

**COMUNA
SCOBINȚI
PRIMĂRIE**

**ADMINISTRAȚIE
PUBLICĂ LOCALĂ**

**PROTECȚIA INFORMAȚIILOR
CLASIFICATE**

Cod: PO – APL – 07

Ediția I

Revizia 0

Exemplar nr.

Pagina 1 din 15

1. Lista responsabililor cu elaborarea, verificarea, avizarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției procedurii documentate.

	Elemente privind responsabilii/ operațiunea	Numele și prenumele	Funcția	Data	Semnătura
	1	2	3	4	5
1.1.	Elaborat	Rusu Cristina	Secretar general U.A.T.		
1.2.	Verificat	Rusu Cristina	Secretar general U.A.T.		
1.3.	Avizat	Rusu Cristina	PC		
1.4.	Aprobat	Hrițcu Gheorghe	Primar		

**COMUNA
SCOBINȚI
PRIMĂRIE**

**ADMINISTRAȚIE
PUBLICĂ LOCALĂ**

**PROTECȚIA INFORMAȚIILOR
CLASIFICATE**

Cod: PO – APL – 07

Ediția I

Revizia 0

Exemplar nr.

Pagina 2 din 15

2. Formular evidență modificări

	Nr. ediției/ reviziei	Data ediției/ reviziei	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediției sau reviziei ediției	Avizul conducătorului compartimentului în cadrul căruia s-a elaborat procedura
	1	2	3	4	5	6
2.1.	Ediția I		X	X		
2.2.	Revizia 0					

COMUNA SCOBINȚI PRIMĂRIE ADMINISTRAȚIE PUBLICĂ LOCALĂ	PROTECȚIA INFORMAȚIILOR CLASIFICATE Cod: PO – APL – 07	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 4 din 15

4. SCOP

4.1. Scopul prezentei proceduri este de a prezenta activitatea privind protecția informațiilor clasificate și a surselor confidențiale ce asigură acest tip de informații.

Protejarea acestor informații se face prin instituirea sistemului național de protecție a informațiilor.

5. DOMENIU DE APLICARE

5.1. Procedura se aplică în cadrul aparatului propriu al primarului.

6. DOCUMENTE DE REFERINȚĂ

6.1. Reglementări internaționale

6.2. Legislație primară

6.2.1. Legea nr. 51/1991 privind securitatea națională a României, republicată (r1), cu completările ulterioare

6.2.2. Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare.

6.2.3. Legea nr. 182/2002 privind protecția informațiilor clasificate, cu modificările și completările ulterioare

6.3. Legislație secundară

6.3.1. Hotărârea nr. 353/2002 pentru aprobarea Normelor privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România

6.3.2. Hotărârea nr. 585/2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România

6.3.3. Ordinul nr. 600/2018 pentru aprobarea Codului controlului intern managerial al entităților publice, emis de Secretariatul General al Guvernului.

6.4. Alte documente, inclusiv reglementări interne ale entității publice

6.4.1. ROF, ROI, Planuri de acțiuni, dispoziții ale primarului.

6.4.2. Dispoziția Primarului pentru numirea Comisiei de monitorizare, coordonare și îndrumare metodologică pentru dezvoltarea sistemului de control intern/managerial.

6.4.3. Regulament de organizare și funcționare a Comisiei de monitorizare, coordonare și îndrumare metodologică pentru dezvoltarea sistemului de control intern/managerial.

7. DEFINIȚII ȘI ABREVIERI

7.1. Definiții ale termenilor:

7.1.1. *Certificate de securitate* - documentele care atestă verificarea și acreditarea persoanei de a deține, de a avea acces și de a lucra cu informații clasificate.

7.1.2. *Clasele de secretizare* - secrete de stat și secrete de serviciu.

7.1.3. *Ediție procedură* – forma actuală a procedurii; ediția unei proceduri se modifică atunci când deja au fost realizate 3 revizii ale respectivei proceduri sau atunci când modificările din structura procedurii depășesc 50% din conținutul reviziei anterioare.

7.1.4. *Informații* - orice documente, date, obiecte sau activități, indiferent de suport, forma, mod de exprimare sau de punere în circulație.

7.1.5. Informații clasificate - informațiile, datele, documentele de interes pentru securitatea națională, care, datorită nivelurilor de importanță și consecințelor care s-ar produce ca urmare a dezvăluirii sau diseminării neautorizate, trebuie să fie protejate.

7.1.6. Informații secrete de serviciu - informațiile a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat.

7.1.7. Informații secrete de stat - informațiile care privesc securitatea națională, prin a căror divulgare se pot prejudicia siguranța națională și apărarea țării.

7.1.8. Nivelurile de secretizare se atribuie informațiilor clasificate din clasa secrete de stat și sunt:

- *strict secret de importanță deosebită* - informațiile a căror divulgare neautorizată este de natură să producă daune de o gravitate excepțională securității naționale;

- *strict secrete* - informațiile a căror divulgare neautorizată este de natură să producă daune grave securității naționale;

- *secrete* - informațiile a căror divulgare neautorizată este de natură să producă daune securității naționale.

7.1.9. Număr ediție - număr de ordine acordat documentului la elaborare și/sau la o modificare de anvergură.

7.1.10. Număr revizie - număr de ordine acordat la modificarea parțială a documentului (a unei secțiuni/ pagini).

7.1.11. Procedură documentată – modul specific de realizare a unei activități sau a unui proces, editat pe suport de hârtie sau în format electronic; procedurile documentate pot fi proceduri de sistem și proceduri operaționale.

7.1.12. Procedură operațională (procedură de lucru) - procedură care descrie un proces sau o activitate care se desfășoară la nivelul unui sau mai multor compartimente dintr-o entitate, fără aplicabilitate la nivelul întregii entități publice.

7.1.13. Protecție juridică - ansamblul normelor constituționale și al celorlalte dispoziții legale în vigoare, care reglementează protejarea informațiilor clasificate;

7.1.14. Protecție prin măsuri procedurale – ansamblul reglementărilor prin care emitentii și deținătorii de informații clasificate stabilesc măsurile interne de lucru și de ordine interioară destinate realizării protecției informațiilor;

7.1.15. Protecție fizică - ansamblul activităților de pază, securitate și apărare, prin măsuri și dispozitive de control fizic și prin mijloace tehnice, a informațiilor clasificate;

7.1.16. Protecția personalului - ansamblul verificărilor și măsurilor destinate persoanelor cu atribuții de serviciu în legătura cu informațiile clasificate, spre a preveni și înlătura riscurile de securitate pentru protecția informațiilor clasificate.

7.1.17. Revizie procedură - acțiunea de modificare respectiv adăugare sau eliminare a unor informații, date, componente ale unei ediții a unei proceduri, modificări ce implică de regulă sub 50% din conținutul procedurii.

7.2. Abrevieri ale termenilor:

- | | | |
|---------------|--------|--|
| 7.2.1. | HG | = Hotărârea Guvernului |
| 7.2.2. | O.U.G. | = Ordonanța de Urgență a Guvernului României |
| 7.2.3. | SCIM | = Sistem de control intern/managerial |
| 7.2.4. | CM | = Comisia de monitorizare |
| 7.2.5. | P.O. | = Procedură operațională. |
| 7.2.6. | PC | = Președintele Comisiei de monitorizare |
| 7.2.7. | ST | = Secretariat Tehnic al Comisiei de monitorizare |

COMUNA SCOBINȚI PRIMĂRIE ADMINISTRAȚIE PUBLICĂ LOCALĂ	PROTECȚIA INFORMAȚIILOR CLASIFICATE Cod: PO – APL – 07	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 6 din 15

- 7.2.8. A.P.L. = Administrație Publică Locală
7.2.9. R.O.F. = Regulament de Organizare și Funcționare
7.2.10. R.O.I. = Regulament de Ordine Interioară

8. DESCRIEREA ACTIVITĂȚII SAU PROCESULUI

8.1. Generalități

8.1.1. Informațiile clasificate se împart în secrete de stat și secrete de serviciu.

Informațiile secrete de stat sunt informațiile care privesc securitatea națională, prin a căror divulgare se pot prejudicia siguranța națională și apărarea țării și care, în funcție de importanța lor, se deosebesc pe niveluri de secretizare astfel:

- strict secret de importanță deosebită – informațiile a căror divulgare neautorizată este de natură să producă daune de o gravitate excepțională securității naționale;
- strict secrete – informațiile a căror divulgare neautorizată este de natură să producă daune grave securității naționale;
- secrete – informațiile a căror divulgare neautorizată este de natură să producă daune securității naționale.

Potrivit legii, în categoria informațiilor secrete de stat sunt cuprinse, pe niveluri de secretizare, informațiile care se referă la:

- a) sistemul de apărare a țării și elementele de bază ale acestuia, operațiile militare, tehnologiile de fabricație, caracteristicile armamentului și tehnicii de luptă utilizate exclusiv în cadrul elementelor sistemului național de apărare;
- b) planurile, precum și dispozitivele militare, efectivele și misiunile forțelor angajate;
- c) cifrul de stat și alte elemente criptologice stabilite de autoritățile publice competente, precum și activitățile în legătură cu realizarea și folosirea acestora;
- d) organizarea sistemelor de protecție și apărare a obiectivelor, sectoarelor și la rețelele de calculatoare speciale și militare, inclusiv la mecanismele de securitate a acestora;
- e) datele, schemele și programele referitoare la sistemele de comunicații și la rețelele de calculatoare speciale și militare, inclusiv la mecanismele de securitate a acestora;
- f) activitatea de informații desfășurată de autoritățile publice stabilite prin lege pentru apărarea țării și siguranța națională;
- g) mijloacele, metodele, tehnica și echipamentul de lucru, precum și sursele de informații specifice, folosite de autoritățile publice care desfășoară activitate de informații;
- h) hărțile, planurile topografice, termogramele și înregistrările aeriene de orice tip, pe care sunt reprezentate elemente de conținut sau obiective clasificate secrete de stat;
- i) studiile, prospecțiunile geologice și determinările gravimetrice cu densitate mai mare de un punct pe kilometru pătrat, prin care se evaluează rezervele naționale de metale și minereuri rare, prețioase, disperse și radioactive, precum și datele și informațiile referitoare la rezervele materiale, care sunt în competența Administrației Naționale a Rezervelor de Stat;
- j) sistemele și planurile de alimentare cu energie electrică, energie termică, apă și alți agenți necesari funcționării obiectivelor clasificate secrete de stat;
- k) activitățile științifice, tehnologice sau economice și investițiile care au legătură cu siguranța națională ori cu apărarea națională sau prezintă importanță deosebită pentru interesele economice și tehnico-științifice ale României;
- l) cercetările științifice în domeniul tehnologiilor nucleare, în afara celor fundamentale, precum și programele pentru protecția și securitatea materialelor și a instalațiilor nucleare;

m) emiterea, imprimarea bancnotelor și baterea monedelor metalice, machetele emisiunilor monetare ale Băncii Naționale a României și elementele de siguranță ale însemnelor monetare pentru depistarea falsurilor, nedestinate publicității, precum și imprimarea și tipărirea hârtiilor de valoare de natura titlurilor de stat, a bonurilor de tezaur și a obligațiunilor de stat;

n) relațiile și activitățile externe ale statului român, care, potrivit legii, nu sunt destinate publicității, precum și informațiile altor state sau organizații internaționale, față de care, prin tratate ori înțelegeri internaționale, statul român și-a asumat obligația de protecție. Legea interzice clasificarea ca secrete de stat a informațiilor, datelor sau documentelor în scopul ascunderii încălcărilor legii, erorilor administrative, limitării accesului la informațiile de interes public, restrângerii ilegale a exercițiului unor drepturi ale vreunei persoane sau lezării altor interese legitime.

Informațiile secrete de serviciu sunt informațiile a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat;

Informațiile secrete de serviciu se referă la acele activități care, fără a constitui, în înțelesul legii, secrete de stat, nu trebuie cunoscute decât pentru îndeplinirea atribuțiilor de serviciu, divulgarea lor putând prejudicia interesul instituției.

Conducătorii persoanelor juridice de drept public sau privat sunt abilitați să stabilească informațiile care constituie secrete de serviciu, precum și regulile de protecție a acestora și, totodată, să coordoneze și să controleze măsurile privitoare la protecția acestora, în conformitate cu normele stabilite prin hotărâre a Guvernului.

Legea interzice clasificarea ca secrete de serviciu a informațiilor care, prin natura sau conținutul lor, sunt destinate să asigure informarea cetățenilor asupra unor probleme de interes public sau personal, respectiv a celor de natură să favorizeze ori să acopere eludarea legii sau obstrucționarea justiției.

8.2. Resurse necesare

8.2.1. Resurse materiale

Logistică: mobilier, rechizite, calculatoare, scanere, servere, software cu licență, rețea, imprimante, posibilități de stocare a informațiilor.

8.2.2. Resurse umane

Personalul din cadrul primăriei cu sarcini de serviciu stabilite în acest sens.

8.2.3. Resurse financiare

Cotă parte din cheltuielile generale ale primăriei în vederea achiziționării materialelor consumabile necesare acestei activități și asigurării serviciilor de întreținere a logisticii.

8.3. Modul de lucru

8.3.1. Accesul la informațiilor clasificate

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

Necesitatea de a cunoaște este principiul conform căruia accesul la informații clasificate se acordă, în mod individual, exclusiv persoanelor care, pentru îndeplinirea îndatoririlor de serviciu, trebuie să aibă acces la acestea.

Certificatul de securitate este documentul eliberat persoanei cu atribuții nemijlocite în domeniul protecției informațiilor clasificate, respectiv funcționarului de securitate sau salariatului din structura de securitate, care atestă verificarea și acreditarea de a deține, de a avea acces și de a lucra cu informații clasificate de un anumit nivel de secretizare.

Autorizația de acces la informații clasificate este documentul eliberat cu avizul instituțiilor abilitate, de conducătorul persoanei juridice deținătoare de astfel de informații, prin care se confirmă că, în exercitarea atribuțiilor profesionale, posesorul acestuia poate avea acces la informații secrete de stat de un anumit nivel de secretizare, potrivit principiului “necesității de a cunoaște”.

Certificatul de securitate, respectiv, 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.

HG 353/2002 privind “Standardele de protecție a informațiilor NATO clasificate în România” și HG 585/2002 privind “Standardele naționale de protecție a informațiilor clasificate în România”, în corelație cu standardele de protecție a informațiilor clasificate operabile în Alianța Nord-Atlantică, precizează că verificările de securitate pentru avizarea eliberării certificatelor de securitate/autorizațiilor de acces la informații secrete au în vedere persoanele care:

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

În vederea eliberării certificatului de securitate sau autorizației de acces la informații clasificate conducătorul unității solicită, în scris, Oficiului Registrului Național al Informațiilor Secrete de Stat (ORNISS), efectuarea verificărilor de securitate asupra persoanei care urmează să aibă acces la informații secrete de stat.

Oficiul Registrului Național al Informațiilor Secrete de Stat organizează evidența listelor și a informațiilor din această categorie și a termenelor de menținere în nivelurile de clasificare, a personalului verificat și avizat pentru lucrul cu informațiile secrete de stat.

În funcție de avizul comunicat de autoritatea desemnată, ORNISS va aproba eliberarea certificatului de securitate/autorizației de acces și va încunoștiința oficial conducătorul unității. După obținerea aprobării, conducătorul unității va notifica la ORNISS și va elibera certificatul de securitate sau autorizația de acces, după caz.

Autoritățile și instituțiile publice întocmesc liste proprii cuprinzând categoriile de informații secrete de stat în domeniile lor de activitate, care se aproba și se actualizează prin hotărâre a Guvernului. De asemenea, acestea sunt obligate să țină un registru de evidență a certificatelor de securitate/autorizațiilor de acces la informații clasificate.

Verificarea în vederea avizării pentru accesul la informații secrete de stat se efectuează potrivit competențelor, de către Autoritățile Desemnate de Securitate (ADS).

Autoritatea Desemnată de Securitate este instituția abilitată prin lege să stabilească, pentru domeniul său de activitate și responsabilitate, structuri și măsuri proprii privind coordonarea și controlul activităților referitoare la protecția informațiilor secrete de stat.

Sunt autorități desemnate de securitate, potrivit HG 585/2002: Ministerul Apărării Naționale, Ministerul de Interne, Ministerul Justiției, Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Protecție și Pază, Serviciul de Telecomunicații Speciale.

Serviciul Român de Informații este abilitat să efectueze verificări pentru:

- personalul propriu;
- personalul autorităților și instituțiilor publice din zona de competență, potrivit legii;
- personalul agenților economici cu capital integral sau parțial de stat și al persoanelor juridice de drept public sau privat.

Ministerul Apărării Naționale efectuează verificări și avizează eliberarea certificatelor de securitate/autorizațiilor de acces pentru:

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

Serviciul de Informații Externe este abilitat prin lege să avizeze pe baza verificărilor de securitate accesul la informații clasificate pentru:

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

Ministerul de Interne, Ministerul Justiției, Serviciul de Protecție și Pază și Serviciul de Telecomunicații Speciale avizează accesul la informații clasificate pentru personalul propriu și persoanele juridice a căror activitate o coordonează.

8.3.2. Modalitățile de protecție a informațiilor clasificate

Protecția informațiilor clasificate se realizează prin protecția juridică care consta în ansamblul normelor constituționale și al celorlalte dispoziții legale în vigoare, care reglementează protejarea informațiilor clasificate.

Conducătorii unităților deținătoare de secrete de stat sunt obligați să asigure condițiile necesare pentru ca toate persoanele care gestionează astfel de informații să cunoască reglementările în vigoare referitoare la protecția informațiilor clasificate. Ei au obligația de a înștiința, în scris, autoritățile desemnate de securitate, potrivit competențelor, prin cel mai operativ sistem de comunicare, despre compromiterea unor astfel de informații.

Înștiințarea se face în scopul obținerii sprijinului necesar pentru recuperarea informațiilor, evaluarea prejudiciilor, diminuarea și înlăturarea consecințelor.

În cazul săvârșirii de infracțiuni la protecția secretului de stat, unitățile deținătoare trebuie să sesizeze organele de urmărire penală și să pună la dispoziția acestora datele și materialele necesare probării faptelor.

Structura/funcționarul de securitate are obligația de a ține evidența cazurilor de încălcare a reglementărilor de securitate, a documentelor de cercetare și a măsurilor de soluționare, conform competențelor.

Protecția prin măsuri procedurale reprezintă ansamblul reglementărilor prin care emitenții și deținătorii de informații clasificate stabilesc măsurile interne de lucru și de ordine interioară destinate realizării protecției informațiilor;

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

Măsurile procedurale de protecție a informațiilor secrete de stat vor fi integrate în programul de prevenire a scurgerii de informații clasificate, care va fi prezentat, spre avizare, autorității abilitate să coordoneze activitatea și să controleze măsurile privitoare la protecția informațiilor clasificate.

Protecția fizică reprezintă ansamblul activităților de pază, securitate și apărare, prin măsuri și dispozitive de control fizic și prin mijloace tehnice, a locurilor în care sunt gestionate informații clasificate.

Măsurile de protecție fizică se concretizează în sisteme automate pentru supraveghere, control, acces, gratii la ferestre, încuietori la uși, pază la intrări, patrulare de securitate, dispozitive de alarmă, mijloace pentru detectarea observării, ascultării sau interceptării, dimensionate în raport cu:

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

Protecția personalului constă în ansamblul verificărilor și măsurilor de educație protectivă a persoanelor care au sau vor avea acces la informațiile clasificate.

Protecția personalului se realizează prin:

- verificarea persoanelor în vederea eliberării certificatului/autorizației de acces la informații clasificate;
- identificarea surselor de fisc și prevenirea incidentelor de securitate care pot conduce la compromiterea informațiilor clasificate;
- includerea persoanelor într-un sistem permanent de pregătire, în vederea însușirii corecte de către acestea a standardelor de securitate și a modului de implementare eficientă a măsurilor de protecție informațiilor clasificate.

Unitățile deținătoare de informații secrete de stat au obligația de a asigura protecția personalului care are acces la informații clasificate sau care este desemnat să asigure securitatea acestora.

Protecția surselor generatoare de informații (INFOSEC) este ansamblul măsurilor și structurilor destinate protecției informațiilor clasificate prelucrate, stocate sau transmise prin intermediul sistemelor informatice de comunicații și al altor sisteme electronice, împotriva oricăror acțiuni care pot aduce atingere confidențialității, integrității, disponibilității și autenticității acestora.

Măsurile INFOSEC acoperă securitatea calculatoarelor, a transmisiilor, a emisiilor, securitatea criptografică, precum și depistarea și prevenirea amenințărilor la care sunt expuse informațiile și sistemele.

8.3.3. Verificarea de securitate a persoanelor care vor avea acces la informațiile clasificate

Verificare de securitate reprezintă totalitatea măsurilor întreprinse de autoritățile desemnate de securitate, conform competențelor legale, pentru stabilirea onestității și profesionalismului persoanelor, în scopul avizării eliberării certificatului de securitate sau autorizației de acces la informații clasificate.

Persoanele care solicită acces la informații clasificate secrete de stat trebuie să își dea acordul pentru a fi verificate cu privire la onestitatea și profesionalismul lor și să completeze formulare tip de verificare. Candidații la funcții publice ce presupun accesarea și competența de a permite cunoașterea unor astfel de informații, vor fi verificați anterior numirii în funcții.

În cadrul procedurilor de avizare se acordă o atenție specială persoanelor care:

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

Decizia privind avizarea eliberării certificatului de securitate/autorizațiilor de acces este condiționată de:

- a) loialitatea indiscutabilă a persoanei;
- b) caracterul, obiceiurile, relațiile și discreția persoanei, care să ofere garanții asupra:
 - corectitudinii în gestionarea informațiilor secrete de stat;
 - oportunității accesului neînsoțit în compartimente, obiective, zone și locuri de securitate în care se află informații secrete de stat;

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

Principalele criterii de evaluare a compatibilității în acordarea avizului pentru eliberarea certificatului de securitate sau autorizației de acces vizează trăsăturile de caracter, situațiile sau împrejurările din care pot rezultă riscuri și vulnerabilități de securitate.

La acordarea avizului de securitate, sunt relevante și vor fi luate în considerare caracterul, conduita profesională sau socială, concepțiile și modul de viață al soțului, soției, al concubinului sau concubinei persoanei solicitante.

Următoarele situații pot fi imputabile atât persoanei care a solicitat acces la informații secrete de stat cât și soțului, soției, respectiv, concubinului sau concubinei:

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 organizații ori puteri străine inamice ordinii de stat și de drept din țara noastră;

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

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

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

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

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

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

d) consuma 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 informațiilor clasificate;

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

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

Persoanele care urmează să desfășoare o activitate sau să fie încadrate într-un loc de muncă ce presupune accesul la informații clasificate vor prezenta conducătorului unității un angajament scris de păstrare a secretului și sunt obligate să asigure protecția acestora, potrivit legii.

Obligațiile se mențin și după încetarea raporturilor de muncă, de serviciu sau profesionale, pe întreaga perioadă a menținerii clasificării informației.

Persoanele juridice de drept privat au obligația să respecte și să aplice reglementările în vigoare stabilite pentru autoritățile și instituțiile publice, în domeniul lor de activitate.

8.3.4. Controlul privind protecția informațiilor clasificate

Controlul are ca scop:

a) evaluarea eficienței măsurilor concrete de protecție adoptate la nivelul diverșilor deținători de informații clasificate, în conformitate cu legea și alte norme în materie, precum și cu programele proprii de prevenire a scurgerii de informații clasificate;

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

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

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

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

Serviciul Român de Informații are competența generală de exercitare a controlului asupra modului de aplicare a măsurilor de protecție de către instituțiile publice și unitățile deținătoare de informații clasificate.

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

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

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

8.3.5. Sancțiuni

Contravențiile și sancțiunile prevăzute se constată și se aplică, în limitele competențelor ce le revin, de către persoane anume desemnate din Serviciul Român de Informații, Ministerul Apărării Naționale, Ministerul de Interne, Ministerul Justiției, Serviciul de Informații Externe, Serviciul de Protecție și Pază și Serviciul de Telecomunicații Speciale. Pot să constate contravențiile și să aplice sancțiunile prevăzute, în limitele competențelor stabilite:

a) persoane anume desemnate din ORNISS;

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

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

8.3.6. Recomandări pentru persoanele care au acces la informații clasificate

Cele mai frecvente situații de compromitere a informațiilor clasificate sunt:

– neglijența manifestată în gestionarea informațiilor clasificate;

– nerespectarea reglementărilor cu privire la acest tip de informații. De multe ori, persoanele care lucrează cu aceste date nu cunosc suficient de bine reglementările privind lucrul cu informații clasificate sau, din delăsare, nu iau în serios necesitatea respectării stricte a acestora;

– transparența exagerată în cadrul unor activități de cooperare care favorizează accesul la date și documente secrete ce excedează clauzelor contractuale;

– lipsa de experiență, corelată cu “atitudinea de bună-credință”.

Persoana nu află sau află prea târziu intențiile ascunse ale culegerii de informații. Deseori se întâmplă ca cineva să divulge secrete fără să constientizeze că a devenit un “furnizor util” de informații importante. Însă buna-credință nu absolvă de răspundere. Justiția nu va putea trece cu vederea că au fost divulgate secrete de stat, fapt ce ar putea aduce grave prejudicii siguranței naționale.

Condiția de bază pentru asigurarea păstrării secretului este respectarea și aplicarea cu strictețe a prevederilor legale.

Este foarte important ca modul și concepția de viață, situația materială, personalitatea și obiceiurile unei persoane care are acces la informații clasificate să fie de așa natură încât aceasta să nu poată fi atrasă în acțiuni ce contravin legii. Încercarea de influențare a unei astfel de persoane se poate face atât în mod direct și deschis, prin prezentarea anumitor avantaje, cât “acoperit”, prin disimularea intențiilor și câștigarea treptată a încrederii persoanei respective.

Există reguli simple, prin aplicarea cărora se poate evita producerea situațiilor de compromitere sau divulgare a informațiilor clasificate:

– Evitați accesul “accidental” al persoanele neautorizate la informații clasificate. Documentele clasificate nu vor fi lăsate nesupravegheate, iar la părăsirea biroului se va aplica “clean- desk policy” – regula biroului curat!

– Nu discutați despre conținutul documentelor secrete în prezența persoanelor neautorizate!

– Clasificați cu atenție documentele pe care le redactați. Solicitați sprijinul persoanei competente în atribuirea nivelurilor de secretizare!

– Verificați documentele primite/transmise pe baza de semnătură, respectiv integritatea acestora (nr. file, ambalaj etc.)!

– Multiplicați și distrugeți documentele clasificate conform regulilor existente. Ciornele sau notele care conțin informații clasificate se supun acelorași reguli!

– Utilizați pentru transmiterea electronică (fax, e-mail) a materialelor doar modalitățile aprobate!

– Respectați regulile de transport a documentelor clasificate. Pe timpul transportării nu lăsați documentele nesupravegheate!

– Asigurați-vă că nu ați amestecat documente secrete cu cele personale, pentru a nu pleca cu acestea la încheierea programului de lucru!

– Dacă participați la o întâlnire, luați cu dumneavoastră numai documentele necesare, pentru care ați primit aprobare!

Utilizarea calculatorului

În multe instituții sistemele de protecție a rețelelor de calculatoare nu sunt suficient de performante. Sunt tot mai frecvente încercările de penetrare a calculatoarelor/rețelelor de calculatoare, mai ales în cazul conectării la Internet.

Dintre cele mai importante reguli de protecție amintim:

– Utilizatorii rețelei de calculatoare trebuie să fie autorizați și să aibă acces numai la partițiile proprii!

– Rețeaua de calculatoare din instituții pe care se procesează informații clasificate trebuie să fie independentă de restul sistemului informatic! Dacă este neapărat necesar să legați rețeaua cu informații clasificate la o rețea externă, atunci folosiți mai multe niveluri de siguranță (codificare, parole, verificări, software antivirus)!

– Accesul la Internet și la e-mail trebuie să se facă de la un calculator independent, pe care nu sunt procesate informații clasificate și care nu este conectat la rețeaua internă!

Ap - aplicat

COMUNA SCOBINȚI PRIMĂRIE ADMINISTRAȚIE PUBLICĂ LOCALĂ	PROTECȚIA INFORMAȚIILOR CLASIFICATE Cod: PO – APL – 07	Ediția I
		Revizia 0
		Exemplar nr.
		Pagina 15 din 15

10. ANEXE, ÎNREGISTRĂRI, ARHIVĂRI

Nr. anexă	Denumirea anexei	Elaborator	Aprobă	Număr de exemplare	Difuzare	Arhivare		Alte elemente
						Loc	Perioada	
1	--							
2	--							
3	--							
4	--							
5	--							
6	--							

11. CUPRINS

Numărul componentei în cadrul procedurii operaționale	Denumirea componentei din cadrul procedurii operaționale	Pagina
	Coperta	
1	Lista responsabililor cu elaborarea, verificarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției procedurii operaționale.	1
2	Situația edițiilor și a reviziilor în cadrul edițiilor procedurii operaționale	2
3	Lista cuprinzând persoanele la care se difuzează ediția sau, după caz, revizia din cadrul ediției procedurii operaționale.	3
4	Scopul procedurii operaționale	4
5	Domeniul de aplicare a procedurii operaționale	4
6	Documentele de referință (reglementări) aplicabile activității procedurate	4
7	Definiții și abrevieri ale termenilor utilizați în procedura operațională	4
8	Descrierea procedurii operaționale	5
9	Responsabilități și răspunderi în derularea activității	14
10	Anexe, înregistrări, arhivări	15
11	Cuprins	15