Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

STANDARD NAŢIONAL din 13 iunie 2002

de protecţie a informaţiilor clasificate în România

Capitolul 1

DISPOZIȚII GENERALE

Articolul 1

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

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

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

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

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

e)regulile de identificare şi marcare, inscripționările şi menţiunile obligatorii pe documentele secrete de stat, în funcție de nivelurile de secretizare, cerinţele de evidență a numerelor de exemplare şi a destinatarilor, termenele şi regimul de păstrare, interdicţiile de reproducere şi circulație;

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

i)protecția surselor generatoare de informaţii - INFOSEC.

Articolul 2

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

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

a)Strict secret de importanţă deosebită - NATO top secret

b)Strict secret - NATO secret

c)Secret - NATO confidential

d)Secret de serviciu - NATO restricted

Articolul 3

Termenii folosiți în prezentele standarde au următorul înţeles:

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

– aviz de securitate industrială - document eliberat de către ADS prin care se atestă că obiectivul industrial contractant a implementat toate măsurile de securitate necesare protecției informaţiilor clasificate vehiculate în derularea contractului încheiat;

– certificat de securitate - document eliberat persoanei cu atribuţii nemijlocite în domeniul protecției informaţiilor clasificate, respectiv funcționarului de securitate sau salariatului din structura de securitate, care atestă verificarea şi acreditarea de a deține, de a avea acces şi de a lucra cu informaţii clasificate de un anumit nivel de secretizare;

– certificat de securitate industrială - document eliberat de ORNISS unui obiectiv industrial, prin care se atestă că este abilitat să deruleze activităţi industriale şi/sau de cercetare ce presupun accesul la informaţii clasificate;

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

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

– contractant - unitate industrială, comercială, de execuţie, de cercetare-proiectare sau prestatoare de servicii în cadrul unui contract clasificat;

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

– 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 informației clasificate de sub incidenţa reglementărilor protective prevăzute de lege;

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

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

a)hârtie - documente olografe, dactilografiate sau tipărite, schite, hărți, planșe, 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;

– funcționar de securitate - persoana care îndeplinește atribuţiile de protecţie a informaţiilor clasificate în cadrul autorităţilor, instituţiilor publice, agenților 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 evidență, accesare, procesare, multiplicare, manipulare, transport, transmitere, inventariere, păstrare, arhivare sau distrugere a informaţiilor clasificate;

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

– marcare - activitatea de inscripționare a nivelului de secretizare a informației şi de semnalare a cerințelor speciale de protecţie a acesteia;

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

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

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

– protecția surselor generatoare de informaţii - ansamblul măsurilor destinate protecției informaţiilor elaborate, stocate sau transmise prin sisteme ori rețele de prelucrare automată a datelor şi/sau de comunicații;

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

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

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

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

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

– unitate deținatoare de informaţii clasificate sau unitate - autoritate sau instituție 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 deține informaţii clasificate;

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Capitolul 2

CLASIFICAREA ŞI DECLASIFICAREA INFORMAȚIILOR. MĂSURI MINIME DE PROTECȚIE 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 naţională şi de consecințele ce s-ar produce ca urmare a dezvăluirii sau diseminării lor neautorizate.

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

a)strict secret de importanţă deosebită;

b)strict secret;

c)secret.

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

Articolul 5

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 6

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

Articolul 7

Listele cu informaţii secrete de serviciu se stabilesc de conducătorii unităţilor deținatoare 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 îndeplinirea atribuţiilor de serviciu, divulgarea lor putând prejudicia interesul unităţii.

Articolul 9

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

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

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

Articolul 12

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

– 50 de ani pentru informaţiile clasificate strict secret;

– 30 de ani pentru informaţiile clasificate secret.

(3) Termenele prevăzute la alin. (2) pot fi prelungite prin hotărâre a Guvernului, pe baza unei motivații temeinice, la solicitarea conducătorilor unităţilor deținătoare de informaţii clasificate sau, după caz, a împuterniciților şi funcționarilor superiori abilitați să atribuie nivelurile de secretizare.

Articolul 13

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

Articolul 14

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 15

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

Articolul 16

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

Articolul 17

(1) Informaţiile vor fi clasificate numai în cazul în care se impune protecția acestora, iar nivelurile de secretizare şi termenele de clasificare subzista atât timp cât dezvăluirea sau diseminarea lor neautorizată ar putea prejudicia siguranţa naţională, apărarea țării, 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, deținatorii de informaţii secrete de stat şi secrete de serviciu, stabilite astfel potrivit H.C.M. nr. 19 din 14 ianuarie 1972, vor prezenta persoanelor sau autorităţilor publice împuternicite să atribuie niveluri de secretizare propuneri privind încadrarea acestor informaţii în noi clase şi niveluri de secretizare, după caz.

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

Secţiunea a 2-a

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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 motivată a emitentului.

Articolul 20

(1) Informaţiile se declasifică dacă:

a)termenul de clasificare a expirat;

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

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

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

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

Articolul 21

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

Articolul 22

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

Articolul 23

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

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

Articolul 24

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

Secţiunea a 3-a

Măsuri minime de protecţie a informaţiilor clasificate

Articolul 25

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

a)clasele şi nivelurile de secretizare a informaţiilor;

b)volumul şi suportul informaţiilor;

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

d)amenințările, riscurile şi vulnerabilitatile ce pot avea consecințe asupra informaţiilor clasificate.

Articolul 26

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

Articolul 27

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

Articolul 28

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

Secţiunea a 4-a

Structura/funcționarul de securitate

Articolul 29

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

(4) Seful structurii de securitate, respectiv funcționarul de securitate, este un adjunct al conducătorului persoanei juridice sau un membru al consiliului de administrație al unității.

Articolul 30

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

Articolul 31

(1) Structura/funcționarul de securitate are următoarele atribuții generale:

a)elaborează și supune aprobării conducerii unității normele interne privind protecția informațiilor clasificate, potrivit legii;

b)întocmește programul de prevenire a scurgerii de informații clasificate și îl supune avizării instituțiilor abilitate, iar după aprobare, acționează pentru aplicarea acestuia;

c)coordonează activitatea de protecție a informațiilor clasificate, în toate componentele acesteia;

d)asigură relaționarea cu instituția abilitată să coordoneze activitatea și să controleze măsurile privitoare la protecția informațiilor clasificate, potrivit legii;

e)monitorizează activitatea de aplicare a normelor de protecție a informațiilor clasificate și modul de respectare a acestora;

f)consiliază conducerea unității în legătură cu toate aspectele privind securitatea informațiilor clasificate;

g)informează conducerea unității despre vulnerabilitatile și riscurile existente în sistemul de protecție a informațiilor clasificate și propune măsuri pentru înlăturarea acestora;

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

h)acordă sprijin reprezentanților autorizați ai instituțiilor abilitate, potrivit competențelor legale, pe linia verificării persoanelor pentru care se solicită accesul la informaţii clasificate;

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

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

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

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

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

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

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

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

Articolul 32

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

Secţiunea a 5-a

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Accesul la informaţiile clasificate

Articolul 33

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

Articolul 34

Persoanele care au acces la informaţii strict secrete de importanţă deosebită, în condiţiile prevăzute de prezentele standarde, vor fi înregistrate în fișa 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, cât şi periodic, cu privire la conţinutul reglementărilor privind protecția informaţiilor clasificate.

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

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

Articolul 36

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 37

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

Articolul 38

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

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

Articolul 39

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

Capitolul 3

REGULI GENERALE PRIVIND EVIDENȚA, ÎNTOCMIREA, PĂSTRAREA, PROCESAREA, MULTIPLICAREA, MANIPULAREA, TRANSPORTUL, TRANSMITEREA ŞI DISTRUGEREA INFORMAȚIILOR CLASIFICATE

Articolul 40

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

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

Articolul 41

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

b)numerele de înregistrare se înscriu pe toate exemplarele documentului şi pe anexele acestora, fiind precedate de un zero (0) pentru documentele secrete, de două zerouri (00) pentru cele strict secrete, de trei zerouri (000) pentru cele strict secrete de importanţă deosebită şi de litera "S" pentru secrete de serviciu;

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

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

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

Articolul 42

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

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

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 43

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

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

Articolul 44

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

Articolul 45

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

Articolul 46

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

(2) Nivelul de secretizare se marchează prin ștampilare, dactilografiere, tipărire sau ograf, astfel:

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 47

Porțiunile 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 aceleași 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 inscripționate, sub destinatar, cu menţiunea "Personal".

Articolul 51

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 52

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

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

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

Articolul 54

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

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

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

Articolul 55

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 56

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

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

Articolul 57

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

Articolul 58

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

Articolul 59

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

(2) Emitentii şi deținătorii de informaţii clasificate sunt obligați să înregistreze şi să țină evidența tuturor documentelor şi materialelor primite, expediate sau a celor întocmite de unitatea proprie, potrivit legii.

(3)În registrele pentru evidența 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 evidență se face consecutiv, pe parcursul unui an calendaristic.

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

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

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

Articolul 62

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 63

Hărțile, planurile topografice, asamblajele de hărți şi alte asemenea documente se înregistrează în registrele pentru evidența informaţiilor clasificate prevăzute în anexele nr. 4, 5 şi 6.

Articolul 64

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

Articolul 65

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

Articolul 66

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

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

Articolul 67

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

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

Articolul 68

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

(1) Evidenţierea operaţiunii de multiplicare se face prin marcare atât pe original, cât şi pe toate copiile rezultate.

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

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

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

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

Articolul 69

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

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

(3) Extrasul dintr-un document care conține informaţii clasificate se face în baza cererii pentru copiere, cu aprobarea conducătorului unităţii, iar documentul rezultat va avea menționat 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 dorește să aibă control exclusiv asupra reproducerii, documentul va conține o indicație vizibilă cu următorul conținut: "Reproducerea acestui document, totală sau parţială, este interzisa".

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 71

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

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

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

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

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

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

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

Articolul 72

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 73

Documentele clasificate pot fi microfilmate sau stocate pe discuri optice ori pe suporți magnetici în următoarele condiţii:

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

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

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

Articolul 74

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

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

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

Articolul 75

În cazul în care un document secret de stat este studiat de o persoană abilitată, pentru care s-a stabilit necesitatea de a accesa astfel de documente în vederea îndeplinirii sarcinilor de serviciu, această activitate trebuie consemnată în fișa de consultare, conform modelului din anexa nr. 1.

Articolul 76

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

Articolul 77

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

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

Articolul 78

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

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 79

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

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

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 într-o formă de evidență.

Articolul 81

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

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

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

Articolul 82

Conducătorii unităţilor deținătoare de informaţii clasificate vor desemna, din structura de securitate proprie, în condiţiile prezentelor standarde, cel puţin un delegat împuternicit

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

pentru transportul şi executarea operaţiunilor de predare-primire a corespondenței clasificate, între aceasta şi unitatea specializată a Serviciului Român de Informaţii.

Capitolul 4

PROTECȚIA INFORMAȚIILOR SECRETE DE STAT

Secţiunea 1

Obligaţiile şi răspunderile ce revin autorităţilor şi instituţiilor publice, agenților economici şi altor persoane juridice pentru protecția informaţiilor secrete de stat

Articolul 83

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

Articolul 84

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

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

Articolul 85

Până la înființarea şi organizarea structurii de securitate sau, după caz, până la numirea funcționarului de securitate, conducătorii unităţilor deținătoare de informaţii secrete de stat vor desemna o persoană care să îndeplinească temporar atribuţiile specifice protecției informaţiilor clasificate, prin cumul de funcții.

Articolul 86

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

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

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

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

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

j)să întocmeasca ghidul pe baza căruia se va realiza încadrarea corectă şi uniforma în nivelurile de secretizare a informaţiilor secrete de stat, în strictă conformitate cu legea şi

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

să îl prezinte, spre aprobare, împuterniciților și funcționarilor superiori abilitați prin lege să atribuie nivelurile de secretizare;

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

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

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

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

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

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

Secţiunea a 2-a

Protecția juridică

Articolul 87

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

Articolul 88

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

(2)Înștiințarea prevăzută la alin. (1) se face în scopul obținerii sprijinului necesar pentru recuperarea informaţiilor, evaluarea prejudiciilor, diminuarea şi înlăturarea consecințelor.

(3)Înștiințarea 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;

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

c)precizări cu privire la eventuala informare a emitentului.

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

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

Articolul 89

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

Articolul 90

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

a)dacă informaţiile respective au fost compromise;

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

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

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

(3)În cazul săvaârșirii de infracțiuni la protecția secretului de stat, unitatile deținătoare au obligaţia de a sesiza organele de urmărire penală şi de a pune la dispoziţia acestora datele şi materialele necesare probării faptelor.

Articolul 91

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

(1) Structura/funcționarul de securitate are obligaţia de a tine evidența cazurilor de încălcare a reglementărilor de securitate, a documentelor de cercetare şi a măsurilor de solutionare şi să le pună la dispoziţia autorităţilor desemnate de securitate, conform competențelor 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 deținător sau cele determinate de conţinutul informaţiilor secrete de stat, inclusiv drepturile patrimoniale ce revin emitentului din contractele de cesiune şi licență, precum şi litigiile referitoare la nerespectarea dispoziţiilor legale privind dreptul de autor şi drepturile conexe, invențiile şi inovațiile, protecția modelelor industriale, combaterea concurenței neloiale şi a celor stipulate în tratatele, acordurile şi înţelegerile la care România este parte, sunt de competenţa instanţelor judecătorești.

Secţiunea a 3-a

Protecția prin măsuri procedurale

Articolul 93

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

Articolul 94

(1)Măsurile procedurale de protecţie a informaţiilor secrete de stat vor fi integrate în programul de prevenire a scurgerii de informaţii clasificate, întocmit potrivit anexei nr. 10, care va fi prezentat, spre avizare, autorităţii abilitate să coordoneze activitatea şi să controleze măsurile privitoare la protecția informaţiilor clasificate, potrivit legii.

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 95

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

Secţiunea a 4-a

Protecția fizică

Articolul 96

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

Articolul 97

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

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

b)tipul containerelor în care sunt depozitate informaţiile;

c)caracteristicile clădirii şi zonei de amplasare.

Articolul 98

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

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

– reguli de însoţire, supraveghere şi prevenire a accesului persoanelor neautorizate la informaţii clasificate.

Articolul 99

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

Articolul 100

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

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 recunoaștere individuală aplicat personalului.

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

(2) Unităţile deţinătoare de informaţii secrete de stat vor institui un sistem propriu de control al vizitatorilor, destinat interzicerii accesului neautorizat al acestora în zonele de securitate.

Articolul 102

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

Articolul 103

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

Articolul 104

Personalul inclus în sistemul de pază şi apărare a obiectivelor, sectoarelor şi locurilor în care sunt gestionate informaţii secrete de stat trebuie să deţină autorizație de acces corespunzător nivelului de secretizare a informaţiilor necesare îndeplinirii 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 distanță, în locurile în care se află informaţii secrete de stat.

Articolul 106

Conducătorii unităţilor deținătoare de informaţii secrete de stat vor stabili reguli cu privire la circulația şi ordinea interioară în zonele de securitate, astfel încât accesul să fie permis exclusiv posesorilor de certificate de securitate şi autorizaţii de acces, cu respectarea principiului necesităţii de a cunoaște.

Articolul 107

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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 însemne sau echipamente specifice.

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

(3) Evidența legitimațiilor, permiselor şi a altor însemne şi echipamente distinctive va fi ţinută de structura/funcționarul de securitate al unităţii.

Articolul 109

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

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

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

Articolul 110

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

Articolul 111

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

(1) Permisele de acces vor fi individualizate prin aplicarea unor semne distinctive.

(2) Permisele de acces se vizează semestrial.

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

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 administrativă sau în zonele de securitate este permis numai dacă sunt însoțite de persoane anume desemnate, cu bilet de intrare eliberat pe baza documentelor de legitimare de conducătorul unității.

Articolul 114

(1) Accesul angajaților agenților economici care efectuează lucrări de construcții, reparații şi întreţinere a clădirilor, instalaţiilor sau utilităților 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 reprezentanților autorizați ai agenților economici în cauză.

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

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

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

Articolul 115

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Reprezentanții instituţiilor care, potrivit competențelor legale, au atribuţii de coordonare şi control pe linia protecției informaţiilor clasificate au acces la obiectivele, sectoarele şi locurile în care sunt gestionate informaţii clasificate, pe baza legitimației de serviciu şi a delegației speciale, semnată de conducătorul autorității pe care o reprezintă.

Articolul 116

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

Articolul 117

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

Articolul 118

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

Articolul 119

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

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

Articolul 120

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

d)planul de evacuare a documentelor şi modul de acțiune în caz de urgență;

e)procedura de raportare, cercetare şi evidență 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 păstrarea informaţiilor strict secrete de importanţă deosebită în zona de securitate clasa I;

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

Articolul 122

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

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

Articolul 123

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 124

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

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

Articolul 125

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

Articolul 126

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

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

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

c)grupa C - încuietori pentru mobilierul de birou.

Articolul 127

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

Articolul 128

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 129

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

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

Articolul 130

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

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

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

Articolul 131

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

Articolul 132

Cheile şi combinațiile încuietorilor vor fi schimbate:

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

b)de fiecare dată când se constată că au intervenit situaţii de natură să le facă vulnerabile;

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

Articolul 133

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

Articolul 136

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

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

Articolul 137

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 138

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

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

Articolul 139

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

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

Secţiunea a 5-a

Protecția personalului

Articolul 140

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

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

Articolul 141

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

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

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

(4)În funcție de avizul comunicat de autoritatea desemnată, ORNISS va aproba eliberarea certificatului de securitate sau autorizației de acces şi va încunoștiința oficial conducătorul unităţii.

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 142

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

Articolul 143

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

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

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

c)pot fi vulnerabile la acţiuni ostile, ca urmare a importanței funcției în care vor fi numite, a mediului de relații sau a locului de muncă anterior.

Articolul 144

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

(2)Când persoanele urmează să îndeplinească funcții 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

Unitățile care gestionează informaţii clasificate sunt obligate să țină un registru de evidență a certificatelor de securitate şi autorizaţiilor de acces la informaţii clasificate - anexa nr. 18.

Articolul 146

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 147

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

Articolul 148

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

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

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

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

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

Articolul 149

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 150

(1) După primirea formularelor, instituția abilitată va efectua verificările în termenele prevăzute la art. 148 şi va comunica, în scris - anexa nr. 20, la ORNISS, avizul privind acordarea certificatului de securitate sau autorizației 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 protecției 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 lucrătoare de la primirea răspunsului de la autoritatea desemnată de securitate, ORNISS va decide asupra acordării certificatului de securitate/autorizației de acces la informaţii secrete de stat şi va comunica unității solicitante - anexa nr. 21.

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

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

Articolul 152

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

a)Serviciul Român de Informaţii, pentru:

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

– personalul propriu;

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

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

– personalul din cadrul Parchetului Naţional Anticorupție.

b)Ministerul Apărării Naţionale, pentru:

– personalul militar şi civil propriu;

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

c)Serviciul de Informaţii Externe, pentru:

– personalul militar sau civil propriu;

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

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

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

Litera d) a alin. (1) al art. 152 a fost modificată de pct. 3 din HOTĂRÂREA nr. 2.202 din 30 noiembrie 2004, publicată în MONITORUL OFICIAL nr. 1.225 din 20 decembrie 2004.

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 153

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

Articolul 154

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

Articolul 155

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

Articolul 156

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

Articolul 157

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

a)loialitatea indiscutabilă a persoanei;

b)caracterul, obiceiurile, relațiile şi discreția persoanei, care să ofere garanții asupra:

– corectitudinii în gestionarea informaţiilor secrete de stat;

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

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

Articolul 158

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

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

Articolul 159

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 160

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

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

b)are antecedente penale sau a fost sancționat contravențional pentru fapte care indică tendințe infracționale;

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

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

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

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

g)a încălcat reglementările privind protecția informaţiilor clasificate;

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 161

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

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

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

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

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

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

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

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

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

Articolul 162

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

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

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

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

d)investigații la locul de muncă şi la domiciliu, care să acopere o perioadă de zece ani anteriori datei avizului sau începând de la vârsta de 18 ani;

e)un interviu cu persoana verificată, dacă se consideră că ar putea clarifica aspecte rezultate din verificările efectuate.

Articolul 163

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

e)în cazul în care, din verificările intreprinse, rezultă incertitudini cu privire la sănătatea psihică 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 evidențiază riscuri de securitate, se va realiza o verificare suplimentară, cu folosirea metodelor şi mijloacelor specifice instituţiilor cu atribuţii în domeniul siguranței naţionale.

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

Articolul 165

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

c)stabilirea naţionalităţii persoanei şi cetăţeniei prezente şi anterioare;

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

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

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

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

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

i)solvabilitatea şi reputaţia financiară a persoanei;

j)stabilirea indiciilor şi obţinerea de probe conform cărora persoana solicitantă este sau a fost membru ori afiliat al vreunei organizaţii, asociaţii, mişcări, grupări străine sau autohtone, care au sprijinit sau au susţinut comiterea unor acte de violenţă, în scopul afectării drepturilor altor persoane, sau care încearcă să schimbe ordinea de stat prin mijloace neconstituţionale.

Articolul 166

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 167

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

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

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

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

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

d)la apariția unor riscuri de securitate din punct de vedere al compatibilității accesului la informaţii clasificate.

Articolul 168

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 169

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

Articolul 170

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

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

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

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

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

Articolul 171

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 172

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

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

Articolul 173

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

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

Articolul 174

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

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

Articolul 175

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

a)la solicitarea ORNISS;

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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 autorizației 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 înapoierea exemplarului 2 al certificatului de securitate sau al autorizației de acces, după care va distruge ambele exemplare, pe bază de proces-verbal.

Secţiunea a 6-a

Accesul cetățenilor străini, al cetățenilor români care au şi cetățenia altui stat, precum şi al persoanelor apatride la informaţiile secrete de stat şi în locurile în care se desfăşoară activităţi, se expun obiecte sau se execută lucrări din această categorie

Articolul 178

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

Articolul 179

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 180

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

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

Articolul 181

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

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

Articolul 182

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

Capitolul 5

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

CONDIŢIILE DE FOTOGRAFIERE, FILMARE, CARTOGRAFIERE ŞI EXECUTARE A UNOR LUCRĂRI DE ARTE PLASTICE ÎN OBIECTIVE SAU LOCURI CARE PREZINTĂ IMPORTANŢĂ DEOSEBITĂ PENTRU PROTECȚIA INFORMAȚIILOR SECRETE DE STAT

Articolul 183

(1) Este interzisă fotografierea, filmarea, cartografierea sau executarea de lucrări de arte plastice pe teritoriul României, în obiective, zone sau locuri de importanţă deosebită pentru protecția informaţiilor secrete de stat, fără autorizație specială eliberată de către ORNISS, care va ține evidența acestora, conform anexei nr. 23.

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

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

Articolul 184

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

Articolul 185

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 186

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

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

Alin. (2) al art. 186 a fost modificat pct. 1 al articolului unic din HOTĂRÂREA nr. 185 din 9 martie 2005, publicată în MONITORUL OFICIAL nr. 247 din 24 martie 2005.

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

Articolul 187

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

Articolul 188

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

Articolul 189

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

(2) Ministerele şi celelalte organe ale administraţiei publice centrale şi locale, care întocmesc documente geodezice, topo-fotogrammetrice şi cartografice cu caracter secret de stat, le vor nominaliza în listele proprii de informaţii clasificate, potrivit dispoziţiilor legale în vigoare.

Articolul 190

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

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

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

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

Art. 190 a fost modificat prin pct. 2 al articolului unic din HOTĂRÂREA nr. 185 din 9 martie 2005, publicată în MONITORUL OFICIAL nr. 247 din 24 martie 2005.

Capitolul 6

EXERCITAREA CONTROLULUI ASUPRA MĂSURILOR PRIVITOARE LA PROTECȚIA INFORMAȚIILOR CLASIFICATE

Articolul 191

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 192

Controlul are ca scop:

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

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

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

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

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

Articolul 193

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

(2)În cazul în care controlul relevă fapte şi disfuncționalități de natură să reprezinte riscuri majore de securitate pentru protecția informaţiilor clasificate va fi informat, de îndată,

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Consiliul Suprem de Apărare a Țării, iar instituția controlată va dispune măsuri imediate de remediere a deficiențelor constatate, va iniția cercetarea administrativă şi, după caz, va aplica măsurile sancționatorii şi va sesiza organele de urmărire penală, în situaţia în care rezultă indicii că s-ar fi produs infracțiuni.

Articolul 194

În funcție de obiectivele urmărite, controalele pot fi:

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

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

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

Articolul 195

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

a)planificate;

b)inopinate;

c)determinate de situaţii de urgență.

Articolul 196

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

Articolul 197

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Capitolul 7

SECURITATEA INDUSTRIALĂ

Secţiunea 1

Dispoziții generale

Articolul 198

Prevederile prezentului capitol se vor aplica tuturor persoanelor juridice de drept public sau privat care desfăşoară ori solicită să desfășoare 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 protecţiei informaţiilor clasificate care fac obiectul activităţilor contractuale

Articolul 199

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

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

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

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

Articolul 200

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

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

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

i)verifică şi prezintă ORNISS propuneri de soluționare a sesizărilor, reclamațiilor şi observațiilor referitoare la modul de aplicare şi respectare a standardelor de protecţie în cadrul contractelor clasificate.

Secţiunea a 3-a

Protecția informaţiilor clasificate care fac obiectul activităţilor contractuale

Articolul 201

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

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

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

Articolul 202

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

Articolul 203

La clasificarea contractelor se vor aplica următoarele reguli generale:

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 204

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

Articolul 205

În cazul în care contractantul cedează unui subcontractant realizarea unei părţi din contractul clasificat, se va asigura că acesta deține autorizație sau certificat de securitate industrială şi este obligat sa înștiințeze contractorul, iar la încheierea subcontractului să prevadă 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 reprezentanți autorizați ai obiectivelor industriale care deţin autorizație de securitate industrială eliberată de către ORNISS, care va ține evidența acestora.

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

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

Articolul 207

(1) Invitațiile la licitații sau prezentări de oferte, în cazul contractelor clasificate, trebuie să conţină o clauză prin care potențialul ofertant este obligat sa înapoieze documentele clasificate care i-au fost puse la dispoziţie, în cazul în care nu depune oferta până la data

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

stabilită sau nu câștigă competiția într-un termen precizat de organizator, care să nu depășească 15 zile de la comunicarea rezultatului.

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

Articolul 208

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

Articolul 209

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

Articolul 210

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

Articolul 211

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

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

i)respectă procedura stabilită pentru protecția informaţiilor clasificate legate de contract.

Articolul 212

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

Articolul 213

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

a)ORNISS a emis certificatul de securitate industrială;

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Secţiunea a 4-a

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

Articolul 214

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

Articolul 215

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

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

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

Articolul 216

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 217

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

a)prevenirea accesului persoanelor neautorizate la informaţii clasificate;

b)garantarea că informaţiile clasificate sunt distribuite pe baza existenței certificatului de securitate industrială şi a principiului necesității de a cunoaște;

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

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

Articolul 218

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

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

b)să fie stabil din punct de vedere economic;

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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 află în procedura reorganizării judiciare sau a falimentului;

c)este implicat într-un litigiu care îi afectează stabilitatea economică;

d)nu își îndeplinește obligaţiile financiare către stat;

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

Articolul 220

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

(2) Sunt considerate riscuri de securitate:

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 221

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

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

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

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

Articolul 222

În termen de 7 zile lucrătoare 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 desemnată de securitate competentă trebuie să garanteze că:

a)agentul economic nu prezintă riscuri de securitate;

b)sunt aplicate în mod corespunzător măsurile de securitate fizică, prevăzute de reglementările în vigoare, precum şi normele privind accesul persoanelor la informaţii clasificate;

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 224

Verificările de securitate se realizează astfel:

a)verificarea de securitate de nivel I - pentru eliberarea avizului necesar autorizației de securitate industrială;

b)verificarea de securitate de nivel II - pentru eliberarea avizului necesar certificatului de securitate industrială de nivel secret;

c)verificarea de securitate de nivel III - pentru eliberarea avizului necesar certificatului de securitate industrială de nivel strict secret;

d)verificarea de securitate de nivel IV - pentru eliberarea avizului necesar certificatului de securitate industrială de nivel strict secret de importanţă deosebită.

Articolul 225

În cadrul verificării de securitate se desfăşoară următoarele activităţi:

(1) Pentru verificările de securitate de nivel I:

a)verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială, conform anexei nr. 25;

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

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

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

(2) Pentru verificările de securitate de nivel II:

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

d)verificarea modului de implementare şi de aplicare a normelor şi măsurilor de securitate fizică, de securitate a personalului şi a documentelor, prevăzute pentru nivelul secret.

(3) Pentru verificarea de securitate de nivel III:

a)verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială - anexa nr. 27;

b)evaluarea statutului de securitate a fiecărei persoane cu putere de decizie - asociaţi/acţionari, administratori, persoanele din comitetul director şi structura de securitate - ori executivă implicată în derularea contractului clasificat, precum şi a celor desemnate să participe la activităţile de negociere a acestuia;

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

d)verificarea existenței autorizării sistemului informatic și de comunicații propriu, pentru nivelul strict secret;

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

(4) Pentru verificarea de securitate de nivel IV:

a)verificarea corectitudinii datelor consemnate în chestionarul de securitate industrială - anexa nr. 27;

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

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

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

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

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

Articolul 226

În cazul unui obiectiv industrial la al cărui management/acționariat participă cetăţeni străini, cetăţeni români care au şi cetățenia altui stat sau/şi persoane apatride, ORNISS, împreună cu ADS competentă, va evalua măsura în care interesul strain ar putea

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

reprezenta o amenințare la adresa protecției informaţiilor secrete de stat, care vor fi încredinţate acelui obiectiv industrial.

Articolul 227

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

Articolul 228

În vederea desfăşurării procedurilor de avizare, obiectivul industrial are obligaţia de a permite accesul reprezentanților 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 îndeplinite cerinţele de securitate necesare asigurării protecției la nivelul de clasificare corespunzător informaţiilor vehiculate în cadrul contractului clasificat, ORNISS eliberează şi transmite obiectivului industrial autorizația sau certificatul de securitate industrială.

(2) Dacă se constată că obiectivul industrial nu îndeplinește condiţiile de securitate necesare, ORNISS nu eliberează autorizația sau certificatul de securitate industrială şi informează obiectivul industrial în acest sens. ORNISS nu este obligat să prezinte motivele refuzului. Refuzul eliberării autorizației sau certificatului de securitate industrială va fi comunicat 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 securității, în luarea deciziei de eliberare a autorizației sau certificatului de securitate industrială vor avea prioritate interesele de securitate.

Articolul 230

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 231

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

Articolul 232

Termenele pentru eliberarea autorizației sau certificatului de securitate industrială sunt:

a)pentru autorizația de securitate industrială - 60 de zile lucrătoare;

b)pentru certificat de securitate industrială de nivel secret - 90 de zile lucrătoare;

c)pentru certificat de securitate industrială de nivel strict secret - 120 de zile lucrătoare;

d)pentru certificat de securitate industrială de nivel strict secret de importanţă deosebită - 180 de zile lucrătoare.

Articolul 233

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

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

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

Articolul 234

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

În situaţia în care ORNISS decide retragerea autorizației sau certificatului de securitate industrială va înștiința contractantul, contractorul şi autoritatea desemnată de securitate competentă.

Articolul 235

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

a)la solicitarea obiectivului industrial;

b)la propunerea motivată a autorităţii desemnate de securitate competente;

c)la expirarea termenului de valabilitate;

d)la încetarea contractului;

e)la schimbarea nivelului de certificare acordat inițial.

Capitolul 8

PROTECȚIA SURSELOR GENERATOARE DE INFORMAȚII - INFOSEC

Secţiunea 1

Dispoziții generale

Articolul 236

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

Articolul 237

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

– INFOSEC - ansamblul măsurilor şi structurilor de protecţie a informaţiilor clasificate care sunt prelucrate, stocate sau transmise prin intermediul sistemelor informatice de comunicații şi al altor sisteme electronice, împotriva amenințărilor şi a oricăror acţiuni

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

care pot aduce atingere confidențialității, integrității, disponibilităţii autenticităţii şi nerepudierii informaţiilor clasificate precum şi afectarea funcţionării sistemelor informatice, indiferent dacă acestea apar accidental sau intenționat. Măsurile INFOSEC acoperă securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografică, precum şi depistarea şi prevenirea amenințărilor la care sunt expuse informaţiile şi sistemele;

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

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

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

– funcții şi caracteristici hardware/firmware/software;

– proceduri de operare şi moduri de operare;

– proceduri de evidență;

– controlul accesului;

– definirea zonei de operare a SPAD;

– definirea zonei de operare a posturilor de lucru/a terminalelor la distanță;

– restricții impuse de politica de management;

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

– structuri fizice şi dispozitive;

– mijloace de control pentru personal şi comunicații;

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

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

– RTD locală - rețea de transmisii de date care interconectează mai multe computere sau echipamente de rețea, situate în același perimetru;

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

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

– managementul de risc - are ca scop identificarea, controlul şi minimizarea riscurilor de securitate şi este o activitate continuă de stabilire şi menținere a unui nivel de securitate în domeniul tehnologiei informației şi comunicațiilor - TIC - într-o unitate, în sensul că, pornind de la analiza de risc, identifică şi evaluează amenințările şi vulnerabilitățile şi propune aplicarea măsurilor adecvate de contracarare, proiectate la un preț de cost corelat cu consecințele care ar decurge din divulgarea, modificarea sau ștergerea informaţiilor care trebuie protejate;

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

– produs informatic de securitate - componenta de securitate care se incorporeaza într-un SPAD sau RTD - SIC şi care servește la sporirea sau asigurarea confidențialității,

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

integrității, disponibilităţii, autenticităţii şi nerepudierii informaţiilor stocate, procesate sau transmise;

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

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

COMSEC reprezintă ansamblul de proceduri, incluzând :

a)măsuri de securitate a transmisiilor;

b)măsuri de securitate împotriva radiațiilor - TEMPEST;

c)măsuri de acoperire criptologică;

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

e)măsuri COMPUSEC;

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

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

Prin procesul de evaluare se verifică:

a)prezența facilităților/funcțiilor de securitate cerute;

b)absența efectelor secundare compromițătoare care ar putea decurge din implementarea facilităților de securitate;

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

c)funcționalitatea globală a sistemului de securitate;

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

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

f)existența performanțelor de securitate ale produselor informatice de securitate instalate în SPAD sau RTD-SIC;

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

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

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

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

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

a)elemente de tehnică de calcul;

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

c)echipamente de comunicații;

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

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

Articolul 238

Abrevierile utilizate în prezentul capitol semnifică:

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

b)TIC - tehnologia informației şi comunicațiilor;

c)CSS - cerinţele de securitate specifice.

Articolul 239

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

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

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

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

Articolul 240

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

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

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

Articolul 241

(1) Aplicarea reglementărilor în vigoare referitoare la protecția informaţiilor clasificate în format electronic funcţionează unitar la nivel naţional. Sistemul de emitere şi

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

implementare a măsurilor de securitate adresate protecției informaţiilor clasificate care sunt stocate, procesate sau transmise de SPAD sau RTD - SIC, precum şi controlul modului de implementare a măsurilor de securitate se realizează de către o structură funcțională cu atribuţii de reglementare, control şi autorizare, care include:

a)o agenție pentru acordarea acreditării de funcționare în regim de securitate;

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

c)o agenție responsabilă cu protecția criptografică.

(2) Agențiile menţionate la alin. (1) sunt subordonate instituției desemnate la nivel naţional, pentru protecția informaţiilor clasificate, ORNISS.

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

Articolul 242

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

Articolul 243

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

Articolul 244

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

(3)CSTIC îndeplinește atribuţii privind:

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

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

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

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

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

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

Articolul 245

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

Articolul 246

CSTIC este condusă de către funcționarul de securitate TIC şi are în compunere administratorii de securitate şi, după caz, şi alti specialiști din SPAD sau RTD - SIC.

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Toata structura CSTIC face parte din personalul unităţii care administrează SPAD sau RTD - SIC.

Articolul 247

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

Articolul 248

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

a)planifică dezvoltarea sau achiziția de SPAD sau RTD;

b)propune schimbări ale unei configurații de sistem existente;

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

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

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

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

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

Articolul 249

CSTIC, cu aprobarea autorității de acreditare de securitate, stabilește standardele şi procedurile de securitate care trebuie respectate de către furnizorii de echipamente, pe parcursul dezvoltării, instalarii şi testării SPAD şi RTD - SIC şi răspunde pentru

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

justificarea, selecţia, implementarea şi controlul componentelor de securitate, care constituie parte a SPAD şi RTD - SIC.

Articolul 250

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

Articolul 251

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

Articolul 252

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

Secţiunea a 2-a

Structuri organizatorice cu atribuţii specifice în domeniul INFOSEC

A.Agenția de acreditare de securitate

Articolul 253

Agenția de acreditare de securitate este subordonată instituției desemnate la nivel naţional pentru protecția informaţiilor clasificate, are reprezentanți delegaţi din cadrul ADS implicate, în funcție de SPAD şi RTD - SIC care trebuie acreditate, şi îndeplinește următoarele atribuţii principale:

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

Articolul 254

Agenția de acreditare de securitate își exercită atribuţiile în domeniul INFOSEC în numele instituției desemnate la nivel naţional pentru protecția informaţiilor clasificate şi are responsabilitatea de a impune standarde de securitate în acest domeniu.

B.Agenția de securitate pentru informatică şi comunicații

Articolul 255

Agenția de securitate pentru informatică şi comunicații este structura subordonată instituției desemnate la nivel naţional pentru protecția informaţiilor electronice clasificate, având reprezentanți delegaţi din cadrul ADS implicate care acţionează la nivel naţional.

Articolul 256

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

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

b)elaborează şi promovează reglementări şi standarde specifice;

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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

Articolul 257

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

C.Agenția de protecţie criptografică

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)asigură managementul materialelor şi echipamentelor criptografice;

b)realizează distribuirea materialelor şi echipamentelor criptografice;

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

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

Secţiunea a 3-a

Măsuri, cerinţe şi moduri de operare

A.Măsuri şi cerinţe specifice INFOSEC

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 259

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

(2) Unitățile deținătoare 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

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

B.Cerinţe de securitate specifice SPAD şi RTD - SIC

Articolul 261

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

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

Articolul 262

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

Articolul 263

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

C.Moduri de operare

Articolul 264

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

a)dedicat;

b)de nivel înalt;

c)multi-nivel.

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 cunoaște pentru aceste persoane se stabilește 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 cunoaște nu impune o separare a informaţiilor în cadrul SPAD sau RTD, ca mijloc de securitate a SIC. Celelalte măsuri de protecție prevăzute vor asigura îndeplinirea cerințelor impuse de cel mai înalt nivel de clasificare a informaţiilor gestionate şi de toate categoriile de informaţii cu destinație specială 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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

informaţiilor stocate, procesate sau transmise în cadrul SPAD sau RTD - SIC, iar accesul la informaţii se va face diferențiat, conform principiului necesităţii de a cunoaște.

(2) Pentru a asigura accesul diferențiat la informaţii, conform principiului necesităţii de a cunoaște, 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 destinație specială stocate, procesate, transmise în cadrul SPAD sau RTD - SIC.

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

Articolul 267

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

(2) Administratorii de securitate sunt:

a)administratorul de securitate al SPAD;

b)administratorul de securitate al rețelei;

c)administratorul de securitate al obiectivului SIC.

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

Articolul 269

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

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

Articolul 270

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

Articolul 271

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

E.Utilizatorii şi vizitatorii

Articolul 272

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

(2) Utilizatorii vor fi autorizați 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 cunoaște.

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

Articolul 273

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

Secţiunea a 4-a

Componentele INFOSEC

A.Securitatea personalului

Articolul 274

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

Articolul 275

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

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 rețelei. Este interzis, cu excepţia unor situaţii speciale, ca personalul să facă atât programarea, cât şi operarea sistemelor sau rețelelor şi trebuie instituite proceduri speciale pentru depistarea acestor situaţii.

Articolul 277

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

Articolul 278

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

B.Securitatea fizică

Articolul 279

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

Articolul 280

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

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

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

c)persoanelor care solicită acces temporar sau cu intermitențe în aceste zone trebuie să li se autorizeze accesul, ca vizitatori, de către responsabilul pe probleme de securitate al zonei, desemnat de către administratorul de securitate al obiectivului SIC. Vizitatorii vor fi însoţiţi permanent, pentru a avea garanția că nu pot avea acces la informaţii clasificate şi nici la echipamentele utilizate.

Articolul 281

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

Articolul 282

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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 funcționarea de ansamblu a sistemului, agenția de acreditare de securitate trebuie să stabilească măsuri specifice de protecţie, adaptate la structura acestui SPAD, conform nivelului de clasificare a informaţiilor gestionate.

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

Articolul 283

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

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 distanță.

Articolul 286

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

Articolul 287

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 288

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

Articolul 289

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

Articolul 290

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

E.Controlul şi evidența informaţiilor în format electronic

Articolul 291

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

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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 său de clasificare şi controlat în interiorul zonei SPAD, până în momentul în care este distrus, redus la o copie de arhivă sau pus într-un dosar permanent.

(2) Evidențele acestora vor fi menținute 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 într-o zonă cu terminal/stație de lucru la distanță, se stabilesc proceduri adecvate de securitate, aprobate de către agenția de acreditare de securitate. Procedurile trebuie să cuprindă şi instrucţiuni specifice privind evidența 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 identifică şi se controlează în mod corespunzător nivelului de secretizare.

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

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

a)Pentru nivelul secret:

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

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

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

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 îndeplinirea următoarelor cerinţe:

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

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

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

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

Articolul 296

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

Articolul 297

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

(2) Sunt interzise declasificarea şi refolosirea mediilor de stocare care conţin informaţii strict secrete de importanţă deosebită, acestea putând fi numai distruse, în conformitate cu procedurile operaționale de securitate.

Articolul 298

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

Secţiunea a 5-a

Reguli generale de securitate TIC

A.Securitatea comunicațiilor

Articolul 299

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

Articolul 300

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

B.Securitatea la instalare şi faţă de emisiile electromagnetice

Articolul 301

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 302

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

Articolul 303

Sistemele SPAD şi RTD - SIC care stochează, procesează sau transmit informaţii secrete de stat vor fi protejate corespunzător față de vulnerabilitățile de securitate cauzate de radiațiile compromițătoare - TEMPEST.

C.Securitatea în timpul procesării informaţiilor clasificate

Articolul 304

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

Articolul 305

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

Articolul 306

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

D.Procedurile operaționale de securitate

Articolul 307

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

Articolul 308

Procedurile operaționale de securitate sunt elaborate de către agenția de concepere şi implementare a metodelor, mijloacelor şi măsurilor de securitate, în colaborare cu CSTIC, precum şi cu agenția de acreditare de securitate, care are atribuţii de coordonare, şi alte autorităţi cu atribuţii în domeniu. Agenția 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.Protecția produselor software şi managementul configurației

Articolul 309

CSTIC are obligaţia să efectueze controale periodice, prin care să stabilească dacă toate produsele software originale - sisteme de operare generale, subsisteme şi pachete soft - aflate în folosinţă, sunt protejate în condiţii conforme cu nivelul de clasificare al informaţiilor pe care acestea trebuie să le proceseze. Protecția programelor - software de aplicație se stabilește 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 interzisă utilizarea de software neautorizat de către agenția de acreditare de securitate.

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 311

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

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

(3) Un software care îmbunătățește posibilitățile sistemului și care nu are nici o procedură de securitate nu poate fi folosit înainte de a fi verificat de către CSTIC.

F.Verificări pentru depistarea virusilor de calculator şi a software-ului nociv

Articolul 312

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

Articolul 313

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

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

G.Întreţinerea tehnică a SPAD sau RTD - SIC

Articolul 314

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

(2) Personalul de întreţinere trebuie să deţină certificate de securitate de nivel corespunzător nivelului de secretizare a informaţiilor la care au acces.

Articolul 315

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

Articolul 316

Cerinţele menţionate la art. 314 trebuie stipulate în CSS, iar procedurile de desfăşurare a activităţii respective trebuie stabilite în procedurile operaționale de securitate. Nu se acceptă tipurile de întreţinere care constau în aplicarea unor proceduri de diagnosticare ce implică accesul de la distanță la sistem, decât dacă activitatea respectivă se desfăşoară sub control strict şi numai cu aprobarea agenției de acreditare de securitate.

H.Achiziții

Articolul 317

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

Articolul 318

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

Articolul 319

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

Articolul 320

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

Articolul 321

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

I. Acreditarea SPAD şi RTD - SIC

Articolul 322

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

(2) Subsistemele SPAD şi RTD - SIC şi stațiile de lucru cu acces la distanță sau terminalele vor fi acreditate ca parte integrantă a sistemelor SPAD şi RTD - SIC la care sunt conectate, în cazul în care un sistem SPAD sau RTD - SIC deserveşte atât NATO, cât şi organizaţiile/structurile interne ale țării, acreditarea se va face de către autoritatea

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

naţională de securitate, cu consultarea ADS şi a agenţiilor INFOSEC, potrivit competenţelor.

J.Evaluarea şi certificarea

Articolul 323

În situaţiile ce privesc modul de operare de securitate multi-nivel, înainte de acreditarea propriu-zisă a SPAD sau RTD - SIC, hardware-ul, firmware-ul şi software-ul vor fi evaluate şi certificate de către agenţia de acreditare de securitate, în acest sens, instituţia desemnată la nivel naţional pentru protecţia informaţiilor clasificate va stabili criterii diferenţiate pentru fiecare nivel de secretizare a informaţiilor vehiculate de SPAD sau RTD - SIC.

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

Următoarele situaţii impun evaluarea şi certificarea de securitate în modul de operare de securitate multi-nivel:

a)pentru SPAD sau RTD - SIC care stochează, procesează sau transmite informaţii clasificate strict secret de importanţă deosebită;

b)pentru SPAD sau RTD - SIC care stochează, procesează sau transmite informaţii clasificate strict secret, în cazurile în care:

– SPAD sau RTD - SIC este interconectat cu un alt SPAD sau RTD - SIC - de exemplu, aparţinând altui CSTIC;

– SPAD sau RTD - SIC are un număr de utilizatori posibili care nu poate fi definit exact.

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 326

Procesele de evaluare şi certificare trebuie să se desfăşoare, conform principiilor şi instrucțiunilor aprobate, de către echipe de expertizare cu pregătire tehnică adecvată şi autorizate corespunzător. Aceste echipe vor fi compuse din experți selecționati de către agenția de acreditare de securitate.

Articolul 327

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

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

K.Verificări de rutină pentru menţinerea acreditării

Articolul 328

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

Articolul 329

(1) Modificările care implică reacreditarea sau pentru care se solicită aprobarea anterioară a agenției de acreditare de securitate trebuie să fie identificate cu claritate 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 funcționarea corectă a dispozitivelor de securitate.

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** **www.pregătiremai.ro**, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 330

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

(2) Pentru SPAD sau RTD - SIC care stochează, procesează sau transmit informaţii strict secrete de importanţă deosebită, inspecţia se va face cel puţin o dată pe an.

L.Securitatea microcalculatoarelor sau a calculatoarelor personale

Articolul 331

(1) Microcalculatoarele sau calculatoarele personale care au discuri fixe sau alte medii nevolatile de stocare a informației, ce operează autonom sau ca parte a unei rețele, precum şi calculatoarele portabile cu discuri fixe sunt considerate medii de stocare a informaţiilor, în același sens ca şi celelalte medii amovibile de stocare a informaţiilor.

(2)În măsura în care acestea stochează 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 vreodată stocate sau procesate pe ele, până la trecerea la un alt nivel de clasificare sau declasificarea lor, în conformitate cu procedurile legale.

M.Utilizarea echipamentelor de calcul proprietate privată

Articolul 333

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

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

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

Articolul 334

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

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

Articolul 335

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

Articolul 336

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

O.Marcarea informaţiilor cu destinație specială

Articolul 337

Marcarea informaţiilor cu destinație specială se aplică, în mod obișnuit, informaţiilor clasificate care necesită o distribuţie limitată şi manipulare specială, suplimentar faţă de caracterul atribuit prin clasificarea de securitate.

Capitolul 9

CONTRAVENȚII ŞI SANCȚIUNI LA NORMELE PRIVIND PROTECȚIA INFORMAȚIILOR CLASIFICATE

Articolul 338

(1) Constituie contravenții la normele privind protecția informaţiilor clasificate următoarele fapte:

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

a)deținerea fără drept, sustragerea, divulgarea, alterarea sau distrugerea neautorizată a informaţiilor secrete de stat;

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

c)neîndeplinirea obligaţiilor prevăzute la art. 31, 41-43, 213, 214;

d)nerespectarea normelor prevăzute în art. 140-142, 145, 159, 160, 162, 163, 179-181, 183 alin. (1) şi 185-190;

e)neîndeplinirea sau îndeplinirea defectuoasa a obligaţiilor prevăzute în art. 240 alin. (2) şi (3), art. 243 şi art. 248, precum şi nerespectarea regulilor prevăzute în art. 274-336.

(2) Contravenţiile prevăzute la alin. (1) se sancţionează astfel:

a)contravenţiile prevăzute la alin. (1) lit. a) se sancţionează cu amendă de la 500.000 lei la 50.000.000 lei în cazul faptelor de deținere fără drept sau de alterare a informaţiilor clasificate şi cu amendă de la 10.000.000 lei la 100.000.000 lei, în cazul faptelor de sustragere, divulgare sau distrugere neautorizată a informaţiilor clasificate;

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

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

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

(3) Persoanele sau autorităţile care constată contravenţiile pot aplica, după caz, şi sancţiunea complementară, constând în confiscarea, în condiţiile legii, a bunurilor destinate, folosite sau rezultate din contravenţii.

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

Articolul 339

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

(1) Contravenţiile şi sancţiunile prevăzute la art. 338 se constată şi se aplică, în limitele competenţelor ce le revin, de către persoane anume desemnate din Serviciul Român de Informaţii, Ministerul Apărării Naţionale, Ministerul de Interne, Ministerul Justiţiei, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Pază şi Serviciul de Telecomunicaţii Speciale.

(2) Pot să constate contravenţiile şi să aplice sancţiunile prevăzute la art. 338, în limitele competenţelor stabilite:

a)persoane anume desemnate din ORNISS;

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

c)autorităţile sau persoanele prevăzute de reglementările generale referitoare la regimul juridic al contravenţiilor.

(3) Plângerile împotriva proceselor-verbale de constatare a contravenţiilor şi de aplicare a sancţiunilor se soluţioneaza potrivit reglementărilor generale privind regimul juridic al contravenţiilor.

Capitolul 10

DISPOZIŢII FINALE

Articolul 340

Nomenclatura funcţiilor, condiţiile de studii şi vechime, precum şi salarizarea personalului cu atribuţii privind evidenţa, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea informaţiilor clasificate se stabilesc potrivit actelor normative în vigoare.

Articolul 341

Conducătorii unităţilor care gestionează informaţii clasificate vor lua măsuri ca dispoziţiile prezentelor standarde să fie aduse la cunoştinţa tuturor salariaţilor şi vor intreprinde măsuri pentru:

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

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

b)nominalizarea personalului cu atribuţii şi funcţii privind gestionarea informaţiilor clasificate;

c)iniţierea demersurilor prevăzute de lege şi de prezentele standarde, pentru obținerea abilitărilor privind accesul la informaţii clasificate.

Articolul 342

La solicitarea persoanelor juridice din sfera de competenţă a Serviciului Român de Informaţii, R.A. Rasirom va evalua conformitatea şi va prezenta ORNISS propuneri de eliberare a certificatelor de acreditare a calităţii pentru sistemele şi echipamentele de protecţie fizică a informaţiilor clasificate.

Articolul 343

(1) Prezentele standarde se interpretează şi se aplică în concordanță cuNormele privind protecția informaţiilor clasificate ale Organizaţiei Tratatului Atlanticului de Nord în România, aprobate prin Hotărârea Guvernului nr. 353 din 15 aprilie 2002.

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

Articolul 344

Dispozițiile prezentelor standarde referitoare la contravențiile şi sancțiunile la normele privind protecția 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.

Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***



Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***



Acest act normativ este actualizat **la data de 26.10.2026** și vă este pus la dispoziție **de către** www.pregătiremai.ro, platformă destinată pregătirii pentru examene de ***admitere la școlile de poliție***, ***încadrări directe din sursă externă***, ***master profesional*** și ***trecere în corpul ofițerilor.***

