrugerea materialelor strict secrete şi secrete, în cazuri de urgenta, nu trebuie să afecteze protectia, evacuarea şi/sau distrugerea materialelor strict secrete de importanţa deosebită, sau a materialelor codificate, care vor avea totdeauna prioritate faţă de alte documente clasificate.

+ Anexa 10/C

PROTECTIA SISTEMELOR/SUBSISTEMELOR INFORMATICE
DESTINATE PRELUARII, PRELUCRARII, STOCARII ŞI TRANSMITERII DE DATE ŞI
INFORMATII CLASIFICATE ŞI A INCAPERILOR IN CARE ACESTEA SE AFLA AMPLASATE

- Administratorul şi utilizatorii sistemului destinat preluării, prelucrarii, stocarii şi transmisiei de date şi informaţii clasificate sunt numiti de seful institutiei/agentului economic.
- Administratorul, utilizatorii şi persoanele care au acces la date şi informaţii cu caracter secret de stat, procesate prin sisteme de prelucrare automata a datelor sunt supuse procedurilor de selectionare, verificare şi avizare, potrivit nivelurilor de acces.
- Incaperile unde sunt amplasate sisteme/subsisteme informatice destinate preluării, prelucrarii, stocarii şi transmisiei de date şi informaţii cu caracter secret de stat vor fi asigurate cu sisteme de supraveghere şi control-acces potrivit standardelor în vigoare, corespunzător nivelurilor de clasificare a informaţiilor.
- Sistemul/subsistemul informatic destinat preluării, prelucrarii, stocarii şi transmisiei de date şi informaţii secrete de stat va fi prevăzut cu sistem de secretizare prin metode, mijloace şi echipamente pentru asigurarea integritatii, confidentialitatii şi disponibilităţii acestora.
- Utilizarea sistemelor informatice care preiau, prelucreaza, stocheaza şi transmit date cu caracter secret de stat se face pe bază de parole şi coduri şi chei de criptare care se păstrează în plicuri sigilate la dispoziţia sefului unităţii.
- Accesul în sistemul/subsistemul informatic destinat preluării, prelucrarii, stocarii şi transmiterii de date şi informaţii clasificate se atribuie, individual şi diferentiat, în conformitate cu atribuţiile de serviciu ale fiecarui utilizator pentru pornirea, utilizarea şi oprirea sistemului de calcul, introducerea, citirea, modificarea, stergerea sau transferul de date în/din bazele de date ale sistemului informatic gestionarea şi manipularea cheilor de criptare/decriptare.
- Consultarea, introducerea, modificarea sau stergerea informaţiilor din baza de date se executa numai cu aprobarea sefului institutiei/agentului economic, asigurandu-se o evidenta stricta, în scopul realizării eventualei examinari ulterioare a activităţii, a interactiunii utilizatorilor cu sistemele de calcul, prin memorarea momentului, tipului operaţiei, codului utilizatorului şi datelor accesate de acesta.
- Elaborarea de lucrari din bazele de date ale sistemului/subsistemului destinat preluării, prelucrarii, stocarii şi transmiterii de date şi informaţii clasificate se efectueaza numai pe baza ordinelor rezolutive, ale conducerii unităţii, date pe adrese sau documente interne de lucru.

- Suportii de memorie externa (discurile, discurile portabile, dischetele, benzile magnetice, casetele de banda magnetica, compact-discurile, discurile optice sau magneto-optice), utilizati în sistemul/subsistemul destinat preluării, prelucrarii, stocarii şi transmiterii de date şi informaţii clasificate, au regimul documentelor cu caracter secret de stat şi se păstrează la compartimentul de documente secrete, fiind supuşi procedurilor restrictive identice acestora.
- Instalarea, depanarea sau modificarea configuratiei sistemului de calcul destinat destinat preluării, prelucrarii, stocarii şi transmiterii de date şi informaţii clasificate se executa de personal abilitat, verificat contrainformativ şi controlat.
- Saptamanal, administratorul sistemului informatic destinat preluării, prelucrarii, stocarii şi transmiterii de date şi informaţii clasificate va elimina fisierele temporare de lucru sau iesite din uz şi va verifica integritatea fisierelor stocate pe discuri.

Intrarea şi ieşirea atât a persoanelor cat şi a materialelor vor fi controlate. în incintele în care sistemul/subsistemul poate fi modificat nu se va permite accesul unui singur angajat autorizat (se va institui regula celor doi).

Persoanele care solicită acces temporar sau intermitent în aceste încăperi vor obtine aprobare de vizitator de la administratorul de sistem; vizitatorii trebuie supravegheati permanent pentru a preveni accesul la echipamentele informatice în scopuri ilicite.

Un pericol în domeniul protectiei informaţiilor clasificate procesate, stocate şi transmise prin sistemul de prelucrare automata a datelor îl reprezinta orice actiune, inactiune sau imprejurare de natura sa afecteze integritatea, disponibilitatea sau confidentialitatea datelor, precum şi functionalitatea programelor şi echipamentelor aferente unui sistem informatic.

Constituie pericole:

- pierderea, sustragerea, inlocuirea, alterarea sau distrugerea neautorizata ori accidentala a datelor, programelor, suportilor materiali ai acestora sau a echipamentelor aferente;
- operarea gresita în timpul preluării, prelucrarii, transferului, stocarii sau arhivarii datelor;
- interceptarea şi interpretarea transmisiilor efectuate în cadrul retelei de calculatoare;
- fortarea accesului, accesul neautorizat sau intarzierea accesului autorizat la date, programe, suportii materiali ai acestora sau la echipamentele aferente;
- eludarea restrictiilor privind accesul la date, prin modificarea neautorizata a configuratiilor instalate, programelor sau a drepturilor de acces;
- copierea neautorizata a datelor;
- interceptarea şi interpretarea radiatiilor electromagnetice sau acustice produse de echipamentele de calcul, dispozitivele de transmisiuni sau canalele de comunicatie;
- interceptarea discutiilor sau convorbirilor telefonice referitoare la sistemul informatic;
- exploatarea informativa a personalului implicat în dezvoltarea, întreţinerea sau exploatarea sistemului informatic;
- introducerea în exploatare de produse informatice fără o prealabila testare care să ofere garantii de functionare corecta şi controlata;
- pastrarea, amplasarea, exploatarea, întreţinerea sau depozitarea în condiţii improprii a sistemelor de calcul, suportilor materiali de date sau a dispozitivelor şi echipamentelor destinate asigurarii protectiei şi securitatii datelor;
- nerespectarea reglementarilor referitoare la secretul de stat sau a regulilor de compartimentare a muncii;
- nerespectarea regulilor privind depozitarea, manipularea sau distrugerea suportilor de memorie externa şi a dispozitivelor şi echipamentelor scoase din uz;
- nerespectarea prevederilor, metodologiilor şi a documentatiilor tehnice de întreţinere şi exploatare a sistemelor informatice;
- aparitia de anomalii în functionarea sistemelor de operare, pachetelor de programe sau programelor de aplicatie;
- aparitia de anomalii în functionarea sistemelor informatice;
- aparitia de deranjamente ale canalelor de comunicatie;
- discutarea în condiţii de insecuritate sau cu persoane neautorizate, a unor aspecte privind sistemele de calcul, informaţiile şi datele inmagazinate;
- producerea de calamitati naturale (cutremure, inundaţii, alunecari de teren, etc.);
- producerea de evenimente cu efect distructiv (explozii, incendii, spargeri de conducte, acte de sabotaj, acţiuni teroriste, acte de vandalism, socuri electromagnetice, etc);
- producerea pe orice cale de evenimente cu efecte similare.

POSIBILE PERICOLE, AMENINTARI ORI ATACURI LA ADRESA SECURITATII SISTEMULUI/RETELELOR INFORMATICE

- ascultare pasiva (atac contra confidentialitatii): accesarea sistemului în scopul modificarii informaţiilor generate, transmise, stocate sau afisate pe componentele vulnerabile ale acestuia;
- interceptia: penetrarea neautorizata a sistemului, în scopul modificarii informaţiilor transmise pe o cale de comunicatie;
- deducerea prin interferenta: actiunea unui utilizator autorizat de a corela informaţiile la care are acces, în scopul deducerii unor informaţii clasificate la care nu are dreptul de acces;
- deghizarea ("inselarea" mecanismelor de autentificare): insusirea şi folosirea identităţii unui utilizator autorizat, pentru accesarea sistemului;
- crearea şi utilizarea unor canale disimulate ("ocolirea" controalelor de acces) în scopul transmiterii de informaţii de la un utilizator autorizat către unul neautorizat;
- utilizarea asa-zisei "porti secrete" (trap-desk) pentru evitarea controalelor de acces.

+ Anexa 10/D

MASURI DE PROTECTIE IMPOTRIVA OBSERVARII ŞI ASCULTARII

Protectia împotriva ascultarilor pasive (posibile prin ascultare directa sau furnizate de comunicatii nesigure) se realizează pe baza asistentei tehnice din partea instituţiilor abilitate, prin izolarea fonica a peretilor, usilor, podelelor şi plafoanelor zonelor sensibile.

Protectia împotriva ascultarilor active (prin microfoane, radio-emitatori şi alte dispozitive implantate) necesita inspecţii de securitate tehnica şi/sau fizica a structurii incaperii, accesoriilor, instalaţiilor tehnico-sanitare, echipamentelor şi mobilierului de birou, sistemelor de comunicatii etc. Aceste inspecţii vor fi realizate de institutii competente.

Zone sigure din punct de vedere tehnic

Accesul în zonele protejate împotriva ascultarilor se va controla în mod special.

Incaperile vor fi incuiate sau pazite corespunzător standardelor de securitate fizica, inclusiv când nu sunt ocupate, iar cheile vor fi tratate ca materiale clasificate. Periodic, se vor organiza inspecţii fizice şi/sau tehnice. De asemenea, astfel de inspecţii se vor organiza, în mod obligatoriu, ca urmare a oricarei intrari neautorizate, a unei suspiciuni privind accesul personalului extern şi după executarea lucrărilor de reparatii, întreţinere, zugravire, redecorare etc. Nici un obiect nu se va introduce în aceste zone, fără a fi verificat de către personal specializat în depistarea dispozitivelor de ascultare.

În mod curent, în zonele asigurate din punct de vedere tehnic nu se vor instala telefoane. Totusi, când instalarea acestora este absolut necesară, trebuie prevăzute cu un dispozitiv de deconectare pasiv.

Inspecţiile de securitate tehnica în zonele unde se poarta discutii extrem de sensibile trebuie intreprinse în mod obligatoriu premergator începerii convorbirilor, atât pentru identificarea fizica a dispozitivelor de ascultare cat şi pentru verificarea sistemelor telefonice, electrice, sau de alta natura, care ar putea fi folosite ca mediu de atac.

Verificarea dotarilor electrice /electronice din birouri

Înainte de a fi folosite în zonele în care se lucreaza ori se discuta despre informaţii strict secrete de importanţa deosebită şi strict secrete, echipamentele de comunicatii şi dotarile de orice fel din birouri, în principal cele electrice şi electronice, trebuie verificate de specialisti în securitatea comunicatiilor, pentru a preveni transmiterea ilicita sau din neglijenta a unor informaţii inteligibile.

În aceste zone se va organiza o evidenta a tipului şi numarului de inventar ale fiecarei piese de mobilier sau echipament introduse sau mutate din încăperi, care va fi păstrată sub cheie, iar cheile vor fi protejate corespunzător.

+ Anexa 10/E

SOLUTIONAREA CAZURILOR DE INCALCARE A REGLEMENTARILOR PRIVIND PROTECTIA INFORMATIILOR CLASIFICATE

Cazurile de încălcare a reglementarilor de securitate vor fi comunicate imediat conducătorului institutiei/agentului economic şi instituţiilor abilitate.

Orice încălcare a reglementarilor de securitate va fi cercetata de persoane special desemnate, cu experienta în activitatea de securitate pentru a stabili:

- dacă şi în ce mod au fost compromise informaţii clasificate;
- dacă persoanele neautorizate care au avut, sau ar fi putut avea acces la informaţii clasificate, prezinta suficienta incredere şi loialitate, astfel încât rezultatul compromiterii sa nu creeze prejudicii;
- masurile de remediere, corective sau disciplinare (inclusiv juridice), care sunt recomandate.

În situaţia în care persoanele care au luat cunoştinţa de conţinutul informaţiilor clasificate prezinta incredere, vor fi instruite în mod corespunzător pentru a preveni diseminarea, în caz contrar se va proceda la evaluarea prejudiciului rezultat şi vor fi intreprinse masurile necesare diminuarii acestuia.

Evidenta incalcarilor reglementarilor de securitate

În cadrul autorităţilor şi instituţiilor publice, agentilor economici cu capital integral sau parţial de stat şi altor persoane juridice de drept public sau privat, detinatoare de informaţii clasificate, se va organiza evidenta cazurilor de încălcare a reglementarilor de securitate, a rapoartelor de investigatii şi masurilor corective intreprinse, în consecinţa. Aceste evidente vor fi pastrate timp de trei ani de către structura/functionarul de securitate şi vor fi puse la dispoziţie în timpul controalelor efectuate de reprezentantii autorizati ai instituţiilor abilitate.

Comunicarea compromiterilor

Informaţiile clasificate sunt compromise când conţinutul acestora (total sau parţial) este cunoscut de persoane neautorizate (care nu au autorizare valabila de acces la acestea) ori când au fost supuse riscului acestei cunoasteri neautorizate (informaţiile clasificate pierdute, chiar şi temporar, în afara unei zone de securitate sunt considerate a fi compromise).

Instituţiile abilitate vor fi incunostintate prin cel mai operativ sistem de comunicare asupra circumstantelor compromiterii unor astfel de informaţii.

Scopul principal al comunicarii compromiterii este de a da posibilitatea recuperării informaţiilor, evaluării prejudiciilor şi intreprinderii acţiunilor necesare sau aplicabile pentru minimalizarea consecintelor.

Informarea preliminara trebuie să conţină:

a) o descriere a informaţiilor respective (clasificare şi marcare, numărul de înregistrare, numărul de exemplare, conţinutul, data, emitentul);

b) o scurta prezentare a imprejurarilor în care a avut loc compromiterea, inclusiv data constatarii, perioada în care informaţiile au fost expuse compromiterii şi, dacă se cunoaste, persoanele neautorizate care au avut sau ar fi putut avea acces la acestea;

c) precizări cu privire la eventuala informare a emitentului.

La solicitarea instituţiilor abilitate, informarile preliminare vor fi completate pe măsura derularii cercetarilor.

Evaluarile proprii ale instituţiilor/agentilor economici, referitoare la prejudiciile şi actiunile ce urmeaza a fi intreprinse pentru înlăturarea sau diminuarea acestora, vor fi prezentate în cel mai scurt timp instituţiilor abilitate.

Scoaterea din evidenta a documentelor clasificate pierdute sau distruse

Când exista indicii certe, confirmate în scris de instituţiile abilitate cu atribuţii de control şi investigare a compromiterii informaţiilor clasificate, ca documentul dat în raspundere este iremediabil pierdut (şi nu ratacit), acesta va fi scos din evidenta compartimentului care l-a gestionat, numai după finalizarea cercetarilor, cu avizul instituţiilor abilitate.

+ Anexa 10/F

MASURI DE INSTRUIRE ŞI EDUCATIE PROTECTIVA A PERSOANELOR CARE AU ATRIBUŢII PE LINIA PROTECTIEI INFORMATIILOR CLASIFICATE ŞI A CELOR CARE AU ACCES LA ASTFEL DE INFORMATII

Educatia protectiva are ca principal obiectiv instruirea persoanelor care au acces la informaţii clasificate în vederea aplicarii masurilor legale referitoare la protejarea informaţiilor clasificate.

Educatia personalului se realizează prin derularea unor activităţi specifice în cadrul cărora persoanelor care acceseaza informaţii clasificate le sunt prezentate: prevederile legislaţiei în domeniul protectiei informaţiilor clasificate;

- conţinutul programului de prevenire a scurgerilor de informaţii clasificate;
- competentele instituţiilor abilitate în domeniul protectiei datelor şi informaţiilor clasificate;
- aspectele semnificative pe linia protectiei secretelor de stat cu relevanta în domeniul specific de activitate;
- mijloacele şi metodele utilizate de structurile specializate în culegerea de date şi informaţii clasificate;
- consecintele nerespectarii normelor legale în domeniu;
- alte elemente de interes pentru siguranţa naţionala.

Ca mijloace frecvent utilizate în procesul de educatie protectiva se pot folosi documentare, filme de specialitate, diapozitive, materiale publicitare etc.

+ Anexa 11

ROMÂNIA
(UNITATEA)

Compartimentul ---

CONDICA DE PREDARE - PRIMIRE
a cheilor de la incaperile şi containerele de securitate

Nr. crt.	Numele şi prenumele persoanei careia i-a fost predata cutia cu chei	Data şi ora primirii	Semnatura de primire	Nr. liului	Data şi ora ridicarii	Numele şi prenumele persoanei care a ridicat cutia cu chei	Semnatura de primire	

+ Anexa 12

ROMÂNIA
(institutia)

Compartimentul .....

CERTIFICAT DE SECURITATE
Seria ..... Nr. ..... din .....

Prin prezentul certificat se autorizeaza accesul la informaţii secrete de stat, nivelul --------, pentru dl./d-na (numele, prenumele, datele de identificare) ----------, angajat al institutiei noastre în functia de ---------- .

Certificatul este valabil în perioada ----------.

Seful institutiei,

(semnatura, stampila)

Posesor: ----------
(nume, prenume şi semnatura)

+ Anexa 13

ROMÂNIA
(Institutia)

Compartimentul ---

AUTORIZATIE DE ACCES LA INFORMATII CLASIFICATE
Seria ..... Nr. ..... din .....

Prin prezenta se autorizeaza accesul la informaţii clasificate secret de stat, nivelul ----------, pentru dl./d-na (numele, prenumele, datele de identificare) ----------, angajat al institutiei noastre în functia de ---------- .

Autorizatia este valabila în perioada ---------- .

Seful institutiei,

(semnatura, stampila)
Posesor: ---
(nume, prenume şi
semnatura)
+ Anexa 14
ROMÂNIA
INSTITUTIA DETINATOARE
Nr. ----- din -------
Către
OFICIUL REGISTRULUI NAŢIONAL AL INFORMATIILOR
SECRETE DE STAT
În vederea eliberarii certificatului de securitate/autorizatiei de acces la informaţii clasificate, nivel ----------, pentru (numele, prenumele şi datele de identificare ale persoanei)----------, angajat al (denumirea completa a institutiei), în functia de ----------, va rugam sa initiati procedurile de verificare necesare.
Mentionam ca în prezent persoana detine/nu detine certificat de securitate/autorizatie de acces la informaţii clasificate pentru nivelul ---------- .
Anexam în original chestionarul de securitate corespunzător nivelului solicitat.
Semnatura
Sef institutie
+ Anexa 15

Formular de baza - date personale SECRET DE SERVICIU
Nr..... din ..../..../.... (după completare)
Ex. unic
SPATIU REZERVAT INSTITUTIEI SOLICITANTE

Institutia solicitanta:

Nivelul de acces solicitat: | SECRET | | S.S. | | S.S.I.D. |

Motivul solicitarii:

DATE GENERALE DESPRE SOLICITANT

NUME:

NUME ANTERIOARE

PRENUME:

DATA NASTERII:

LOCUL NASTERII: sat: comuna:

oras/municipiu: judet:

CETATENIA la nastere: actuala:

CARTE/BULETIN IDENTITATE:
Seria: Nr.: Eliberat de: La data:

Cod numeric personal:

DOMICILIUL PERMANENT:
Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:
Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILII PERMANENTE ŞI FLOTANTE IN ULTIMII CINCI ANI:
Tipul de domiciliu: Permanent: Flotant:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Tipul de domiciliu: Permanent: Flotant:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

ADRESE ŞI RESEDINTE IN STRAINATATE IN ULTIMII CINCI ANI:
(pentru perioade peste 3 luni)

Perioada: Tara: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Perioada: Tara: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

STUDII CIVILE ŞI MILITARE

Nr.crt.	Perioada	Institutia	Felul studiilor

LIMBI STRAINE CUNOSCUTE

Nr.crt.	Limba	Nivelul

(În cazul atestatelor se vor indica institutia şi data)

SITUAŢIA MILITARA:

Fără stagiu militar satisfacut: Militar activ: În rezerva:

Seria livretului militar: Numărul livretului militar:

Eliberat de centrul militar: la data:

PASAPOARTE:

Turistic
Seria: Numărul: Eliberat de: La data:

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

Diplomatic
Seria: Numărul: Eliberat de: La data:

CALATORII IN STRAINATATE IN ULTIMII CINCI ANI:

Nr. crt.	Tara	Localitatea	Perioada	Scopul

SITUAŢIA PROFESIONALA:

CIVIL:

Profesia:

Ministerul:

Institutia la care este incadrat:

De la data:

Functia:

De la data:

Adresa de la locul de muncă:

Telefon: Fax: E-mail:

MILITAR:

Gradul: Functia:

Arma de baza: Arma de încadrare:

Unitatea:

Indicativul esalonului superior:

LOCURI DE MUNCĂ IN ULTIMII CINCI ANI:

Nr. crt.	INSTITUTIA	PERIOADA	FUNCTII DETINUTE

SITUAŢIA FAMILIALA ACTUALA

Celibatar(a): Căsătorit(a): Concubinaj:

Despartit(a) în fapt: Divortat(a): Vaduv(a):

Recasatorit(a):

Alte situaţii:

Date referitoare la data şi locul incheierii căsătoriei sau legate de situaţia actuala

DATE DESPRE PARTENERUL DE VIATA (SOT/SOTIE, CONCUBIN/CONCUBINA)

NUME:

NUME ANTERIOARE:

PRENUME:

DATA NASTERII:

LOCUL NASTERII: comuna: oras: judet:

CETATENIA: la nastere: actuala:

PROFESIA:

LOCUL DE MUNCĂ:

DOMICILIUL PERMANENT:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

DOMICILII PERMANENTE ŞI FLOTANTE IN ULTIMII CINCI ANI:

Tipul de domiciliu: Permanent: Flotant:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Tipul de domiciliu: Permanent: Flotant:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Tipul de domiciliu: Permanent: Flotant:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

COPII (inclusiv cei din alte căsătorii)

Nume şi prenume	Data nasterii	Localitatea	Domiciliul	Locul de muncă	Functia

DATE DESPRE PARINTI

TATAL

NATURA RELATIEI: tata natural: tata adoptiv: tata vitreg:

NUME:

NUME ANTERIOARE:

PRENUME:

PROFESIA:

DATA NASTERII

LOCUL NASTERII: comuna: oras: judet:

CETATENIA la nastere: actuala:

DOMICILIUL PERMANENT:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail

MAMA

NATURA RELATIEI: mama naturala: mama adoptiva: mama vitrega:

NUME:

NUME ANTERIOARE:

PRENUME:

PROFESIA:

DATA NASTERII:

LOCUL NASTERII: comuna: oras: judet:

CETATENIA la nastere: actuala:

DOMICILIUL PERMANENT:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail:

DOMICILIUL FLOTANT:

Localitatea: Judeţul/Sectorul:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

Telefon fix: Telefon mobil:

Fax: E-mail

DATE DESPRE FRATI/SURORI

NUME:

PRENUME:

DATA ŞI LOCUL NASTERII

DOMICILIUL:

NUME:

PRENUME:

DATA ŞI LOCUL NASTERII

DOMICILIUL:

NUME:

PRENUME:

DATA ŞI LOCUL NASTERII

DOMICILIUL:

NUME:

PRENUME:

DATA ŞI LOCUL NASTERII:

DOMICILIUL:

ANTECEDENTE ŞI CAZIER

Ati fost vreodata retinut, arestat preventiv, anchetat, pus sub acuzare, judecat, condamnat (inclusiv la amenda penala sau interzicerea unor drepturi), gratiat, amnistiat, eliberat pe cautiune, eliberat condiţionat? DA NU

Ati fost vreodata anchetat administrativ, sanctionat administrativ, amendat de către politie sau autorităţi civile (nu se menţionează amenzile pentru abateri minore, cum sunt cele pentru parcare, dar se menţionează cele pentru fapte grave, precum conducerea sub influenţa alcoolului sau tulburarea ordinii publice)? DA NU

Ati fost vreodata judecat în Consiliul de Onoare, anchetat, judecat sau condamnat de o Curte Martiala, trimis intr-o unitate disciplinara în timpul cat v-ati aflat în serviciul militar? DA NU

Dacă ati răspuns cu da la vreuna din intrebarile de mai sus, detaliati în spatiul de mai jos, inclusiv perioadele şi instituţiile care au sanctionat faptele dvs...

Nr. crt.	FAPTA SAVARSITA	PERIOADA	INSTITUTIA

DATE DE SECURITATE

Solicitantul / Partenerul de viaţa

Ati fost vreodata implicat în acţiuni de: spionaj, terorism, tentative de subminare a ordinii democratice prin mijloace "violente"? DA / DA

NU / NU

Ati fost vreodata membru sau simpatizant al unei grupari implicate în acţiuni menţionate mai sus? DA / DA

NU / NU

Ati fost vreodata în relatii apropiate cu o persoană care a activat sau a simpatizat cu astfel de grupari? DA / DA

NU / NU

Dacă ati răspuns cu da la vreuna dintre intrebari detaliati mai jos.

Solicitantul / Partenerul de viaţa

Ati colaborat cu organele fostei Securitati care au desfăşurat activităţi de politie politica? DA / DA

NU / NU

Considerati ca ati atras atenţia vreunui serviciu de informaţii sau de securitate strain? DA / DA

NU / NU

Considerati ca au fost facute presiuni asupra dumneavoastra sau asupra membrilor familiei dumneavoastra ca urmare a unui incident survenit pe teritoriul altei tari? DA / DA NU / NU

Sunteti în relatii permanente de natura

profesionala sau personala cu cetăţeni straini? | DA | | | DA | |

| NU | | | NU | |

Considerati ca vi s-a solicitat vreodata sa furnizati informaţii clasificate în afara atribuţiilor de serviciu? | DA | | | DA | |

| NU | | | NU | |

Dacă ati răspuns cu da la vreuna dintre intrebari detaliati mai jos.

| |

Solicitantul Partenerul de viaţa

Aveti rude apropiate, din cele menţionate mai sus, care locuiesc în strainatate sau care au locuit mai mult de trei luni în strainatate? | DA | | | DA | |

| NU | | | NU | |

Dacă ati răspuns cu da detaliati mai jos.

Nr. crt.	NUMELE	GRADUL DE RUDENIE	TARA	PERIOADA
	PRENUMELE			

DECLARATIE

Subsemnatul, ...

Declar că toate datele furnizate mai sus sunt reale.

Declar că am luat cunoştinţa de cerinţele procedurii de verificare şi avizare pentru acces la informaţiile naţionale clasificate şi le accept.

Consimt ca toate datele pe care le furnizez să fie verificate, constient fiind de consecintele legale ale declaratiilor false sau omisiunilor cu buna stiinta.

Ma angajez sa furnizez orice date suplimentare care imi vor fi solicitate în eventualitatea unor neclaritati, precum şi sa informez, din proprie iniţiativă, asupra oricarei modificari aparute în cele declarate mai sus.

Sunt de acord ca neacordarea avizului de securitate sa nu-mi fie motivata.

Data,

Semnatura,

Data în prezenta

(numele şi prenumele functionarului de securitate)

Semnatura

+ Anexa 16

FORMULAR SUPLIMENTAR
(se completeaza pentru nivelurile
STRICT SECRET şi STRICT SECRET
DE IMPORTANŢA DEOSEBITĂ)

Nr._____din____.____._____

SECRET DE SERVICIU
(după completare)
Ex. unic

SPATIU REZERVAT INSTITUTIEI SOLICITANTE

Institutia solicitanta: |

Nivelul de acces solicitat: | S.S. | | | S.S.I.D. | |

Motivul solicitarii: |

DATE PERSONALE ALE SOLICITANTULUI

NUME: |

PRENUME: |

DATA NASTERII: |

LOCUL NASTERII: sat: | comuna: |

oras/municipiu: | judet: |

CETATENIA actuala: |

DATA COMPLETARII FORMULARULUI DE BAZA: |

DATE SUPLIMENTARE DESPRE SOLICITANT

În afara domiciliilor, adreselor şi resedintelor indicate în formularul de baza, în ultimii zece ani ati mai avut şi altele?

IN ROMÂNIA

Perioada: | Judet: | Localitatea |

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Judet: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Judet: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

IN STRAINATATE

Perioada: Tara: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Tara: Localitatea:

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Tara: Localitatea

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Tara: Localitatea

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

Perioada: Tara: Localitatea

Strada: Numărul: Bloc:

Scara: Etajul: Apartamentul: Codul postal:

.....

RUDE

Cumnati/cumnate

GRAD DE RUDENIE			
NUMELE ACTUAL			
NUMELE LA NASTERE			
NUME ANTERIOARE			
PRENUMELE			
DATA NASTERII			
LOCUL NASTERII			
CETATENIA ACTUALA			
DOMICILIUL PERMANENT			
OCUPATIA ACTUALA			

Parintii partenerului de viaţa (naturali, vitregi sau adoptivi).

	TATAL	MAMA
GRADUL DE RUDENIE		
NUMELE ACTUAL		

NUMELE LA NASTERE
NUME ANTERIOARE
PRENUMELE
DATA NASTERII
LOCUL NASTERII
CETATENIA ACTUALA
DOMICILIUL PERMANENT
OCUPATIA ACTUALA

REFERINŢE

Nominalizati date de identificare a minimum doua persoane, care sunt de acord să prezinte referinţe despre dumneavoastra şi care va cunosc de cel puţin cinci ani.

Numele şi prenumele	Ocupatia	Locul de munca	Domiciliul permanent	Tel/Fax	Observatii

STARE DE SĂNĂTATE

Ati fost vreodata diagnosticat cu boala psihica?
Dacă răspunsul este afirmativ, detaliati:

Ati suferit incidente de natura medicală care au provocat pierderea temporara a cunostintei?
Dacă răspunsul este afirmativ, detaliati:

Sunteti constient de vreo alta problema medicală, neacoperita de raspunsurile anterioare, care ar putea afecta protectia informaţiilor clasificate?
Dacă răspunsul este afirmativ, detaliati:

Ati avut sau aveti probleme legate de consumul de alcool?
Dacă răspunsul este afirmativ, detaliati:

Ati consumat sau consumaţi substante care creeaza dependenta sau droguri?
Dacă răspunsul este afirmativ, detaliati:

RELATIILE DE FAMILIE

> Aveti neintelegeri dese în familie:

DA | | NU | |

Detaliati cu privire la motivul acestora:

> Aveti persoane în întreţinere din afara căsătoriei?

DA | | NU | | CUNOSCUTE | | NECUNOSCUTE | |

> Faceti referire cu privire la relatiile pe care le aveti cu

cumnatii/cumnatele stabiliti/stabilite în strainatate, precum şi la parintii partenerului de viaţa stabiliti în strainatate.

DECLARATIE

Subsemnatul,.....

Declar că toate datele furnizate mai sus sunt reale.

Declar că am luat cunoştinţa de cerinţele procedurii de verificare şi avizare pentru acces la informaţiile naţionale clasificate şi le accept.

Consimt ca toate datele pe care le furnizez să fie verificate, constient fiind de consecintele legale ale declaratiilor false sau omisiunilor cu buna stiinta.

Ma angajez sa furnizez orice date suplimentare care imi vor fi solicitate în eventualitatea unor neclaritati, precum şi sa informez, din proprie iniţiativă, asupra oricarei modificari aparute în cele declarate mai sus.

Sunt de acord ca neacordarea avizului de securitate sa nu-mi fie motivata.

Data, Semnatura,

Data în prezenta

(numele şi prenumele functionarului de securitate)

Semnatura

+ Anexa 17

Formular financiar SECRET DE SERVICIU

Nr. _____din___. ___ (după completare)

(Se completeaza, numai pentru S.S.I.D.)

Ex. unic

SPATIU REZERVAT INSTITUTIEI SOLICITANTE

Institutia solicitanta:

Motivul solicitarii:

DATE GENERALE DESPRE SOLICITANT

NUME:

NUME ANTERIOARE:

PRENUME:

DATA NASTERII:

LOCUL NASTERII: sat: comuna:

oras/municipiu: judet:

CETATENIA actuala:

SITUAŢIA FAMILIALA

> Cum va apreciati situaţia financiară?

Confortabila: Acceptabila: Dificila: Nu pot aprecia:

Locuinta

> Locuinta pe care o folositi împreună cu ceilalti membri ai familiei este:

Proprietate personala: Inchiriata: Locuinta de serviciu:

PROPRIETĂŢI MOBILE/IMOBILE

> Detaliati

Venituri şi cheltuieli lunare tipice pentru dumneavoastra şi partenerul de viaţa

> Venit anual net realizat în urma activităţii principale.

> Venituri suplimentare realizate din alte activităţi

> Total venituri anuale pe gospodarie.

> Evaluaţi care este valoarea totala a debitelor curente care va greveaza

Sunteti dvs. sau partenerul de viaţa beneficiarii unor castiguri provenind din jocuri de noroc sau alt gen de astfel de castiguri:

DA | | NU | |

Dacă Da detaliati:

Dumneavoastra şi partenerul dumneavoastra de viaţa economisiti

Curent Ocazional Rar

Comparativ cu anul anterior aveti obligaţii şi datorii financiare:

Mai mari: Mai mici: Cam la fel:

Sunteti interesat, dvs. sau partenerul de viaţa în colaborarea cu anumite societăţi comerciale înregistrate în tara? DA NU

Dacă "da", detaliati:
- denumirea societatii comerciale, adresa, domeniul de activitate
- caracterul interesului (asociere, membru în Consiliul de administratie, consilier etc.)

Aveti relatii, dvs. sau partenerul de viaţa cu firme înregistrate în strainatate? DA NU

Dacă da, detaliati:
- denumirea firmei, adresa, domeniul de activitate
- caracterul interesului (asociere, membru în Consiliul de administratie, consilier, contracte de colaborare, concesionare, comision etc.)
- tara de inmatriculare.

Împotriva dvs. sau a asociatilor dvs. au fost initiate, în ultimii 10 ani, proceduri de executare silita? DA NU

Dacă da, detaliati:
- motivul procedurii
- instanţa judecătorească care a hotarat măsura
- autoritatea care a pus-o în aplicare

Aveti alte interese financiare care ar putea intră în conflict cu indatoririle dumneavoastra de serviciu? DA NU

Detaliati:

Detaliati alte aspecte care ne-ar putea ajuta sa înţelegem mai bine situaţia dumneavoastra financiară?

Detaliati:

DECLARATIE

Subsemnatul .....

Declar că toate datele furnizate mai sus sunt reale.

Declar că am luat cunoştinţa de cerinţele procedurii de verificare şi avizare pentru acces la informaţiile naţionale clasificate şi le accept.

Consimt ca toate datele pe care le furnizez să fie verificate, constient fiind de consecintele legale ale declaratiilor false sau omisiunilor cu buna stiinta.

Ma angajez sa furnizez orice date suplimentare care imi vor fi solicitate în eventualitatea unor neclaritati, precum şi sa informez, din proprie iniţiativa, asupra oricarei modificari aparute în cele declarate mai sus.

Sunt de acord ca neacordarea avizului de securitate sa nu-mi fie motivata.

Data, Semnatura,

Data în prezenta

_____

(numele şi prenumele functionarului de securitate)

Semnatura

+ Anexa 18

ROMÂNIA

(Institutia)

_____

Compartimentul _____

REGISTRUL

pentru evidenta certificatelor de securitate/autorizaţiilor de acces la informaţii clasificate

Nr. crt.	Numele şi prenumele şi datele de identificare ale posesorului	Functia şi departamentul/ timentul în care îşi desfăşoară activitatea	Nivelul de acces cerut	Data şi numărul certificatului/ autorizaţiei	Seria valabilităţii	Perioada de retragere	Data retragerii	Motivul retragerii	Obs.

+ Anexa 19

ROMÂNIA
OFICIUL REGISTRULUI NAŢIONAL
AL INFORMATIILOR SECRETE DE STAT
Nr. _____ din _____ . _____ . _____
Către
(Autoritatea desemnata de securitate)

În vederea eliberarii avizului de securitate, nivel_____, pentru _____(numele prenumele şi datele de identificare ale persoanei)_____, angajat al ____(denumirea completa a institutiei)_____ , în functia de _____ va rugam sa initiati procedurile de verificare necesare.
Mentionam ca în prezent persoana detine / nu detine certificat de securitate / autorizatie de acces la informaţii clasificate pentru nivelul _____.
Anexam în original chestionarul de securitate corespunzător nivelului solicitat.
Directorul general al Oficiului Registrului Naţional
al Informaţiilor Secrete de Stat,
(Semnatura)

+ Anexa 20

ROMÂNIA
(Autoritatea desemnata de securitate)
Nr. _____ din _____._____.__
Către
OFICIUL REGISTRULUI NAŢIONAL AL INFORMATIILOR SECRETE DE STAT
La adresa dumneavoastra nr. _____ din _____ va comunicam avizarea pozitiva/negativa a accesului la informaţii secrete de stat de nivel_____ pentru _____(numele, prenumele şi datele de identificare ale persoanei)_____ angajat al instituţiei _____(denumirea institutiei solicitante) _____ în functia de _____.
Seful Autorităţii desemnate de securitate,

+ Anexa 21

ROMÂNIA
OFICIUL REGISTRULUI NAŢIONAL
AL INFORMATIILOR SECRETE DE STAT
Nr. _____ din _____
Către
(Institutia solicitanta)
La adresa dumneavoastra nr. _____ din _____ va comunicam avizarea pozitiva/negativa a accesului la informaţii secrete de stat de nivel_____ pentru ____(numele, prenumele şi datele de identificare ale persoanei) ___ angajat al institutiei dvs., în functia de _____ .
Directorul general al Oficiului Registrului Naţional
al Informaţiilor Secrete de Stat,
(Semnatura)

+ Anexa 22

ROMÂNIA
(Institutia)

Nr. _____ din_____._____.____
Către
OFICIUL REGISTRULUI NAŢIONAL AL INFORMATIILOR SECRETE DE STAT
Va comunicam eliberarea la data de _____ a certificatului de securitate / autorizatiei de acces la informaţii clasificate cu seria_____, nr. _____ pentru dl/d-na _____(numele, prenumele, datele de identificare) _____, angajat al institutiei noastre în functia de _____.
Certificatul/autorizatia este valabil/a în perioada _____, pentru accesul la informaţii clasificate de nivel _____.
Seful institutiei,

_____
(semnatura, stampila)

+ Anexa 23

ROMÂNIA
(Institutia)

_____
Compartimentul _____
REGISTRUL
pentru evidenta autorizaţiilor speciale

Nr. Crt.	Numele, prenumele şi datele de identificare ale posesorului deţinătorului	Denumirea şi adresa completa a unităţii	Data eliberarii şi autorizatiei	Numărul şi seria autorizatiei	Perioada de valabilitate	Obs.

+ Anexa 24

ANTETUL INSTITUTIEI/AGENTULUI ECONOMIC
Adresa Tel.Fax
Către ORNISS

CERERE

pentru eliberarea autorizatiei de securitate industriala

Va rugam sa eliberati autorizatia de securitate industriala pentru _____(denumirea completa a, institutiei/agentului economic)_____ cu sediul în _____ (adresa completa)_____ în vederea participării la proceduri de atribuire a contractelor clasificate.

Anexam, în original, chestionarul de securitate industriala pentru obtinerea autorizatiei de securitate.

Directorul institutiei/ agentului economic,

_____

(semnatura, stampila)

+ Anexa 25

Secret de serviciu
(după completare)

(SE COMPLETEAZA NUMAI PENTRU ELIBERAREA AUTORIZATIEI DE SECURITATE INDUSTRIALA)

CHESTIONAR
de securitate industriala

1. AGENTUL ECONOMIC SOLICITANT

Denumire completa:
Nr. din Registrul Comerţului:
Data ultimei actualizari la Registrul Comerţului:
Denumiri anterioare (dacă este cazul):
Cod fiscal: Cod SIRUES:
Stare Firma
Adresa completa pentru sediul social: Str. ..... nr..... Sectorul/judeţul ..... Localitatea ..... Nr. telefon ..... fax: ..... Telex ..... e-mail ..... Adresa site Internet ..... Cod postal (Casuta postala, dacă este cazul): .....
Adrese anterioare (dacă este cazul):
Statutul juridic:
Forma de proprietate:
Capitalul Capitalul social: .....
Data ultimei modificari a capitalului social: ..... Capital subscris varsat: ..... Capital disponibil ..... Nr. acţiuni: ..... Valoare acţiuni: ..... Actiune nominativa. Exista? [] Da [] Nu Autoritatea/persoana care o detine ..... Adresa site Internet..... Crestere preconizata ..... la data de: ..... Organigrama societatii (se ataseaza la chestionar)
Actionari persoane fizice (care deţin peste 5 % din capitalul social) Numar ..... 1. Nume, prenume ..... Data şi locul nasterii ..... Nr. şi seria actului de identitate Adresa completa: Str. ..... nr. ..... Sectorul/judeţul ..... oras/ municipiu..... Nr. telefon ..... fax: ..... Telex ..... e-mail .... Adresa site Internet..... Cod postal (casuta postala, dacă este cazul): ..... Tara ..... Procentul de acţiuni/părţi sociale detinut _____% începând cu anul: ... (În cazul în care sunt mai mulţi se pot prezenta în anexa, după prezentul model)

Actionari persoane juridice
.....
.....

Agenti economici la care firma solicitanta este acţionar
Numărul de agenti economici: .....
Ce reprezinta pentru dvs.?
[] Furnizor
[] Client
[] Altceva
Procentul de acţiuni detinut_____% începând cu anul: .....

Firmele la care persoane din consiliul de administratie sunt actionari:
1. Numele şi prenumele persoanei:
Denumirea completa a firmei:
Nr. din Registrul Comerţului

2. CONDUCEREA AGENTULUI ECONOMIC ŞI FUNCTIONARUL / STRUCTURA DE SECURITATE RESPONSABIL/RESPONSABILA

Director general
Nume şi prenume: .....
Prenumele tatalui .....

Data numirii în functie: .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa)

Director economic
Nume şi prenume: .....
Prenumele tatalui .....
Data numirii în functie .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa)

Director ştiinţific/tehnic/comercial
Nume şi prenume: .....
Prenumele tatalui .....
Data numirii în functie: .....
Pregatire profesionala .....
Data nasterii: ..... locul:.....tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa)

Membrii consiliului de administratie
1. Nume şi prenume: .....
Prenumele tatalui .....
Data numirii în functie .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa): a)
b)
c).....
2.
3.
4.
5.
6.

Functionarul / Structura de securitate responsabil/responsabila cu protectia
informaţiilor secrete de stat din cadrul agentului economic solicitant:
Nume şi prenume: .....
Prenumele tatalui .....
Functia: .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara.....
Firme la care este [] acţionar [] în conducere [] proprietar
(denumire, adresa completa)

(Datele de la aceasta rubrica se vor completa de către toate persoanele din
structura de securitate a agentului economic)

3. DATE DESPRE PROFILUL ŞI ACTIVITATEA DESFASURATA

Obiectul(ele) principal(e) de activitate:

Numar de angajaţi permanent:

Intreprinderea dvs. este distribuitorul autorizat al altor agenti economici?
(situaţia în ultimii 5 ani)

[] Da [] Nu
Numele şi adresa completa (dacă este cazul)

4. SCURT RAPORT PENTRU ULTIMII 3 ANI DE EXERCITIU FINANCIAR

Sfârşit perioada financiară			
Active fixe - TOTAL			
Conturi în lei:			
Conturi în valută:			
Creante:			
Stocuri:			
Active circulante - TOTAL:			
Capital social:			
Capital varsat:			
Imprumuturi pe termen lung:			
Imprumuturi pe termen scurt			
Datorii - TOTAL			
Total pasiv:			
Cifra de afaceri:			
Total venituri			
Total cheltuieli:			
Profit brut:			
Pierderi (unde este cazul):			

5. BONITATE ŞI GARANTII BANCARE

Bănci cu care lucrati (se vor completa urmatoarele informaţii pentru fiecare banca): Denumire: ..... Adresa completa: Str. ..... nr. ..... Sectorul/judeţul ..... localitatea ..... Nr. telefon ..... fax: ..... Telex ..... e-mail ..... Adresa site Internet..... Numar cont: ..... Data deschiderii contului: ..... Creditul este: [] garantat [] negarantat Marimea creditului: .....
Mijloace de plată la cumparare [] acreditiv [] ordin de plată [] transfer bancar [] condiţii speciale [] Altele:.....
Exista reclamatii împotriva firmei pentru plăţile cu furnizorii sau clientii? [] Da [] Nu Dacă DA: Numărul reclamatiilor: Data înregistrării: .... Pentru suma de (valoarea fiecarei plati contestate): Reclamatia a fost rezolvata? [] Da [] Nu Alte comentarii legate de aceasta:

6. INFORMATII DE SECURITATE

Considerati ca firma dumneavoastra a atras atenţia unui serviciu de informaţii sau de securitate strain?	DA	NU
Au existat cazuri când au fost solicitate informaţii cu caracter sensibil în afara atribuţiilor de serviciu?		
Institutia sau vreunul dintre angajaţi a fost implicat(a) sau a sprijinit activităţi de: - spionaj - terorism - sabotaj?		
Ati avut vreodata angajaţi care au sprijinit sau au fost implicati în una dintre activităţile de mai sus?		
Aveti cunoştinţa de orice alte împrejurări, condiţii (factori de risc), nedeclarate în raspunsurile precedente, care au putut influenţa activitatea dvs. sau a personalului din subordine, cum ar fi: obisnuinta utilizarii unor substante psihotrope,		

dependenta de alcool, dificultati financiare deosebite?		

7. DATE REFERITOARE LA SISTEMUL DE PROTECTIE A INFORMATIILOR SECRETE DE STAT

7.1. PROTECTIA INFORMATIILOR

MENTIONATI NIVELUL DE CLASIFICARE A INFORMATIILOR GESTIONATE:

[] secrete de stat - S.S.I.D. [] [] secrete de serviciu
- S.S. []
- S []

7.1.1. LOCUL/LOCURILE UNDE SE CONCENTREAZA DATE şi INFORMATII SECRETE DE STAT

	DA	NU
- incapere destinata numai protectiei informaţiilor		
- incapere destinata numai sistemului/subsistemului de calcul destinat preluării, prelucrarii, stocarii şi transmisiei datelor şi informaţiilor secrete de stat		
- incaperile sunt prevăzute cu:		
- pereti antifonati		
- uşi şi incuietori speciale		
- podele şi tavane speciale pentru zone sensibile		
- alte locuri unde se concentreaza date şi informaţii sau se desfăşoară activităţi cu caracter secret de stat		

În legătură cu acestea se vor face precizări privind pozitia faţă de punctul de acces şi control, imprejurimi, garantiile ce le prezinta în asigurarea protectiei datelor şi informaţiilor ori activităţilor secrete de stat
.....
.....
.....

7.1.2. MASURI DE PROTECTIE FIZICA A INCAPERILOR SAU LOCURILOR UNDE SE PASTREAZA SAU SE CONCENTREAZA DATE ŞI INFORMATII SECRETE DE STAT ORI ACTIVITĂŢI CU CARACTER SECRET DE STAT

	DA	NU
Zone de securitate existente:		
. Zona de securitate clasa I / II (pentru gestionarea informaţiilor secrete de stat)		
- perimetrul este clar definit şi protejat, având toate intrarile şi iesirile controlate		
- accesul persoanelor neautorizate este permis conform prevederilor interne, cu escorta sau prin controale specifice		
. Zona administrativa (pentru manipularea şi depozitarea informaţiilor SECRETE DE SERVICIU)		
- perimetrul ofera posibilitatea de control al personalului şi/sau vehiculelor		
- sunt utilizate:		
. registre şi jurnale speciale pentru corespondenta, evidenta, transport etc.		
. mape speciale de pastrare		
. sigilii		
. fise de predare-primire		
. ecusoane de acces		
. mobila de birou adecvata zonei administrative		

7.1.3. PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ŞI DE TELECOMUNICATII DESTINAT PRELUARII, PRELUCRARII, STOCARII ŞI TRANSMISIEI DE DATE ŞI INFORMATII SECRETE DE STAT

Echipament de comunicatie şi de birotica existent (telefoane, fax, telex, xerox)

- în zona de securitate clasa I

- în zona de securitate clasa a II-a

Echipament informatic

- aveti acces la Internet		
- este utilizat un sistem de securizare		
. pe server-ul principal		
. la nivel de utilizator		

7.1.4. MASURI PROCEDURALE DE PROTECTIE A INFORMATIILOR SECRETE DE STAT SAU A ACTIVITĂŢILOR CU CARACTER SECRET DE STAT		
Aveti elaborate proceduri privind:		
- clasificarea informaţiilor după niveluri de securitate		
- accesul pentru personalul propriu		
- accesul pentru personalul din afara, inclusiv straini şi reprezentanti ai mass-media		
- multiplicarea, transportul şi circulatia documentelor în interiorul şi în afara institutiei, atât în timpul, cat şi în afara programului de lucru		
- protectia sistemului/subsistemului informatic şi de telecomunicatii		
- controlul intern, activitatea de analiza şi evaluare a modului în care se respecta prevederile legale în vigoare, din care să reiasă periodicitatea controalelor, cine le executa, documentele ce se intocmesc şi cum se valorifica, raspunderi şi sancţiuni		
- instruirea personalului autorizat a avea acces		

7.2. PROTECTIA PERSONALULUI

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZA SA AIBA ACCES LA INFORMATII SECRETE DE STAT							
NR. CRT.	NUME, PRENUME PARINTI	PRENUME	DATA, LOC NASTERE	PROFESIE, FUNCTIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVATII **)

**) Se va inscrie ca menţiune dacă are/urmeaza să aibă acces şi orice alte observatii considerate necesare.

8. DATE CU PRIVIRE LA PROCESE PENALE SAU CONTRAVENTII CA URMARE A INCALCARII LEGILOR

	DA	NU
În ultimii 10 ani a fost declansata împotriva intreprinderii dvs. o actiune în justiţie care să se fi soldat printr-o hotărâre definitivă ce a afectat grav activitatea acesteia?		

În caz de răspuns afirmativ, precizati când, de ce, denumirea instanţei judecătoreşti, sentinta, pedeapsa şi perioada de executare.

În ultimii 5 ani intreprinderea pe care o conduceti a fost acuzata de incalcarea legii şi, drept urmare, sa fiti sanctionat cu amendă?		

În caz de răspuns afirmativ, aratati când, cum, de ce, autoritatea care a constatat fapta şi cuantumul amenzii.

Orice schimbare referitoare la datele cuprinse în chestionar se transmite imediat sub forma de completare la chestionar.

Functia, numele, prenumele şi semnatura conducătorului unităţii solicitante.....

Stampila unităţii solicitante.....

Localitatea şi data completarii chestionarului

.....

ANGAJAMENT

Subsemnatul(a).....
(numele, initiala tatalui, prenumele - cu majuscule)
în calitate de ..... la .....
(functia) (denumirea completa a institutiei/agentului economic)
cu sediul în .....
(adresa completa)
certific pe propria-mi raspundere ca informaţiile declarate în prezentul chestionar sunt exacte.
Declar că personalul angajat care are / va avea acces la informaţii secrete de stat a luat la cunoştinţa de prevederile legale referitoare la protectia informaţiilor secrete de stat şi ma angajez ca le voi respecta.
Am cunoştinţa de faptul ca, dacă, prin imprudenta şi/sau neglijenta noastra, o informatie, un procedeu sau un fisier al cărui depozitar

suntem şi care are un nivel de clasificare, va fi distrus, deturnat, sustras, reprodus sau adus la cunoştinţa fie publicului, fie unei persoane neautorizate, cei vinovati vor suporta consecintele potrivit legislaţiei în vigoare.

Data..... Semnatura .....

+ Anexa 26

Secret de serviciu
(după completare)

(SE COMPLETEAZA NUMAI PENTRU ELIBERAREA CERTIFICATULUI DE SECURITATE INDUSTRIALA DE NIVEL "SECRET")

CHESTIONAR
de securitate industriala

Autorizare pentru nivelul de securitate:
[] SECRET

1. AGENTUL ECONOMIC SOLICITANT

Denumirea completa:

Nr. din Registrul Comerţului:

Data ultimei actualizari la Registrul Comerţului:

Denumiri anterioare (dacă este cazul):

Cod fiscal: Cod SIRUES:

Stare Firma

Adresa completa pentru sediul social:
Str. ..... nr. ....
Sectorul/judeţul..... localitatea .....
Nr. telefon ..... fax: .....
Telex ..... e-mail .....
Adresa site Internet.....
Cod postal (Casuta postala, dacă este cazul): .....

Adrese anterioare (dacă este cazul):

Statutul juridic:

Forma de proprietate:

Capitalul
Capitalul social: .....
Data ultimei modificari a capitalului social: .....
Capitalul subscris varsat: .....
Capital disponibil .....
Nr. acţiuni/părţi sociale: .... Valoarea unei acţiuni/ părţi sociale:.....
Actiune nominativa. Exista? [] Da [] Nu
Autoritatea/persoana care o detine .....
Adresa site Internet.....
Crestere preconizata ..... la data de: .....
Organigrama societatii (se ataseaza la chestionar)

Actionari persoane fizice (care deţin peste 5 % din capitalul social)
Numar .....
1. Nume, prenume .....
Data şi locul nasterii .....
Nr. şi seria actului de identitate .....
Adresa completa:
Str. ..... nr. .....
Sectorul/judeţul ..... localitatea .....
Nr. telefon ..... fax: .....
Telex ..... e-mail .....
Adresa site Internet.....
Cod postal (Casuta postala, dacă este cazul): .....
Tara .....
Procentul de acţiuni/ părţi sociale detinut __% începând cu anul:

(În cazul în care sunt mai mulţi, se pot prezenta în anexa după prezentul model)

Actionari persoane juridice:
.....
.....

Agenti economici la care firma solicitanta este acţionar
Numărul de agenti economici: .....

Ce reprezinta pentru dvs.?
[] Furnizor
[] Client
[] Altceva

Procentul de acţiuni/părţi sociale detinut _____% începând cu anul:.....

Firmele la care persoane din consiliul de administratie sunt actionari:
1. Numele şi prenumele persoanei:
Denumirea completa a firmei:
Nr. din Registrul Comerţului

2. AUTORIZAREA DEJA OBTINUTA

Autorizatie: [] Da [] Nu

Numărul şi seria autorizatiei de securitate:
.....

Valabila de la: ..... la .....

Autoritatea emitenta: .....

3. CONDUCEREA INTREPRINDERII ŞI FUNCTIONARUL /
STRUCTURA DE SECURITATE RESPONSABIL/RESPONSABILA

Director general
Nume şi prenume: .....
Prenumele tatalui .....
Data numirii în functie: .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa)

Director economic
Nume şi prenume: .....
Prenumele tatalui .....
Data numirii în functie .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara.....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa)

Director ştiinţific/tehnic/comercial
Nume şi prenume: .....
Prenumele tatalui .....
Data numirii în functie: .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
Membrii Consiliului de Administratie
1. Nume şi prenume: .....
Prenumele tatalui .....
Data numirii în functie .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara.....
Firme la care este [] acţionar, [] în conducere, [] proprietar

(denumire, adresa completa):a)
b)
c)....
2.
3.
4.
5.
6.

Functionarul / Structura de securitate responsabil/responsabila cu protectia
informaţiilor secrete de stat din intreprinderea solicitanta:
Nume şi prenume: .....
Prenumele tatalui .....
Functia: .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa)
(Datele de la aceasta rubrica se vor completa de către toate persoanele din
structura de securitate a agentului economic.)

4. DATE DESPRE PROFILUL ŞI ACTIVITATEA DESFASURATA

Obiectul(ele) principal(e) de activitate:

Numar de angajaţi permanent:

Intreprinderea dvs. este distribuitorul autorizat al altor agenti
economici? (situaţia în ultimii 5 ani)
.

[] Da [] Nu

Numele şi adresa completa (dacă este cazul)

Marci înregistrate
Nume şi descriere (ce reprezinta)

Cărui tip de clienti se adreseaza activitatea/serviciile/produsele dvs.?

5. BONITATE ŞI GARANTII BANCARE

Bănci cu care lucrati (se vor completa urmatoarele informaţii pentru fiecare banca):
Denumire: .....
Adresa completa:
Str. ..... nr. .....
Sectorul/judeţul ..... localitatea .....
Nr. telefon ..... fax: .....
Telex ..... e-mail .....
Adresa site Internet.....
Numar cont: .....
Data deschiderii contului: .....
Creditul este: [] garantat [] negarantat
Marimea creditului:.....

Mijloace de plată la cumparare
[] acreditiv [] ordin de plată [] transfer bancar [] condiţii speciale
[] Altele:.....

Exista reclamatii împotriva firmei pentru plăţile cu furnizorii sau clientii?

[] Da [] Nu

Dacă DA:
Numărul reclamatiilor:
Data înregistrării:
.....
.....

Pentru suma de (valoarea fiecarei plati contestate):
Reclamatia a fost rezolvata? [] Da [] Nu
Alte comentarii legate de aceasta:

6. SCURT RAPORT PENTRU ULTIMII 3 ANI DE EXERCITIU FINANCIAR

Sfârşit perioada financiară			
Active fixe - TOTAL			
Conturi în lei:			
Conturi în valută:			
Creante:			
Stocuri:			
Active circulante - TOTAL:			
Capital social:			
Capital varsat:			
Iprumuturi pe termen lung:			
Imprumuturi pe termen scurt			
Furnizori şi conturi asimilate:			
Datorii - TOTAL			
Total pasiv:			
Cifra de afaceri:			
Total venituri			
Total cheltuieli:			
Profit brut:			
Pierderi (unde este cazul):			
Venituri din export			

Trezoreria neta:

7. INFORMATII DE SECURITATE

	DA	NU
Considerati ca firma dumneavoastra a atras atenţia unui serviciu de informaţii sau de securitate strain?		
Au existat cazuri când au fost solicitate informaţii cu caracter sensibil în afara atribuţiilor de serviciu?		
Intreprinderea sau vreunul dintre angajaţi a fost implicat(a) sau a sprijinit activităţi de: - spionaj - terorism - sabotaj?		
Ati avut vreodata angajaţi care au sprijinit sau au fost implicati în una dintre activităţile de mai sus?		
Aveti cunoştinţa de orice alte împrejurări, condiţii (factori de risc), nedeclarate în raspunsurile precedente, care au putut influenţa activitatea dvs. sau a personalului din subordine, cum ar fi: obisnuinta utilizarii unor substante psihotrope, dependenta de alcool, dificultati financiare deosebite?		

8. DATE REFERITOARE LA SISTEMUL DE PROTECTIE INFORMATIILOR SECRETE DE STAT
8.1. PROTECTIA INFORMATIILOR

	DA	NU
8.1.1. LOCUL/LOCURILE UNDE SE CONCENTREAZA DATE ŞI INFORMATII SECRETE DE STAT		
- incapere destinata numai protectiei informaţiilor		
- incapere destinata numai sistemului/subsistemului de calcul destinat preluării, prelucrarii, stocarii şi transmisiei datelor şi informaţiilor secrete de stat		
- incaperile sunt prevăzute cu: - pereti antifonati - uşi şi incuietori speciale - podele şi tavane speciale pentru zone sensibile		
- alte locuri unde se concentreaza date şi informaţii sau se desfăşoară activităţi cu caracter secret de stat		

În legătură cu acestea se vor face precizări privind pozitia faţă de punctul de acces şi control, imprejurimi, garantiile ce le prezinta în asigurarea protectiei datelor şi informaţiilor ori activităţilor secrete de stat.
.....
.....

	DA	NU
8.1.2. MASURI DE PROTECTIE FIZICA A INCAPERILOR SAU LOCURILOR UNDE SE PASTREAZA SAU SE CONCENTREAZA DATE ŞI INFORMATII SECRETE DE STAT ORI ACTIVITĂŢI CU CARACTER SECRET DE STAT		
Zone de securitate existente: . Zona de securitate clasa a II-a (pentru gestionarea informaţiilor până la nivelul SECRET, cu acces neautorizat conform prevederilor interne, cu escorta sau prin controale specifice)		
- perimetrul este clar definit şi protejat, având toate intrarile şi iesirile controlate		
- accesul persoanelor neautorizate este permis conform prevederilor interne, cu escorta sau prin controale specifice		
. Zona administrativa (pentru manipularea şi depozitarea informaţiilor SECRETE DE SERVICIU)		
- perimetrul ofera posibilitatea de control al personalului şi/sau al vehiculelor		
- sunt utilizate:		
. registre şi jurnale speciale pentru corespondenta, evidenta, transport etc.		
. mape speciale de pastrare		
. sigilii		
. fise de predare-primire		
. ecusoane de acces		
. mobila de birou adecvata zonei administrative		
8.1.3. PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ŞI DE TELECOMUNICATII DESTINAT PRELUARII, PRELUCRARII, STOCARII ŞI		

TRANSMISIEI DE DATE ŞI INFORMATII SECRETE DE STAT
Echipament de comunicatie şi de birotica existent (telefoane, fax, telex, xerox)
- în zona de securitate clasa I
- în zona de securitate clasa a Îl-a
Echipament informatic

- aveti acces la Internet		
- este utilizat un sistem de securizare		
. pe server-ul principal		
. la nivel de utilizator		

8.1.4. MASURI PROCEDURALE DE PROTECTIE A INFORMATIILOR SECRETE DE STAT SAU A ACTIVITĂŢILOR CU CARACTER SECRET DE STAT		
Aveti elaborate proceduri privind:		
- clasificarea informaţiilor după niveluri de securitate		
- accesul pentru personalul propriu		
- accesul pentru personalul din afara, inclusiv straini şi reprezentanti ai mass-media		
- multiplicarea, transportul şi circulatia documentelor în interiorul şi în afara institutiei, atât în timpul, cat şi în afara programului de lucru		
- protectia sistemului/subsistemului informatic şi de telecomunicatii		
- controlul intern, activitatea de analiza şi evaluare a modului în care se respecta prevederile legale în vigoare, din care să reiasă periodicitatea controalelor, cine le executa, documentele ce se intocmesc şi cum se valorifica, raspunderi şi sancţiuni		
- instruirea personalului autorizat a avea acces		

8.2. PROTECTIA PERSONALULUI

LISTA PERSOANELOR CARE AU ACCES SAU URMEAZA SA AIBA ACCES LA INFORMATII SECRETE DE STAT							
NR. CRT.	NUME, PRENUME PARINTI	PRENUME NASTERE	DATA, LOC FUNCTIE	PROFESIE, TELEFON	DOMICILIU, ACCES	NIVEL DE **)	OBSERVATII

**) Se va inscrie ca menţiune dacă are/urmeaza să aibă acces şi orice alte observatii considerate necesare.

9. DATE CU PRIVIRE LA PROCESE PENALE SAU CONTRAVENTII CA URMARE A INCALCARII LEGILOR

	DA	NU
În ultimii 10 ani a fost declansata împotriva intreprinderii dvs. o actiune în justiţie?		

În caz de răspuns afirmativ, precizati când, de ce, denumirea instanţei judecătoreşti, sentinta, pedeapsa şi perioada de executare.

În ultimii 5 ani intreprinderea pe care o conduceti a fost acuzata de incalcarea legii?		

În caz de răspuns afirmativ, aratati când, cum, de ce, autoritatea care a constatat fapta şi cuantumul amenzii.

Orice schimbare referitoare la datele cuprinse în chestionar se transmite imediat sub forma de completare la chestionar.

Functia, numele, prenumele şi semnatura
conducătorului unităţii solicitante.....
Stampila unităţii solicitante.....
Localitatea şi data completarii chestionarului
.....

ANGAJAMENT

Subsemnatul(a).....
(numele, initiala tatalui, prenumele - cu majuscule)
în calitate de ..... la .....
(functia) (denumirea completa a institutiei/agentului economic)
cu sediul în .....
(adresa completa)
certific pe propria-mi raspundere ca informaţiile declarate în prezentul chestionar sunt exacte.
Declar că personalul angajat care are / va avea acces la informaţii secrete de stat a luat la cunoştinţa de prevederile legale referitoare la protectia informaţiilor secrete de stat şi ma angajez ca le voi respecta.
Am cunoştinţa de faptul ca, dacă, prin imprudenta şi/sau neglijenta noastra, o informatie, un procedeu sau un fisier al cărui depozitar suntem şi care are un nivel de clasificare va fi distrus, deturnat, sustras, reprodus sau adus la cunoştinţa fie publicului, fie unei persoane neautorizate, cei vinovati vor suporta consecintele potrivit legislaţiei în vigoare.

Data..... Semnatura.....

+ Anexa 27

Secret de serviciu
(după completare)

(SE COMPLETEAZA NUMAI PENTRU ELIBERAREA CERTIFICATULUI DE SECURITATE INDUSTRIALA DE NIVEL "STRICT SECRET" ŞI "STRICT SECRET DE IMPORTANŢA DEOSEBITĂ")

Observatie! Pentru nivelul "STRICT SECRET DE IMPORTANŢA DEOSEBITĂ" se completeaza şi rubricile cu " * ".

CHESTIONAR
de securitate industriala

Autorizare pentru nivelul de securitate:
[] STRICT SECRET
*[] STRICT SECRET DE IMPORTANŢA DEOSEBITĂ

1. AGENTUL ECONOMIC SOLICITANT

Denumirea completa:

Nr. din Registrul Comerţului:

Data ultimei actualizari la Registrul Comerţului:

Denumiri anterioare (dacă este cazul):

Cod fiscal: Cod SIRUES:

Stare Firma

Adresa completa pentru sediul social:
Str. ..... nr. ....
Sectorul/judeţul..... localitatea .....
Nr. telefon ..... fax: .....
Telex ..... e-mail .....
Adresa site Internet.....
Cod postal (Casuta postala, dacă este cazul): .....

Adrese anterioare (dacă este cazul):

Statutul juridic:

Forma de proprietate:

Capitalul
Capitalul social: .....
Data ultimei modificari a capitalului social: .....
Capitalul subscris varsat: .....
Capital disponibil .....
Nr. acţiuni/părţi sociale: .... Valoarea unei acţiuni/ părţi sociale:.....
Actiune nominativa. Exista? [] Da [] Nu
Autoritatea/persoana care o detine .....
Adresa site Internet.....
Crestere preconizata ..... la data de: .....
Organigrama societatii (se ataseaza la chestionar)

Asociaţi persoane fizice (care deţin peste 5 % din capitalul social)
Numar .....

1. Nume, prenume .....
Data şi locul nasterii .....
Nr. şi seria actului de identitate .....
Adresa completa:
Str. ..... nr. .....
Sectorul/judeţul ..... localitatea .....
Nr. telefon ..... fax: .....
Telex ..... e-mail .....
Adresa site Internet.....
Cod postal (Casuta postala, dacă este cazul): .....
Tara .....
Procentul de acţiuni/ părţi sociale detinut __% începând cu anul:
(În cazul în care sunt mai mulţi, se pot prezenta în anexa după prezentul model)

Asociaţi persoane juridice
Se completeaza un chestionar identic cu cel al agentului economic solicitant, până la capitolul 7 inclusiv, de către actionarii care nu deţin autorizatie/certificat de securitate.

* Agenti economici la care firma solicitanta este asociata
Numărul de agenti economici: .....
Pentru fiecare agent economic se vor completa urmatoarele date:
Denumirea: .....
Adresa completa:
Str. ..... nr. .....
Sectorul/judeţul ..... localitatea.....
Nr. telefon ..... fax: .....
Telex ..... e-mail .....
Adresa site Internet.....
Cod postal (casuta postala, dacă este cazul): .....
Tara .....

Ce reprezinta pentru dvs.?
[] Furnizor
[] Client
[] Altceva
Procentul de acţiuni / părţi sociale detinut __% începând cu anul: .....

*Firmele la care persoane din consiliul de administratie sunt actionari
1. Numele şi prenumele persoanei:
Denumirea completa a firmei:
Nr. din Registrul Comerţului

2. NIVELUL DE AUTORIZARE DEJA OBTINUT

Autorizatie / Certificat obţinut [] Da [] Nu

Nivelul de acces al certificatului detinut:
[]

Seria şi numărul autorizatiei / certificatului de securitate:
.....

Valabil de la: ..... la .....

Autoritatea emitenta: .....

3. CONDUCEREA INTREPRINDERII ŞI FUNCTIONARUL / STRUCTURA DE SECURITATE

Director general
Nume şi prenume: .....
Prenumele tatalui .....
Data numirii în functie: .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa)

Director economic
Nume şi prenume: .....
Prenumele tatalui .....
Data numirii în functie .....
Pregatire profesionala .....
Data nasterii: .....locul:.....tara.....
Firme la care este [] acţionar, [] în conducere, [] proprietar

(denumire, adresa completa)

Director ştiinţific/tehnic/comercial
Nume şi prenume: .....
Prenumele tatalui .....
Data numirii în functia: .....
Pregatire profesionala .....
Data nasterii: ..... locul: ..... tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa)

Membrii consiliului de administratie
1. Nume şi prenume: .....
Prenumele tatalui .....

Data numirii în functie .....
Pregatire profesionala .....
Data nasterii: ..... locul: ..... tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa): a)
b)
c)...
2.
3.
4.
5.
6.

Functionarul/Structura de securitate responsabil/responsabila
cu protectia informaţiilor clasificate din institutia solicitanta:
Nume şi prenume: .....
Prenumele tatalui .....
Functia: .....
Pregatire profesionala .....
Data nasterii: ..... locul: ..... tara .....
Firme la care este [] acţionar, [] în conducere, [] proprietar
(denumire, adresa completa)

(Datele de la aceasta rubrica se vor completa de către toate
persoanele din structura de securitate a agentului economic.)

*4 SUCURSALE, FILIALE SAU PUNCTE DE LUCRU

* Denumire completa:

Denumiri anterioare (dacă este cazul):	Datele schimbarilor

* Adresa completa:
Str. ..... nr. .....
Sectorul/judeţul ..... localitatea ....
Nr. telefon ..... fax: .....
Telex ..... e-mail .....
Adresa site Internet .....
Cod postal (casuta postala, dacă este cazul): .....
Tara .....

Adrese anterioare (dacă este cazul):

*Forma de detinere a spatiului:	[] proprietate Numărul actului şi forma juridica:	[] inchiriata De la (denumire, adresa completa):

* Agentul economic detine:
[] birouri [] magazine [] hoteluri [] fabrici [] depozite
[] ateliere [] laboratoare [] santiere [] spatii de prezentare
[] camere securizate Altele:

* Descrierea amplasamentului sediului:
[] zona comerciala centrala [] zona comerciala periferica [] zona rurala
[] zona industriala [] incinta comerciala [] zona rezidentiala

* Spatii subinchiriate altor agenti economici, cu specificarea
denumirii şi obiectului lor de activitate:

5. DATE DESPRE PROFILUL ŞI ACTIVITATEA DESFASURATA

Obiectul(ele) principal(e) de activitate:

Numar de angajaţi permanent:
Cu studii superioare:
Cu studii medii:
Personal auxiliar:

Numar de colaboratori
Persoane fizice .....
Persoane juridice .....

* Vanzari la intern (situaţia în ultimii 5 ani)
Procentul din vanzarile totale .....
Termenele de livrare (în zile) .....
Condiţii de plată (numerar, cec, ordin de plată, cont curent etc.)
.....

* Importuri (situaţia în ultimii 5 ani)
Procentul importurilor la realizarea produselor .....
Ce se importa (materie prima şi/sau ansamble, subansamble,
produse finite).....

Tarile de unde se importa: |
..... |
Termene de import (în zile) ..... |
Condiţii de plată (numerar, cec, ordin de plată, cont curent etc.) |
..... |

* Exporturi (situaţia în ultimii 5 ani) |
Procent din activitate reprezentat de importuri: ..... |
Ce se exporta (materie prima şi/sau ansamble, subansamble, |
produse finite) ..... |
Tarile în care se exporta: ..... |
Termene de export (în zile) ..... |
Condiţii de plată (numerar, cec, ordin de plată, cont curent etc.) |
..... |

Institutia dvs. este distribuitorul autorizat al altor agenti |
economici? (situaţia în ultimii 5 ani) |

[] Da [] Nu |

Numele şi adresa completa (dacă este cazul) |

Marci înregistrate |
Nume şi descriere (ce reprezinta) |

Caror tip de clienti se adreseaza |
activitatea/serviciile/produsele dvs.? |

* Principalii clienti cu care institutia dvs. are contract (denumire, adresa completa)	Valoarea fiecarui contract	Perioada

6. BONITATE ŞI GARANTII BANCARE

Bănci cu care lucrati (se vor completa urmatoarele informaţii |
pentru fiecare banca): |

Denumire: ..... |
Adresa completa: |
Str. ..... nr. ..... |
Sectorul/judeţul ..... localitate ..... |
Nr. telefon ..... fax: ..... |
Telex ..... e-mail ..... |
Adresa site Internet ..... |
Numar cont: ..... |
Data deschiderii contului: ..... |
Creditul este: [] garantat [] negarantat |
Marimea creditului: ..... |
Natura garantiei (dacă este credit "garantat"): |

* Creditul este utilizat în totalitate? [] Da [] Nu |
* Banca a acordat facilitatea de neacoperire a contului? [] Da [] Nu |
* Dacă DA, până la ce suma poate merge neacoperirea: ..... |
* Dacă DA, aceasta facilitate este folosita? [] Da [] Nu |

Mijloace de plată la cumparare |

[] acreditiv [] ordin de plată [] transfer bancar [] condiţii speciale |
[] Altele:..... |

Exista reclamatii împotriva firmei? |

[] Da [] Nu |

Dacă DA: |

Numărul reclamatiilor: .....
Data înregistrării:
.....
.....

Pentru suma de (valoarea fiecarei plati contestate):

Reclamatia a fost rezolvata: [] Da [] Nu

Alte comentarii legate de aceasta:

* Planuri viitoare (noi investitii, patrundere pe noi piete etc.)

7. SCURT RAPORT PENTRU ULTIMII 3 ANI DE EXERCITIU FINANCIAR

Sfârşit perioada financiară			
Active fixe - TOTAL			
Conturi în lei:			
Conturi în valută:			
Creante:			
Stocuri:			
Active circulante - TOTAL:			
Total active:			
Capital social:			
Capital varsat:			
Capitaluri proprii:			
Imprumuturi pe termen lung:			
Imprumuturi pe termen scurt			
Furnizori şi conturi asimilate:			
Datorii - TOTAL			
Total pasiv:			
Cifra de afaceri:			
Total venituri			
Total cheltuieli:			
Profit brut:			
Pierderi (unde este cazul):			
Venituri din export			
Trezoreria neta:			

8. INFORMATII DE SECURITATE

	DA	NU
Considerati ca firma dumneavoastra a atras atenţia unui serviciu de informaţii sau de securitate strain?		
Credeti ca au fost facute presiuni asupra firmei sau angajatilor ca urmare a unui incident survenit pe teritoriul altei tari?		
Sunt mentinute relatii permanente, profesionale, personale cu cetăţeni straini ? Natura acestora.		
Au existat cazuri când au fost solicitate informaţii cu caracter sensibil în afara atribuţiilor de serviciu?		
Intreprinderea sau vreunul din angajaţi a fost implicat(a) sau a sprijinit activităţi de: - spionaj - terorism - sabotaj?		
Ati avut vreodata angajaţi care au sprijinit sau au fost implicati intr-una dintre activităţile de mai sus?		
Aveti cunoştinţa de orice alte împrejurări, condiţii (factori de risc), nedeclarate în raspunsurile precedente, care au putut influenţa activitatea dvs. sau a personalului din subordine, cum ar fi: obisnuinta utilizarii unor substante psihotrope, dependenta de alcool, dificultati financiare deosebite?		

9. DATE REFERITOARE LA SISTEMUL DE PROTECTIE A INFORMATIILOR SECRETE DE STAT

9.1. PROTECTIA INFORMATIILOR

9.1.1. LOCUL/LOCURILE UNDE SE CONCENTREAZĂ DATE şi INFORMATII SECRETE DE STAT	DA	NU
- incapere destinata numai protectiei informaţiilor secrete de stat		
- incapere destinata numai sistemului/subsistemului de calcul destinat preluării, prelucrarii, stocarii şi transmisiei datelor şi informaţiilor secrete de stat		
- incaperile sunt prevăzute cu: - pereti antifonati - uşi şi incuietori speciale - podele şi tavane speciale pentru zone sensibile		
- alte locuri unde se concentreaza date şi informaţii sau se desfăşoară activităţi cu caracter secret de stat		

În legătură cu acestea se vor face precizări privind pozitia faţă de punctul de acces şi control, imprejurimi, garantiile ce le prezinta în asigurarea protectiei datelor şi informaţiilor ori activităţilor secrete de stat

.....
.....
.....

9.1.2. MASURI DE PROTECTIE FIZICA A INCAPERILOR SAU LOCURILOR UNDE SE PASTREAZA SAU SE CONCENTREAZĂ DATE ŞI INFORMATII SECRETE DE STAT ORI ACTIVITĂŢI CU CARACTER SECRET DE STAT	DA	NU
Zone de securitate existente: Zona de securitate clasa I (pentru gestionarea informaţiilor până la nivelul STRICT SECRET DE IMPORTANŢA DEOSEBITĂ, cu acces autorizat)		
- perimetrul este clar definit şi protejat, având toate intrarile şi iesirile controlate		
- este marcată zona specificarea restrictiei şi menţionarea zonei de securitate		
- exista control al sistemului de intrare, care să permită doar accesul persoanelor autorizate pentru intrarea în zona		

(Dacă DA, descrieti sistemul(ele) de protecţie mecanica, electrica, electronică, informationala, optica, acustica etc.)

- sistemul de protecţie utilizat este omologat şi/sau aprobat de un serviciu specializat			
(Dacă DA, menţionaţi care.)			
Zona de securitate clasa a II-a (pentru gestionarea informaţiilor până la nivelul SECRET, cu acces neautorizat conform prevederilor interne, cu escorta sau prin controale specifice)			
─ perimetrul este clar definit şi protejat, având toate intrarile şi iesirile controlate			
- accesul persoanelor neautorizate este permis conform prevederilor interne, cu escorta sau prin controale specifice			
Zona administrativa (pentru manipularea şi depozitarea informaţiilor SECRETE DE SERVICIU)			
- perimetrul ofera posibilitatea de control a personalului şi/sau vehiculelor			
- sunt utilizate:			
■ registre şi jurnale speciale pentru corespondenta, evidenta, transport etc.			
■ mape speciale de pastrare			
■ sigilii			
■ fise de predare-primire			
■ ecusoane de acces			
■ mobila de birou adecvata zonei administrative			

9.1.3. PREZENTAREA SISTEMULUI/SUBSISTEMULUI INFORMATIC ŞI DE TELECOMUNICATII DESTINAT PRELUARII, PRELUCRARII, STOCARII ŞI TRANSMISIEI DE DATE ŞI INFORMATII SECRETE DE STAT			
Echipament de comunicatie şi de birotica existent (telefoane, fax, telex, xerox)			
- în zona de securitate clasa I			
- în zona de securitate clasa a II-a			
Echipament informatic			
- numar calculatoare			
- utilizati calculatoarele în retea Intranet			
- aveti acces la Internet			
- este utilizat un sistem de securizare			
■ pe server-ul principal			
■ la nivel de utilizator			
* Menţionaţi tipul server-ului principal şi distribuitorul, administratorul (în cazul în care este o firma specializata care asigura servicii), precum şi locul/locurile unde sunt amplasate calculatoarele conectate în retea la server-ul care stocheaza informaţii clasificate			
9.1.4. MASURI PROCEDURALE DE PROTECTIE A INFORMATIILOR SECRETE DE STAT SAU A ACTIVITĂŢILOR CU CARACTER SECRET DE STAT			
Aveti elaborate proceduri privind:			
- clasificarea informaţiilor după niveluri de securitate			
- accesul pentru personalul propriu			

- accesul pentru personalul din afara, inclusiv straini şi reprezentanti ai mass-media		
- multiplicarea, transportul şi circulatia documentelor în interiorul şi în afara intreprinderii, atât în timpul cat şi în afara programului de lucru		
- protectia sistemului/subsistemului informatic şi de telecomunicatii		
- controlul intern, activitatea de analiza şi evaluare a modului în care se respecta prevederile legale în vigoare, din care să reiasă periodicitatea controalelor, cine le executa, documentele ce se intocmesc şi cum se valorifica, raspunderi şi sancţiuni		
- instruirea personalului autorizat a avea acces		

9.2. PROTECTIA PERSONALULUI

9.2.1. LISTA PERSOANELOR CARE AU ACCES SAU URMEAZA SA AIBA ACCES LA INFORMATII SECRETE DE STAT

NR. CRT.	NUME, PRENUME PARINTI	PRENUME	DATA, LOC NASTERE	PROFESIE, FUNCTIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVATII**)

**) Se va inscrie ca menţiune dacă are/urmeaza să aibă acces şi orice alte observatii considerate necesare.

9.2.2. LISTA PERSOANELOR AUTORIZATE SA ADMINISTREZE SISTEMUL/SUBSISTEMUL INFORMATIC ŞI DE TELECOMUNICATII, PRECUM ŞI CEI CARE LUCREAZA IN REŢEAUA INTRANET CU ACCES LA INFORMATII SECRETE DE STAT

NR. CRT.	NUME, PRENUME PARINTI	PRENUME	DATA, LOC NASTERE	PROFESIE, FUNCTIE	DOMICILIU, TELEFON	NIVEL DE ACCES	OBSERVATII**)

**) Se va inscrie echipamentul pe care-l administreaza sau faptul ca are acces Intranet.

10. DATE CU PRIVIRE LA PROCESE PENALE SAU CONTRAVENTII CA URMARE A INCALCARII LEGILOR

În ultimii 10 ani a fost declansata împotriva intreprinderii dvs. o actiune în justiţie?	DA	NU
În caz de răspuns afirmativ precizati când, de ce, denumirea instanţei judecătoreşti, sentinta, pedeapsa şi perioada de executare.		
În ultimii 5 ani intreprinderea pe care o conduceti a fost acuzata de incalcarea legii?		
În caz de răspuns afirmativ aratati când, cum, de ce, autoritatea care a constatat fapta şi cuantumul amenzii		

Orice schimbare referitoare la datele cuprinse în chestionar se transmite imediat sub forma de completare la chestionar.

Functia, numele, prenumele şi semnatura conducătorului unităţii solicitante .....

Stampila unităţii solicitante .....

Localitatea şi data completarii chestionarului .....

ANGAJAMENT(1)

Subsemnatul(a) ...../(numele, initiala tatalui, prenumele - cu majuscule) /..... în calitate de ..../(functia)/..... la ...../(denumirea completa a institutiei/agentului economic)..... cu sediul în ...../(adresa completa)/..... certific pe propria-mi raspundere ca informaţiile declarate în prezentul

chestionar sunt exacte.
Declar că personalul angajat care are/va avea acces la informaţii secrete de stat a luat la cunoştinţa de prevederile legale referitoare la protectia informaţiilor secrete de stat şi ma angajez ca le voi respecta.
Am cunoştinţa de faptul ca, dacă, prin imprudenta şi/sau neglijenta noastra, o informatie, un procedeu sau un fisier al cărui depozitar suntem şi care are un nivel de clasificare va fi distrus, deturnat, sustras, reprodus sau adus la cunoştinţa fie publicului, fie unei persoane neautorizate, cei vinovati vor suporta consecintele potrivit legislaţiei în vigoare.
Data ..... Semnatura .....

---

(1) Se completeaza atât pentru nivelul "STRICT SECRET", cat şi pentru nivelul "STRICT SECRET DE IMPORTANŢA DEOSEBITĂ".

+ Anexa 28

ROMÂNIA
OFICIUL REGISTRULUI NAŢIONAL
AL INFORMATIILOR SECRETE DE STAT
AUTORIZATIE DE SECURITATE INDUSTRIALA
Nr. ..... din .....
Oficiul Registrului Naţional al Informaţiilor Secrete de Stat autorizeaza ...../(denumirea completa a institutiei/agentului economic) ..... pentru participarea la proceduri de negociere a unui contract, în cadrul caruia sunt gestionate informaţii clasificate.
Prezenta autorizatie este valabila până la data de .....
Directorul general al Oficiului Registrului
Naţional al Informaţiilor Secrete de Stat
.....
(semnatura, stampila)

+ Anexa 29

ROMÂNIA
OFICIUL REGISTRULUI NAŢIONAL
AL INFORMATIILOR SECRETE DE STAT
CERTIFICAT DE SECURITATE INDUSTRIALA
Nr. ..... din .....
Oficiul Registrului Naţional al Informaţiilor Secrete de Stat certifica ..../(denumirea completa a institutiei/agentului economic)/..... pentru derularea contractului în care sunt gestionate informaţii secrete de stat de nivelul ..... .
Prezentul certificat este valabil pe durata derularii contractului.
Directorul general al Oficiului Registrului
Naţional al Informaţiilor Secrete de Stat
.....
(semnatura, stampila)

+ Anexa 30

ANTETUL INSTITUTIEI/AGENTULUI ECONOMIC
Adresa ..... Tel./Fax .....
Către ORNISS
CERERE
pentru eliberarea certificatului de securitate industriala
Va rugam sa eliberati certificatul de securitate industriala nivel ..... pentru ...../(denumirea completa a institutiei/agentului economic)/..... cu sediul în .....(adresa completa)..... în vederea derularii contractului clasificat .....
Obiectul contractului este .....
.....
Beneficiarul este .....
.....
Mentionam ca în prezent intreprinderea noastra detine/nu detine autorizatie de securitate/certificat de securitate industriala pentru nivelul .....
Anexam, în original, chestionarul de securitate industriala.
Directorul institutiei/agentului economic
.....
(semnatura, stampila)

+ Anexa 31

ROMÂNIA
(Institutia)
.....
Compartimentul

.....
REGISTRUL
pentru evidenta autorizaţiilor de securitate industriala

Nr. crt.	Denumirea şi adresa completa a obiectivului industrial de secu-ritate indus-triala	Data elibe-rarii autori-zaţiei de secu-ritate indus-triala	Seria şi nr. autori-zaţiei de secu-ritate indus-triala	Perioada de vala-bilitate	Data retra-gerii	Motivul retra-gerii	Obs.

\+ Anexa 32
ROMÂNIA
(Institutia)
.....
Compartimentul
.....
REGISTRUL
pentru evidenta certificatelor de securitate industriala

Nr. crt.	Denumirea şi adresa completa a obiectivului industrial de secu-ritate indus-triala	Nivelul de acces rarii certifi-catului de secu-ritate indus-triala	Data elibe-rarii certi-ficatu-lui de secu-ritate indus-triala	Seria şi nr. de vala-bilitate	Perioada de retra-gerii	Data retra-gerii	Motivul	Obs.