GHID DE PROTECȚIE A INFORMAȚIILOR CLASIFICATE

sau

un **PIC** despre **SECRETE**

DESPRE SECRETELE DE ODINIOARĂ...

cretul nu este un concept nou, specific perioadei ntemporane. Omul, prin natura sa, a manifestat totdeauna un interes deosebit față de acesta, iar nevoia a-l proteja a apărut ca o consecință firească.

rcetători din toate domeniile au depus eforturi pentru scifrarea secretelor din cele mai vechi timpuri, unele ntinuând să rămână, însă, bine ascunse.

MĂTASEA - istoria mătăsii începe, potrivit lui Confucius, în anul 2640 î. Hr., iar pentru aproximativ 3000 de ani chinezii au păstrat cu strictețe secretul fabricării acesteia. Monopolul asupra producției de mătase și de porțelan - un alt secret bine păzit - le-a permis chinezilor să domine economic restul lumii timp de câteva sute de ani. Secretul mătăsii era atât de bine păstrat încât, în antichitate, romanii, deși mari admiratori ai acesteia, credeau că este fabricată din frunze de copac. În 552 d. Hr., împăratul bizantin Justinian a trimis în China doi călugări care au reușit să fure ouă de viermi de mătase, ascunzându-le în măciulia unui baston. Operațiunea este considerată prima acțiune cunoscută de spionaj industrial.

BETONUL ROMAN - un amestec unic de roci vulcanice, var și apă de mare le-a permis constructorilor din antichitate să ridice construcții care rezistă și astăzi. După analizarea unei mostre de beton ce datează din anul 37 î. Hr., oamenii de știință au descoperit rețeta acestuia.

FOCUL GRECESC - a fost inventat în timpul domniei împăratului bizantin Constantin al IV-lea Pogonatul (665-685 d.Hr.) de către Kallinikos, meșteșugar și arhitect din Heliopolis. Acesta a devenit cea mai redutabilă armă a imperiului bizantin, asigurându-i supremația maritimă pentru câteva sute de ani. Focul grecesc a rămas un secret până azi, cercetătorii neputând decât să-i aproximeze formula chimică, metodele de fabricare și pe cele de utilizare.

REȚETA COCA-COLA - a fost pusă la punct de către John Pemberton, farmacist american rănit în Războiul de Secesiune și devenit, astfel, dependent de morfină. În încercarea de a găsi variante de tratament al durerii care să nu dea dependență, a elaborat, prin încercări succesive, rețeta Coca-Cola, definitivată în 1886 și descrisă la vremea respectivă drept un produs “delicios,

revigorant, înviorător, antrenant” și un “important fortifiant pentru creier”.
Din 1919, rețeta este păstrată în seif și se spune că numai doi angajați cunosc formula și procesul de obținere a băuturii, acestora fiindu-le interzis să călătorească în același avion.
Rețeta rămâne și astăzi unul dintre cele mai bine păstrate secrete comerciale, chiar dacă există voci care afirmă că s-a reușit recrearea acesteia.

... ȘI DE ASTĂZI

Păstrarea secretelor este, în continuare, o necesitate, cu precădere în domenii sensibile și de interes major pentru asigurarea securității statelor și cetățenilor din întreaga lume.
Odată cu trecerea timpului, au fost instituite sisteme de protecție din ce în ce mai complexe a acestora, care să prevină utilizarea lor în alte scopuri decât cele pentru care au fost emise și de către alte persoane decât cele îndreptățite, conform legii, să o facă.
În România, protecția informațiilor clasificate este reglementată printr-un set de acte normative elaborat în acord cu legislația specifică aplicabilă la nivelul Organizației Tratatului Atlanticului de Nord și Uniunii Europene - **Legea nr. 182/2002** privind protecția informațiilor clasificate*, Standardele naționale de protecție a informațiilor clasificate în România, aprobate prin **HG nr. 585/2002***, **HG nr. 781/2002** privind protecția informațiilor secrete de serviciu, Normele privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România, aprobate prin **HG nr. 353/2002*** și **HG nr. 1349/2002** privind colectarea, transportul, distribuirea și protecția corespondenței clasificate pe teritoriul României*.

Legiuitorul a avut în vedere, în principal, stabilirea unor mecanisme care să permită protejarea informațiilor clasificate împotriva:

- acțiunilor de spionaj, compromitere sau acces neautorizat;
- alterării sau modificării conținutului lor;
- sabotajelor ori distrugerilor neautorizate.

Concomitent, a urmărit asigurarea securității sistemelor informatice și de transmitere a acestor informații.

* Cu modificările și completările ulterioare.

CLASIFICAREA INFORMAȚIILOR

Informațiile clasificate sunt datele care necesită o protecție specială datorită importanței lor și consecințelor care s-ar produce ca urmare a diseminării neautorizate a acestora.

Clasificarea informațiilor se realizează prin încadrarea într-o clasă și, după caz, într-un nivel de secretizare.

Clasele de secretizare a informațiilor:

- **SECRET DE STAT** - divulgarea informațiilor prejudiciază securitatea națională și apărarea țării. În funcție de gravitatea prejudiciilor, acestora li se atribuie niveluri de secretizare diferite - strict secret de importanță deosebită, strict secret sau secret;
- **SECRET DE SERVICIU** - divulgarea informațiilor este de natură să determine prejudicii unei persoane juridice de drept public sau privat.

În relația cu NATO și UE, legislația națională prevede următoarea echivalență a claselor și nivelurilor de secretizare:

SECRET DE SERVICIU - NATO RESTRICTED - RESTREINT UE

SECRET - NATO CONFIDENTIAL - CONFIDENTIEL UE

STRICT SECRET - NATO SECRET - SECRET UE

STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ - COSMIC TOP SECRET - TRES SECRET UE

Atribuirea clasei și a nivelului de secretizare a informațiilor se realizează prin consultarea:

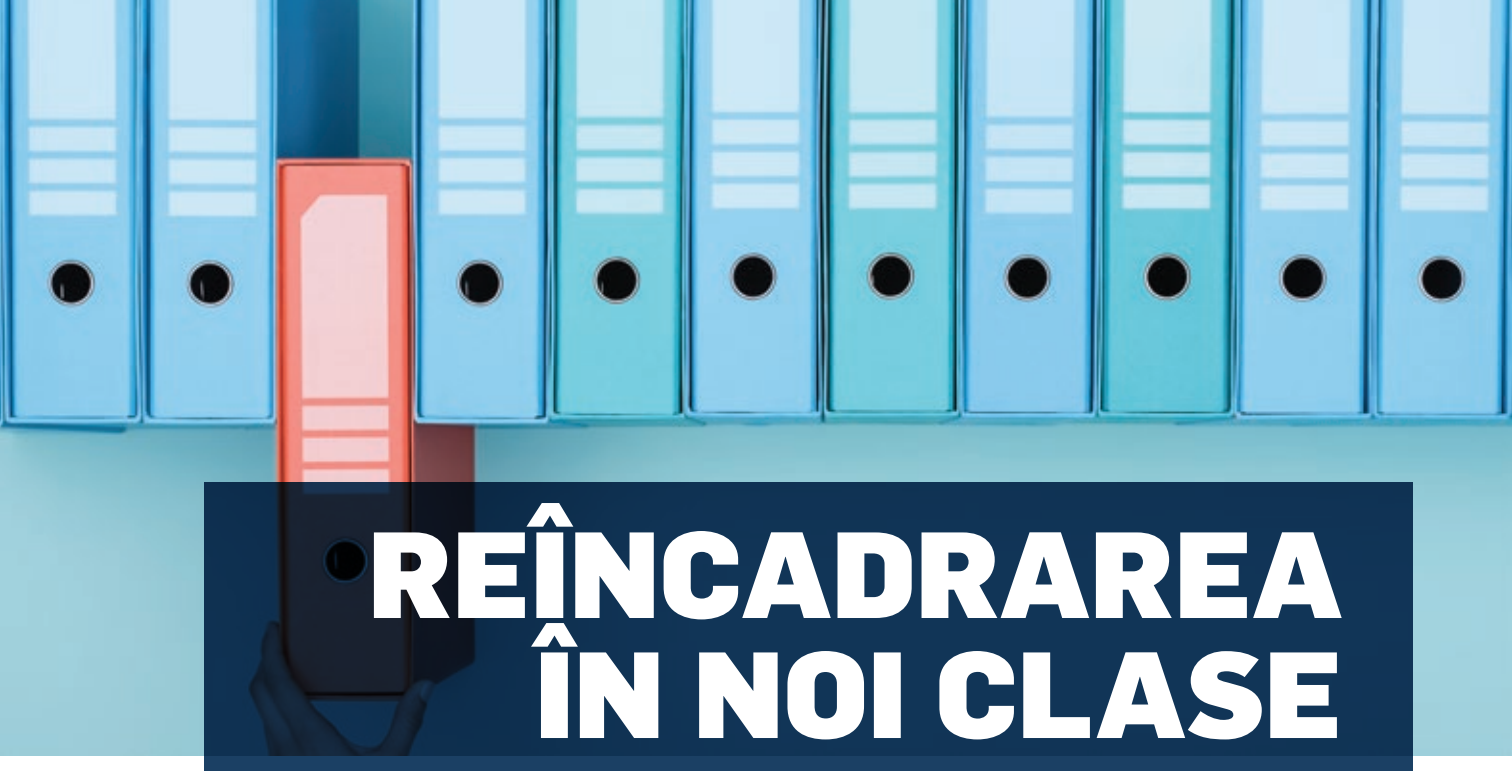
- ghidului de clasificare a informațiilor secrete de stat, elaborat de entitățile deținătoare de astfel de informații și aprobat de împuterniciții sau, după caz, de funcționarii superiori abilitați să atribuie nivelurile de secretizare, conform legii;
- listelor cu categorii de informații secrete de stat, care se aprobă și se actualizează prin hotărâre a Guvernului;
- listelor cu categorii de informații secrete de serviciu, stabilite de către conducătorii entităților deținătoare de astfel de informații.

În cazul informațiilor secrete de stat, termenele de clasificare sunt de până la:

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

Aceste termene pot fi prelungite prin hotărâre a Guvernului, în situații temeinic motivate.
Nivelurile de secretizare și termenele de clasificare se mențin atât timp cât diseminarea neautorizată a informațiilor ar putea prejudicia securitatea națională, apărarea țării, ordinea publică sau interesele persoanelor juridice de drept public sau privat.

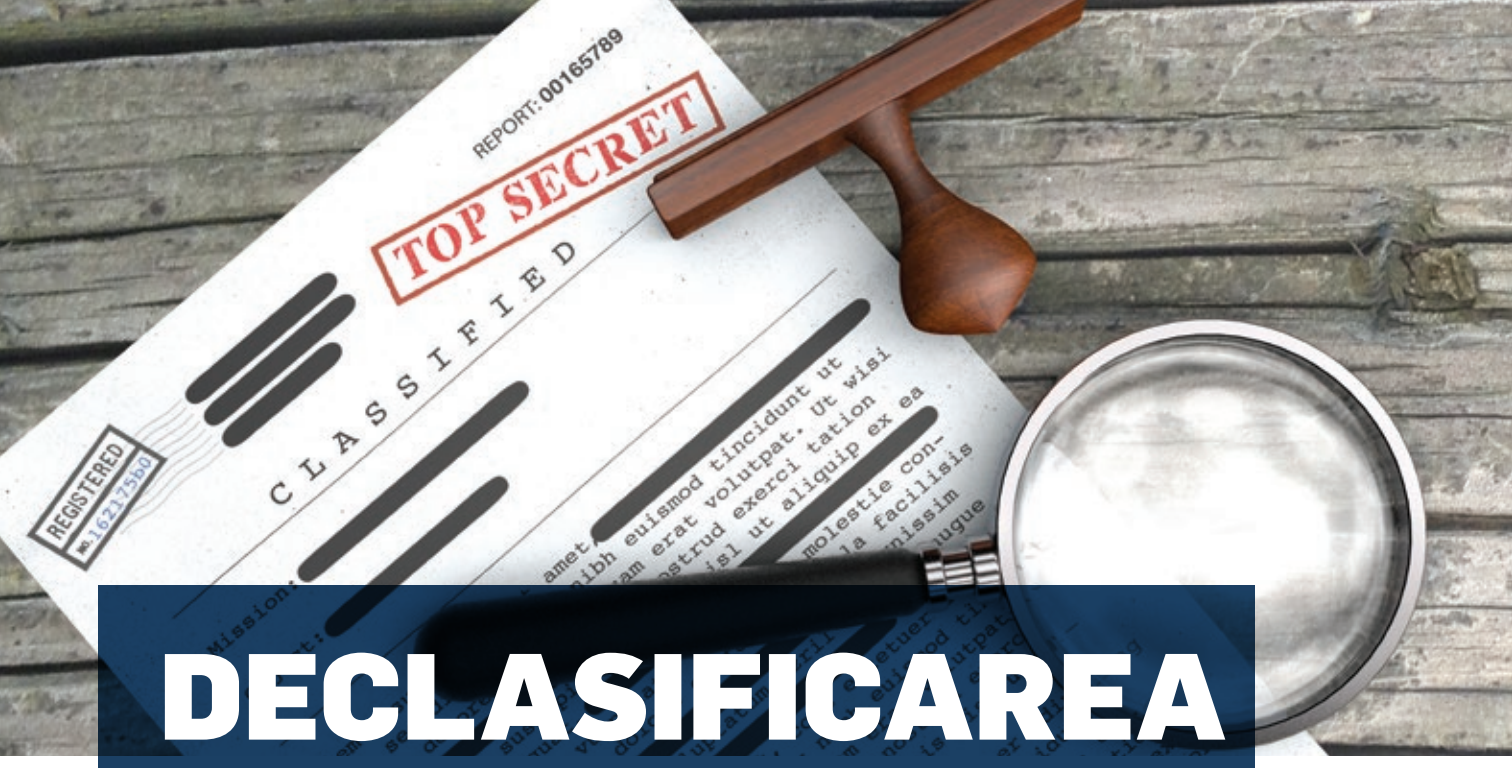
DE REȚINUT! Este interzisă clasificarea informațiilor în scopul ascunderii încălcărilor legii și erorilor administrative, limitării accesului la informațiile de interes public, restrângerii ilegale a exercițiului unor drepturi ale vreunei persoane sau lezării altor interese legitime.



REÎNCADRAREA ÎN NOI CLASE SAU NIVELURI DE SECRETIZARE

Periodic, persoanele împuternicite să atribuie niveluri de secretizare - prevăzute la art. 19 din Legea nr. 182/2002 - au responsabilitatea de a dispune verificarea informațiilor secrete de stat și de a reevalua, dacă este necesar, nivelurile și termenele de clasificare.

Eventualele modificări ale acestora vor fi notificate de către emitent, în scris, tuturor deținătorilor respectivelor informații.



DECLASIFICAREA INFORMAȚIILOR

Categoriile de informații secrete de stat se declasifică printr-o hotărâre emisă de Guvernul României, la solicitarea motivată a emitentului.

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

Informațiile secrete de stat se declasifică în situațiile în care:

- termenul de clasificare stabilit a expirat;
- dezvăluirea nu mai poate prejudicia securitatea națională, apărarea țării, ordinea publică ori interesele deținătorilor;
- clasa și nivelul de secretizare au fost atribuite de o persoană neîmputernicită prin lege.

De asemenea, vor fi declasificate, cu acordul emitentului și informațiile clasificate despre care s-a stabilit cu certitudine, în condițiile legii, că sunt compromise sau iremediabil pierdute.

Informațiile secrete de serviciu se declasifică de către șeful instituției:

- când diseminarea lor nu mai prejudiciază interesele persoanei juridice sau la expirarea termenului de clasificare;
- prin eliminarea acestora de pe listele stabilite și aprobate de către entitățile emitente.

RESPONSABILITĂȚI ÎN PROTECȚIA INFORMAȚIILOR CLASIFICATE

Sistemul de protecție a informațiilor clasificate este complex și presupune exercitarea de atribuții la nivelul mai multor autorități și instituții publice.

Consiliul Suprem de Apărare a Țării - CSAȚ

Oficiul Registrului Național al Informațiilor Secrete de Stat - ORNISS

Autoritățile Desemnate de Securitate - ADS

Conducătorul entității deținătoare de informații clasificate

Structura/funcționarul de securitate

Persoanele autorizate pentru acces la informații clasificate

CSAȚ - asigură coordonarea, la nivel național, a tuturor programelor de protecție a informațiilor clasificate.

ORNISS - asigură implementarea unitară, la nivel național, a măsurilor de securitate a informațiilor naționale clasificate, precum și a celor echivalente care fac obiectul tratatelor, înțelegerilor și acordurilor bilaterale sau multilaterale la care România este parte.

ADS - stabilesc, pentru domeniile lor 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 legii: Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Ministerul Justiției, **Serviciul Român de Informații**, Serviciul de Informații Externe, Serviciul de Protecție și Pază, Serviciul de Telecomunicații Speciale.

> ***Serviciul Român de Informații*** *asigură, prin unitatea sa specializată - Direcția Generală Securitate Internă - coordonarea generală a activității și controlul măsurilor privitoare la protecția informațiilor secrete de stat.*

Principalele atribuții ale SRI în acest domeniu:

- elaborarea, în cooperare cu autoritățile publice, a standardelor naționale pentru protecția informațiilor clasificate și a obiectivelor de implementare a acestora;
- efectuarea de verificări, la solicitarea conducătorului entității, cu privire la persoanele care urmează să ocupe funcții ce presupun accesul la informații și activități cu caracter secret de stat sau care, potrivit legii, nu pot fi divulgate;
- acordarea avizului de specialitate asupra programelor de prevenire a scurgerilor de informații clasificate, întocmite de entitățile din sfera de responsabilitate care dețin asemenea informații;
- efectuarea verificărilor de securitate pentru acordarea avizului de securitate industrială necesar eliberării autorizației sau, după caz, a certificatului de securitate industrială;
- verificarea modului în care sunt respectate și aplicate normele legale privind protecția informațiilor clasificate;
- constatarea nerespectării normelor privind protecția informațiilor clasificate și aplicarea sancțiunilor contravenționale prevăzute de lege;
- sesizarea organelor de urmărire penală atunci când faptele constituie infracțiuni;
- acordarea, la cererea conducătorului entității, a asistenței de specialitate pentru prevenirea scurgerii de date sau informații clasificate;
- conlucrarea cu ORNISS în toate problemele privind aplicarea legislației în materie;
- organizarea colectării, transportului, distribuirii și protecției corespondenței clasificate.

CONDUCĂTORUL ENTITĂȚII DEȚINĂTOARE DE INFORMAȚII CLASIFICATE - persoana căreia îi revine răspunderea privind protecția acestor informații în cadrul entității pe care o conduce.

Câteva dintre principalele sale responsabilități în domeniu:

- asigură organizarea activității structurii/funcționarului de securitate;
- stabilește persoanele care necesită acces la informații clasificate pentru exercitarea atribuțiilor de serviciu și întreprinde demersurile legale pentru obținerea avizului necesar, respectiv pentru eliberarea certificatului de securitate/autorizației de acces;
- asigură condițiile necesare cunoașterii reglementărilor referitoare la protecția informațiilor clasificate de către toți angajații care lucrează cu astfel de informații;
- supune avizării instituțiilor abilitate Programul propriu de prevenire a scurgerii de informații clasificate și asigură aplicarea acestuia;
- analizează modul în care structura/funcționarul de securitate și personalul autorizat asigură protecția informațiilor clasificate;
- asigură măsurile necesare de evidență și control al informațiilor clasificate, astfel încât să se poată stabili, în orice moment, locul în care se află aceste informații;
- sesizează instituțiile competente în legătură cu incidentele de securitate și riscurile la adresa informațiilor secrete de stat;
- dispune efectuarea de cercetări și, după caz, sesizează organele de urmărire penală în situația compromiterii informațiilor clasificate.

STRUCTURA/FUNCȚIONARUL DE SECURITATE - asigură implementarea măsurilor de protecție a informațiilor clasificate în entitățile deținătoare de astfel de informații.

Dintre atribuțiile generale ale acestora amintim:

- coordonarea activității de protecție a informațiilor clasificate, în toate componentele acesteia;
- elaborarea și supunerea spre aprobare conducerii entității a documentelor procedurale specifice;

- organizarea periodică a unor activități de pregătire a persoanelor care au acces la informații clasificate;
- asigurarea relaționării cu instituția abilitată să coordoneze activitatea și să controleze măsurile privitoare la protecția informațiilor clasificate;
- informarea conducerii entității despre vulnerabilitățile și riscurile existente în sistemul de protecție a informațiilor clasificate și propunerea unor măsuri pentru înlăturarea acestora;
- efectuarea, cu aprobarea conducerii entității, de controale privind modul de aplicare a măsurilor legale de protecție a informațiilor clasificate.

DE REȚINUT! Persoana desemnată ca șef al structurii de securitate/funcționar de securitate trebuie să aibă calitatea de adjunct al conducătorului entității sau de membru al consiliului de administrație.

PERSOANELE AUTORIZATE PENTRU ACCES LA INFORMAȚII CLASIFICATE au obligația de a cunoaște și de a respecta toate măsurile de protecție a informațiilor clasificate, respectiv de a utiliza aceste informații exclusiv pentru îndeplinirea atribuțiilor profesionale.

VERIFICĂRILE DE SECURITATE

Verificarea persoanelor în vederea acordării accesului la informații clasificate secrete de stat are ca principal scop identificarea riscurilor de securitate, aferente gestionării acestui tip de informații.

CE SUNT VERIFICĂRILE DE SECURITATE?

Fiecare persoană a cărei funcție implică acces la informații clasificate este verificată, numai pe baza acceptului prealabil, corespunzător nivelului de secretizare a informațiilor care îi sunt necesare pentru exercitarea atribuțiilor de serviciu.

Persoanele care nu își dau acordul pentru derularea procedurii de verificare nu vor face obiectul acesteia și, pe cale de consecință, nu vor fi avizate. După obținerea avizului pozitiv pentru autorizarea accesului la informații secrete de stat, conducătorul entității eliberează certificatul de securitate, respectiv, autorizația de acces la informații secrete de stat.

Accesul la informații clasificate este garantat, sub condiția validării alegerii sau numirii și a depunerii jurământului, pentru: Președintele României, Prim-ministru, miniștri, deputați, senatori, judecători, procurori, respectiv magistrați-asistenți ai Înaltei Curți de Casație și Justiție. Aceștia sunt îndreptățiți să aibă acces la informațiile clasificate în baza unor proceduri interne ale instituțiilor din care fac parte, după ce au luat cunoștință de responsabilitățile ce le revin privind protecția informațiilor clasificate și au semnat angajamentul de confidențialitate.

CE VIZEAZĂ VERIFICĂRILE DE SECURITATE?

Procedurile de verificare sunt stabilite prin Standardele naționale de protecție a informațiilor clasificate. Acestea se efectuează de către autoritățile desemnate de securitate în scopul:

- prevenirii accesului persoanelor neautorizate la informații secrete de stat;
- accesării informațiilor secrete de stat de către deținătorii de certificate de securitate/ autorizații de acces, cu respectarea principiului necesității de a cunoaște;
- identificării persoanelor care, prin acțiunile sau inacțiunile lor, pot pune în pericol securitatea informațiilor secrete de stat.

LIMITĂRI ȘI RESTRICȚII ÎN ACCESAREA INFORMAȚIILOR CLASIFICATE

NECESITATEA DE A CUNOAȘTE

Dacă dreptul de avea acces la informațiile de interes public este garantat prin lege, 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 a informațiilor necesare îndeplinirii atribuțiilor de serviciu.

INCOMPATIBILITĂȚI

Conform legislației în vigoare, există o serie de elemente de incompatibilitate pentru accesul solicitantului la informații secrete de stat. Spre exemplu, solicitantului nu i se poate acorda accesul la informații clasificate dacă:

- a comis sau a susținut, în orice fel, comiterea de acte de spionaj, terorism, trădare;
- are antecedente penale;
- a demonstrat lipsă de loialitate, necinste, incorectitudine sau indiscreție;
- în mod deliberat a ascuns, falsificat sau a interpretat eronat informații cu relevanță în planul securității naționale ori a mințit în completarea formularului de securitate sau la interviul de securitate;
- a încălcat reglementările privind protecția informațiilor clasificate.

GESTIONAREA INFORMAȚIILOR CLASIFICATE

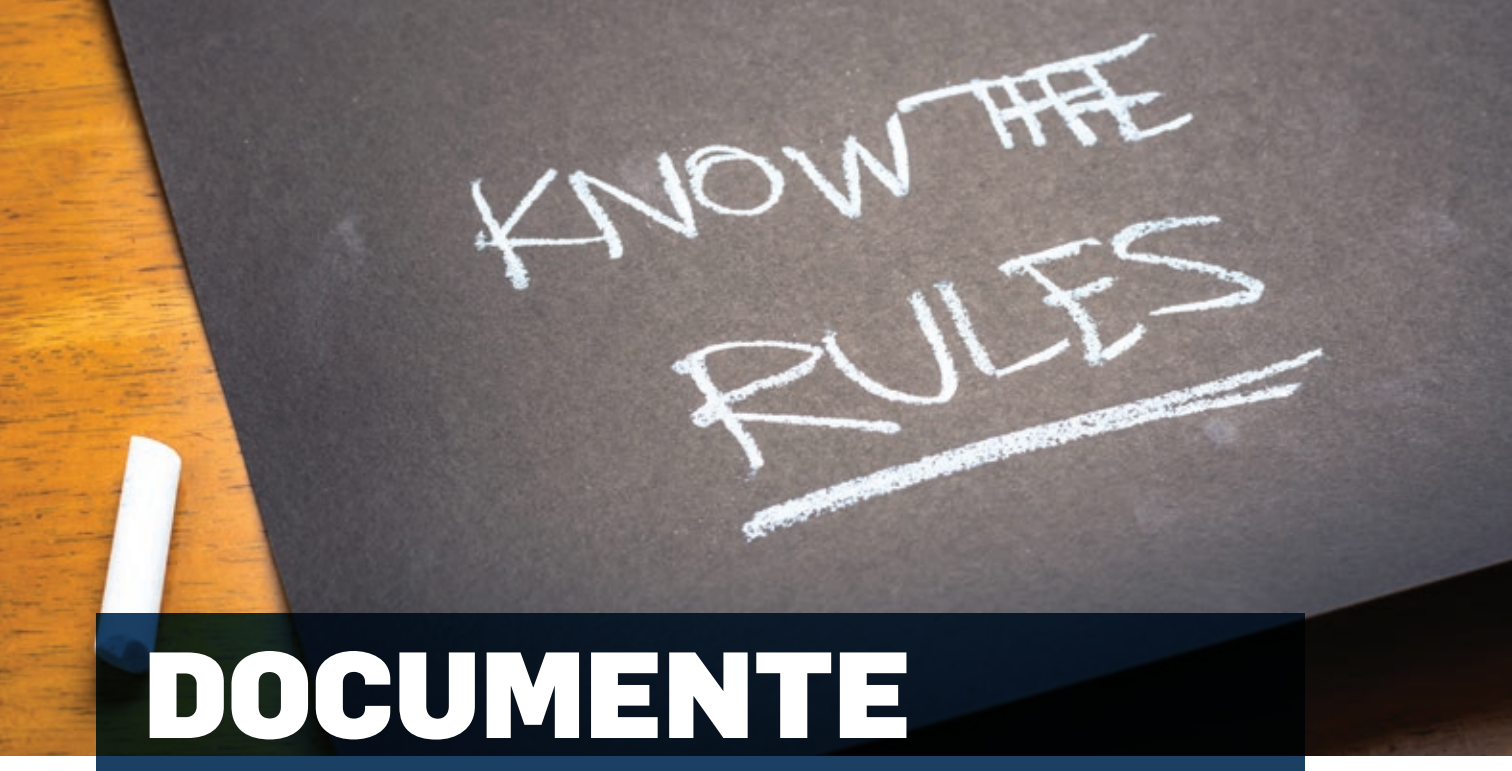
Când o entitate deține informații clasificate, managementul și structura/funcționarul de securitate au obligația de a organiza un sistem protectiv adecvat, pe care trebuie să îl detalieze în Normele interne privind protecția informațiilor clasificate.

În esență, gestionarea corectă a informațiilor clasificate presupune:

MARCAREA - prin menționarea, pe fiecare pagină, a clasei/nivelului de secretizare astfel încât persoanele care intră în contact cu ele să fie conștiente că acestora li se aplică măsuri specifice de acces și protecție;
EVIDENȚA - prin înregistrarea în registre specifice, pentru a se asigura trasabilitatea lor;
TRANSMITEREA - numai cu aprobarea emitentului și respectarea principiului necesității de a cunoaște. Structura/funcționarul de securitate al entității deținătoare trebuie să se asigure că reprezentantul entității destinatare îndeplinește cerințele legale pentru gestionarea de informații clasificate de nivelul celor care fac obiectul transmiterii. Transmiterea informațiilor clasificate în interiorul unei entități se realizează pe bază de semnătură în condica de predare-primire;
MULTIPLICAREA - acestor informații cu aprobarea conducătorului entității, avizul structurii/funcționarului de securitate, de către persoane autorizate. Operațiunile de multiplicare se realizează în zone de securitate și se consemnează în registrul de evidență special constituit;
TRANSPORTUL - prin unitatea specializată a SRI. În privința informațiilor secrete de serviciu, acestea pot fi transportate și prin personal propriu, cu respectarea prevederilor legale;

DE REȚINUT! Corespondența ce conține informații secrete de stat se transportă numai prin echipe de curieri militari. Corespondența ce conține informații secrete de serviciu poate fi transportată și prin personal propriu, autorizat de conducătorul entității beneficiare, cu respectarea prevederilor HG nr. 1349/2002 și a regulilor interne stabilite pentru protecția informațiilor din această clasă.

PĂSTRAREA - exclusiv în zone de securitate sau administrative. În cazul informațiilor secrete de stat, acestea se păstrează în zone de securitate, iar cele secrete de serviciu, în zone administrative;
DISTRUGEREA - numai cu avizul emitentului, pe baza unui proces-verbal semnat de conducătorul instituției, cu avizul șefului structurii/funcționarului de securitate.



DOCUMENTE PROCEDURALE

Asigurarea unui sistem protectiv adecvat este determinată și de existența unui cadru procedural și normativ intern adaptat specificului fiecărei entități, care să stabilească reguli clare în ceea ce privește lucrul cu informații clasificate.

PROGRAMUL DE PREVENIRE A SCURGERII DE INFORMAȚII CLASIFICATE - este documentul care integrează măsurile de protecție implementate la nivelul unui deținător de informații clasificate, fiind clasificat în funcție de clasa/nivelul de secretizare a datelor pe care le conține. Programul este întocmit de structura/funcționarul de securitate și supus avizării instituțiilor abilitate, de către conducătorul entității.

PLANUL DE PAZĂ ȘI APĂRARE A OBIECTIVELOR, SECTOARELOR ȘI LOCURILOR CARE PREZINTĂ IMPORTANȚĂ DEOSEBITĂ PENTRU PROTECȚIA INFORMAȚIILOR CLASIFICATE - deținătorii de informații secrete de stat au obligația întocmirii acestui document, ca anexă la Programul de prevenire. Este de menționat faptul că Planul se înregistrează potrivit celui mai înalt nivel de secretizare a informațiilor protejate și cuprinde totalitatea măsurilor de securitate luate pentru prevenirea accesului neautorizat la acestea.

GHIDUL DE CLASIFICARE A INFORMAȚIILOR SECRETE DE STAT - se întocmește de către autoritățile publice care gestionează informații secrete de stat și se aprobă de către persoanele abilitate să atribuie niveluri de secretizare, conform legii, având ca scop clasificarea corectă și unitară a informațiilor.

NORMELE INTERNE PRIVIND PROTECȚIA INFORMAȚIILOR CLASIFICATE - cuprind reguli clare privind gestionarea informațiilor clasificate la nivelul fiecărei entități care deține astfel de documente. Sunt elaborate de către structura/funcționarul de securitate și aprobate de către conducător.

LISTA INFORMAȚIILOR SECRETE DE STAT - autoritățile publice elaborează liste proprii cuprinzând categoriile de astfel de informații în domeniile lor de activitate, care se aprobă și se actualizează prin hotărâre a Guvernului.

LISTA INFORMAȚIILOR SECRETE DE SERVICIU - se stabilește de către conducătorul persoanei juridice și include categoriile de informații care se referă la activitatea entității și care nu trebuie cunoscute decât de persoanele cărora le sunt necesare pentru îndeplinirea atribuțiilor de serviciu.

LISTA FUNCȚIILOR CARE NECESITĂ ACCES LA INFORMAȚII CLASIFICATE - cuprinde funcțiile care, prin prisma responsabilităților ce le revin, presupun lucrul cu astfel de informații, cu indicarea corespunzătoare a clasei/nivelului de secretizare.

LISTA PERSOANELOR CARE AU SAU VOR AVEA ACCES LA INFORMAȚII CLASIFICATE - se întocmește în raport cu lista funcțiilor care necesită acces la astfel de informații. Este de reținut faptul că pot ocupa funcții care necesită acces la informații clasificate doar persoanele pentru care au fost eliberate certificate de securitate/autorizații de acces, în condițiile legii.

MĂSURI DE PROTECȚIE FIZICĂ

- sunt destinate protejării obiectivelor, sectoarelor și locurilor unde se gestionează informații clasificate, împotriva accesului neautorizat;

- se stabilesc în raport cu nivelul de secretizare, volumul și localizarea informațiilor, tipul containerelor în care sunt depozitate, respectiv caracteristicile clădirii și zonei de amplasare.

Zonele în care se gestionează informații clasificate corespund următoarelor categorii:

- zonă de securitate clasa I - pentru lucrul cu informații de nivel strict secret de importanță deosebită și strict secret;
- zonă de securitate clasa a II-a - pentru lucrul cu informații de nivel secret.

Exemple de măsuri de protecție fizică - gratii la ferestre, încuietori la uși, pază la intrări, sisteme automate pentru supraveghere, control acces, patrule de securitate, dispozitive de alarmă.

DE REȚINUT! Cu informațiile clasificate secret de stat se lucrează exclusiv în încăperile amenajate ca zone de securitate.

PROTECȚIA SURSELOR GENERATOARE DE INFORMAȚII - INFOSEC

Presupune asigurarea securității calculatoarelor, transmisiilor, emisiilor, a securității criptografice, respectiv depistarea și prevenirea amenințărilor la care sunt expuse informațiile clasificate și sistemele prin intermediul cărora acestea sunt vehiculate.

Informațiile clasificate se elaborează și se stochează doar pe sisteme informatice și de comunicații acreditate, conform legii.

Acreditarea reprezintă etapa de acordare a autorizării și aprobării unui sistem informatic și de comunicații de a prelucra informații clasificate, în mediul operațional propriu. În cazul informațiilor clasificate secret de stat, autoritatea de acreditare este ORNISS, iar pentru informațiile secret de serviciu procesul de autorizare este gestionat la nivelul entității gestionare de astfel de informații.

INCIDENTUL DE SECURITATE

Reprezintă orice acțiune sau inacțiune neconformă cu dispozițiile legale în materia protecției informațiilor clasificate, a cărei consecință a determinat sau este de natură a determina compromiterea acestor informații.

Exemple:

- distrugerea sau multiplicarea neautorizată a informațiilor clasificate;
- transportul de documente secrete de stat prin mijloace proprii ale unei entități și nu prin intermediul poștei speciale a SRI;
- gestionarea de informații clasificate în afara zonelor de securitate;
- accesarea de informații secrete de stat/secrete de serviciu de către persoane neautorizate sau fără respectarea principiului necesității de a cunoaște;
- subclasificarea/neclasificarea unor informații;
- diseminarea neautorizată de informații clasificate;
- gestionarea de informații clasificate pe sisteme informatice neacreditate.

În situația identificării unui astfel de incident, conducătorul entității are obligația de a sesiza instituțiile abilitate și de a dispune cercetarea încălcării reglementărilor pentru a stabili:

- dacă informațiile au fost compromise;
- dacă persoanele neautorizate care au avut sau ar fi putut avea acces la informații clasificate prezintă suficientă încredere și loialitate, astfel încât rezultatul compromiterii să nu creeze prejudicii;
- măsurile de remediere - corective, disciplinare sau juridice.

În cazul săvârșirii de infracțiuni, entitățile deținătoare au obligația de a sesiza organele de urmărire penală și de a pune la dispoziția acestora datele și materialele necesare probării faptelor.

ATENȚIE! Nerespectarea normelor legale pe linia protecției informațiilor clasificate generează prejudicii atât securității naționale, cât și intereselor persoanelor juridice.
Conștientizarea cu privire la obligațiile ce revin fiecărei persoane care accesează astfel de date implică, pe lângă loialitatea față de instituția/entitatea în care își desfășoară activitatea profesională, și o responsabilitate în ceea ce privește implementarea și respectarea măsurilor protective.

ÎN LOC DE CONCLUZII... vă reamintim să:

- consultați legislația în vigoare și să solicitați sprijin structurii/funcționarului de securitate atunci când aveți nelămuriri/întrebări cu privire la gestionarea informațiilor clasificate. Managementul entității poate să solicite asistență de specialitate autorității desemnate de securitate în vederea implementării măsurilor protective;
- limitați accesul la informații clasificate doar pentru persoanele care au autorizație de acces de nivel corespunzător și au necesitatea de a le cunoaște;
- respectați regulile atunci când elaborați documente clasificate - marcajele de secretizare sunt primul indicator al faptului că ne aflăm în posesia unor informații importante;
- lucrați cu informații clasificate doar în zonele de securitate sau administrative, după caz;
- redactați informații clasificate doar pe sisteme informatice acreditate;
- participați la activitățile de pregătire în vederea consolidării culturii de securitate;
- înștiințați structura de securitate/managementul entității și instituțiile publice abilitate să coordoneze și controleze activitatea în domeniul protecției informațiilor clasificate, în cazul în care sesizați indicii de insecuritate pentru astfel de informații.

"Dacă îți dezvălui secretele vântului, nu trebuie să dai vina pe acesta pentru că le-a împărtășit copacilor".

KHALIL GIBRAN, poet arab, 1883-1931

AWARENESS