ASPECTE TEORETICE ȘI PRACTICE PRIVIND

CONTROLUL MĂSURILOR PRIVITOARE LA PROTECȚIA INFORMAȚIILOR CLASIFICATE

ÎNTREBĂRI FRECVENTE ȘI RĂSPUNSURI

CE SUNT INFORMAȚIILE CLASIFICATE?

Informațiile care trebuie protejate datorită importanței lor și consecințelor care s-ar produce ca urmare a dezvăluirii neautorizate.

PROTECȚIA ACESTOR INFORMAȚII VIZEAZĂ:

- **protecția juridică și prin măsuri procedurale;**
- **protecția fizică;**
- **protecția personalului;**
- **securitatea documentelor clasificate;**
- **protecția surselor generatoare de informații - INFOSEC.**

CLASELE DE SECRETIZARE A INFORMAȚIILOR:

SECRET DE STAT - divulgarea lor 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 lor este de natură să determine prejudicii unei persoane juridice de drept public sau privat.

CE ESTE INCIDENTUL DE SECURITATE?

Orice acțiune sau inacțiune contrară reglementărilor de securitate a cărei consecință **a determinat sau este de natură să determine compromiterea informațiilor clasificate.**

Conducătorii unităților deținătoare de informații clasificate **și persoanele care gestionează** informații clasificate **au obligația** de a aduce la cunoștința instituțiilor cu atribuții de coordonare și control în domeniu orice indicii din care pot rezulta premise de insecuritate pentru astfel de informații.

ÎNCĂLCĂRILE REGLEMENTĂRILOR DE SECURITATE TREBUIE CERCETATE PENTRU A SE STABILI:

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

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

Informațiile clasificate sunt compromise dacă și-au **pierdut integritatea**, au fost **rătăcite**, **pierdute** ori **accesate**, total sau parțial, **de persoane neautorizate**.

CUM SE STABILESC MĂSURILE DE PROTECȚIE A INFORMAȚIILOR CLASIFICATE?

ÎN RAPORT CU:

- **clasele și nivelurile de secretizare a informațiilor;**
- **volumul și suportul informațiilor;**
- **calitatea, funcția și numărul persoanelor care au sau pot avea acces la informații;**
- **amenințările, riscurile și vulnerabilitățile ce pot avea consecințe asupra informațiilor clasificate.**

CARE SUNT CONDIȚIILE ÎN CARE POT FI ACCESATE INFORMAȚII CLASIFICATE?

- **în baza certificatului de securitate sau autorizației de acces, valabile pentru nivelul de secretizare a informațiilor necesare îndeplinirii atribuțiilor de serviciu;**
- **cu respectarea principiului necesității de a cunoaște.**

CE REPREZINTĂ CONTROLUL MĂSURILOR PRIVITOARE LA PROTECȚIA INFORMAȚIILOR CLASIFICATE?

Activitatea de verificare a modului în care sunt gestionate informațiile clasificate, indiferent de suport - format hârtie / electronic.

ÎN FUNCȚIE DE OBIECTIVELE URMĂRITE, CONTROALELE POT FI:

- **de fond** - presupun verificarea întregului sistem organizatoric, structural și funcțional de protecție a informațiilor clasificate;
- **tematice** - vizează anumite domenii ale activității de protecție a informațiilor clasificate;
- **în situații de urgență** - presupun verificarea unor aspecte punctuale, stabilite ca urmare a identificării unui risc de securitate.

ÎN FUNCȚIE DE MODUL DE ORGANIZARE, CONTROALELE POT FI:

- **planificate;**
- **inopinate;**
- **determinate de situații de urgență.**

CARE ESTE CADRUL NORMATIV ÎN BAZA CĂRUIA SE EFECTUEAZĂ ACTIVITĂȚI DE CONTROL ÎN DOMENIUL PROTECȚIEI INFORMAȚIILOR CLASIFICATE?

- **Legea nr. 182/2002 privind protecția informațiilor clasificate**, cu modificările și completările ulterioare - art. 25 alin. (1);

- **HG nr. 585/2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România**, cu modificările și completările ulterioare - art. 191 alin. (1);

- **HG nr. 781/2002 privind protecția informațiilor secrete de serviciu** - art. 1 lit. e);

- **HG nr. 1349/2002 privind colectarea, transportul, distribuirea și protecția, pe teritoriul României, a corespondenței clasificate**, cu modificările și completările ulterioare - art. 16 lit. b).

CARE ESTE SCOPUL CONTROLULUI?

- **evaluarea eficienței măsurilor concrete de protecție adoptate la nivelul deținătorilor de informații clasificate;**
- **identificarea vulnerabilităților existente în sistemul de protecție a informațiilor clasificate, care ar putea conduce la compromiterea acestor informații;**
- **dispunerea măsurilor de remediere a deficiențelor și de perfecționare a cadrului organizatoric și funcțional la nivelul structurii controlate;**
- **constatarea cazurilor de nerespectare a normelor de protecție a informațiilor clasificate;**
- **aplicarea sancțiunilor contravenționale sau, după caz, sesizarea organelor de urmărire penală, în situația în care faptele constituie infracțiuni;**
- **informarea Consiliului Suprem de Apărare a Țării și Parlamentului cu privire la modul în care unitățile deținătoare de informații clasificate aplică reglementările în materie.**

DE CE REALIZEAZĂ SRI ACTIVITĂȚI DE CONTROL?

Serviciul Român de Informații este Autoritate Desemnată de Securitate și asigură, prin unitatea sa specializată - **Direcția Generală Securitate Internă - coordonarea generală a activității și controlul măsurilor privitoare la protecția informațiilor clasificate gestionate de autoritățile și instituțiile publice, operatorii economici cu capital integral sau parțial de stat și celelalte persoane juridice de drept public sau privat, pentru care instituția noastră este ADS.**

ESTE SRI ABILITAT SĂ EFECTUEZE CONTROALE ȘI LA ENTITĂȚI GESTIONARE EXCLUSIV DE INFORMAȚII SECRETE DE SERVICIU?

Da, în conformitate cu prevederile art. 34 lit. d) și j) din Legea nr. 182/2002, art. 191 alin. (1) din Standardele naționale aprobate prin HG nr. 585/2002 și art. 1 lit. e) din HG nr. 781/2002.

ARE SRI COMPETENȚA DE A VERIFICA MODUL ÎN CARE SUNT GESTIONATE INFORMAȚIILE CLASIFICATE UE/NATO?

Nu. Activitățile de control efectuate de SRI vizează exclusiv verificarea modului de gestionare a informațiilor clasificate naționale. ORNISS exercită aceste atribuții în cazul informațiilor clasificate UE / NATO, conform prevederilor OUG nr. 153/2002, cu modificările și completările ulterioare.

CE CALITATE TREBUIE SĂ ÎNDEPLINEASCĂ OFIȚERII SRI CARE EFECTUEAZĂ ACȚIUNI DE CONTROL?

Să fie abilitați în calitate de agenți constatatori, conform prevederilor OG nr. 2/ 2001 privind regimul juridic al contravențiilor, cu modificările și completările ulterioare.

CINE MAI POATE SĂ VERIFICE STADIUL IMPLEMENTĂRII MĂSURILOR DE PROTECȚIE A INFORMAȚIILOR CLASIFICATE?

Celelalte **Autorități Desemnate de Securitate - Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Ministerul Justiției, Serviciul de Informații Externe, Serviciul de Protecție și Pază, Serviciul de Telecomunicații Speciale.**
Aceste instituții **stabilesc, pentru domeniile lor de activitate și responsabilitate, structuri și măsuri proprii.**

Reprezentantul legal al unității gestionare de informații secrete de stat / secrete de serviciu. Acesta:

- **are obligația** de a analiza, ori de câte ori este necesar, dar cel puțin semestrial, modul în care structura/ funcționarul de securitate și personalul autorizat asigură protecția informațiilor clasificate;
- **poate dispune** structurii/ funcționarului de securitate efectuarea de controale interne privind modul de aplicare a măsurilor legale de protecție a informațiilor clasificate.

CARE SUNT DEMERSURILE REALIZATE DE OFIȚERII SRI LA PREZENTAREA ÎN SEDIUL INSTITUȚIEI CARE URMEAZĂ A FI CONTROLATĂ?

- **relaționarea cu conducătorul persoanei juridice de drept public sau privat / înlocuitorul legal al acestuia;**
- **prezentarea legitimațiilor, delegațiilor speciale și obiectivelor activității de control;**
- **solicitarea Registrului Unic de Control al unității, în vederea consemnării datelor prevăzute de lege.**

CE OBLIGAȚII ARE CONDUCĂTORUL UNITĂȚII GESTIONARE DE INFORMAȚII CLASIFICATE ÎN CAZUL UNUI CONTROL EFECTUAT DE SRI?

- **să pună la dispoziție toate informațiile solicitate privind modul de aplicare a măsurilor prevăzute de lege pentru protecția informațiilor clasificate;**
- **să asigure accesul în toate locațiile în care sunt gestionate informații clasificate.**

CARE SUNT PERSOANELE CARE POT PARTICIPA LA DERULAREA CONTROLULUI?

- **reprezentantul legal al unității controlate / înlocuitorul acestuia;**
- **persoanele cu atribuții și responsabilități în domeniul protecției informațiilor clasificate;**
- **salariați care ocupă funcții ce necesită acces la informații secrete de stat / secrete de serviciu;**
- **alte persoane care pot oferi date/detalii de natură să conducă la conturarea stării de fapt / clarificarea unor aspecte punctuale cu relevanță în planul protecției informațiilor clasificate.**

CARE SUNT PRINCIPALELE CATEGORII DE DOCUMENTE SOLICITATE PE TIMPUL CONTROLULUI?

- **acte administrative de organizare a activității structurii de securitate / compartimentului special / structurilor cu atribuții pe componenta INFOSEC;**
- **documente procedurale elaborate în aplicarea legislației în materie (ex.: liste cuprinzând categoriile de informații clasificate gestionate, funcțiile / persoanele care necesită acces la astfel de date, obiectivele, sectoarele și locurile care prezintă importanță deosebită pentru protecția informațiilor clasificate; programul de prevenire a scurgerii de informații clasificate; planul de pază și apărare; norme interne; ghid de încadrare corectă și uniformă a informațiilor clasificate; alte proceduri de lucru cu informațiile clasificate);**
- **corespondența primită / transmisă, cu incidență în domeniul protecției informațiilor clasificate;**
- **registre specifice de evidență;**
- **documentația de acreditare de securitate a sistemelor informatice prin intermediul cărora sunt prelucrate / stocate informații secrete de stat / secrete de serviciu;**
- **alte înscrisuri oficiale din care rezultă demersurile efectuate de deținătorul de informații clasificate în aplicarea dispozițiilor legale în materie, pe toate componentele protective.**

CE DOCUMENTE SE ÎNTOCMESC CU PRILEJUL CONTROLULUI?

ÎN MOD **OBLIGATORIU**, ECHIPA DE CONTROL ELABOREAZĂ UN ACT DE CONTROL, DENUMIT "**DOCUMENT DE CONSTATARE**", CARE:

- **are caracter nepublic și este destinat exclusiv conducerii entității deținătoare de informații clasificate și persoanelor cu atribuții nemijlocite în domeniul protecției informațiilor clasificate din cadrul acesteia, respectiv celor cu atribuții de coordonare și control, precum și organelor abilitate potrivit legii, după caz;**
- **este un înscris oficial care produce efecte juridice;**
- **cuprinde atât demersurile întreprinse pe linia protecției informațiilor clasificate de către obiectivul controlat, cât și situațiile de neconformitate față de norma de drept, pentru disfuncțiile identificate fiind stabilite termene și măsuri concrete de intrare în legalitate;**
- **se fundamentează pe elemente ce rezultă din înscrisurile prezentate, din discuțiile purtate cu persoanele abilitate, respectiv din constatările nemijlocite ale echipei de control;**
- **este asumat, prin semnătură, de membrii echipei de control, pe de o parte, respectiv de reprezentantul legal al unității controlate/înlocuitorul acestuia, funcționarul de securitate/ șeful structurii de securitate/membri ai structurii de securitate, pe de altă parte.**

În cazul în care se constată contravenții la regimul protecției informațiilor clasificate, se încheie și un **proces-verbal de constatare a contravențiilor și de aplicare a sancțiunilor** care se semnează, pe fiecare pagină, de

către agentul constatator care l-a întocmit și de contravenient/reprezentantul legal al acestuia ori, după caz, de martor.

ÎN CONFORMITATE CU PREVEDERILE OG NR. 2/2001, **SANCȚIUNILE PRINCIPALE** SUNT:

- **avertismentul** – atenționarea scrisă a contravenientului asupra pericolului social al faptei săvârșite, însoțită de recomandarea de a respecta dispozițiile legale; avertismentul se aplică în cazul în care gravitatea faptei este redusă, inclusiv în situațiile în care actul normativ care stabilește contravenția nu prevede această sancțiune;
- **amenda contravențională** – are caracter administrativ și reprezintă o sumă de bani imputată persoanei fizice sau juridice care a săvârșit contravenția.

Cu prilejul controlului poate fi aplicată și **sancțiunea complementară** constând în confiscarea, în condițiile legii, a bunurilor destinate, folosite sau rezultate din contravenții.


FINANCIAL PENALTY

CARE ESTE PROCEDURA LEGALĂ REFERITOARE LA COMUNICAREA DOCUMENTELOR ÎNTOCMITE CU PRILEJUL CONTROLULUI?

- **la încheierea activității de control, după semnarea de către părți, se înmânează conducătorului unității controlate / înlocuitorului legal al acestuia un exemplar al documentului de constatare și, după caz, al procesului-verbal de constatare a contravențiilor și de aplicare a sancțiunilor;**
- **procesul-verbal care nu este semnat de contravenient / reprezentantul legal al acestuia se comunică în termen de cel mult două luni de la data aplicării sancțiunii contravenționale.**

PROCESUL-VERBAL POATE FI CONTESTAT?

Da, în termen de 15 zile de la data primirii/comunicării. Plângerea se depune la judecătoria în a cărei circumscripție a fost săvârșită contravenția și suspendă executarea.

Procesul-verbal neatacat în termenul sus-menționat, precum și hotărârea judecătorească definitivă prin care s-a soluționat plângerea constituie titlu executoriu.

CE SE ÎNTÂMPLĂ CU SUMELE DE BANI PROVENITE DIN APLICAREA AMENZILOR CONTRAVENȚIONALE?

- **în cazul persoanelor juridice - se fac venit integral la bugetul de stat;**
- **în cazul persoanelor fizice - se fac venit integral la bugetele locale ale unității / subdiviziunii administrativ-teritoriale în care contravenientul își are domiciliul.**

CARE SUNT ENTITĂȚILE CARE AU OBLIGAȚIA INSTITUIRII REGISTRULUI UNIC DE CONTROL?

Contribuabilii, persoane juridice înregistrate la Oficiul Național al Registrului Comerțului, autorizate potrivit legii.
Celelalte categorii de contribuabili pot institui registrul unic de control, în funcție de opțiunea acestora.

CE DEMERSURI TREBUIE ÎNTREPRINSE LA NIVELUL UNUI OBIECTIV GESTIONAR DE INFORMAȚII CLASIFICATE ULTERIOR CONTROLULUI PE LINIA PROTECȚIEI INFORMAȚIILOR CLASIFICATE EFECTUAT DE SRI?

În documentul de constatare, **pentru fiecare măsură dispusă este stabilit un termen** corelativ pentru ducerea la îndeplinire a acesteia, respectiv un **“termen general” pentru notificarea SRI** în legătură cu demersurile întreprinse ca urmare a controlului.

În situația în care nu este comunicat un răspuns, **SRI poate să solicite** conducerii obiectivului controlat **detalii cu privire la modul de înlăturare a deficiențelor** constatate **sau să realizeze o nouă activitate de control.**

CARE ESTE PROCEDURA LEGALĂ PENTRU REGLEMENTAREA REGIMULUI JURIDIC AL DOCUMENTELOR CLASIFICATE POTRIVIT HCM NR. 19/1972?

Procedura aplicabilă unor astfel de informații **este reglementată de art. 18 alin. 1 din Standardele naționale, aprobate prin HG nr. 585/2002.**

CONCRET, LA NIVELUL FIECĂREI ENTITĂȚI CARE DEȚINE ASTFEL DE INFORMAȚII SE IMPUNE PARCURGEREA URMĂTOARELOR ETAPE:

- inventarierea documentelor;
- consultarea emitenților acestora cu privire la necesitatea menținerii/reevaluării clasei/nivelului de secretizare.

În cazul în care entitățile care le-au emis nu mai există, solicitarea este adresată succesorilor legali ai acestora sau, după caz, instituțiilor care au în responsabilitate domeniul la care face referire conținutul informațiilor;

- înaintarea propunerilor de încadrare a informațiilor în noi clase/niveluri de secretizare către persoanele / autoritățile publice împuternicite să atribuie nivelurile de secretizare, prevăzute la art. 19 din Legea nr. 182/2002.

De reținut! Informațiile secrete de stat și secrete de serviciu clasificate în baza HCM nr. 19/1972 își păstrează nivelul de secretizare și se protejează conform actualei legislații până la clarificarea regimului lor juridic în condițiile expuse mai sus.

LIPSA MARCAJELOR DE SECRETIZARE ESTE DE NATURĂ SĂ DETERMINE COMPROMITEREA INFORMAȚIILOR CLASIFICATE?

Marcarea informațiilor clasificate are drept scop atenționarea persoanelor care le gestionează sau le accesează că sunt în posesia unor informații în legătură cu care trebuie aplicate măsuri specifice de acces și protecție, în conformitate cu legea.

Atribuirea clasei și nivelului de secretizare a informațiilor se realizează prin consultarea ghidului de clasificare, a listelor cu informații secrete de stat și a listelor cu informații secrete de serviciu, elaborate potrivit legii.

La redactarea informațiilor clasificate trebuie menționate clasa/nivelul de secretizare și numerele de înregistrare specifice.

Absența marcajelor de secretizare reprezintă incident de securitate, fiind de natură să determine compromiterea informațiilor.

SE POT GESTIONA INFORMAȚII CLASIFICATE ÎN LIPSA AVIZULUI DE SPECIALITATE AL SRI ASUPRA PROGRAMULUI DE PREVENIRE A SCURGERII DE INFORMAȚII CLASIFICATE?

Este obligatoriu ca Programul de prevenire a scurgerii de informații clasificate să fie elaborat și transmis, spre avizare, SRI - art. 31 lit. b), coroborat cu art. 86 lit. h) din Standardele naționale aprobate prin HG nr. 585/2002. Întocmirea acestuia se realizează cu respectarea prevederilor anexei nr. 10 la Standardele naționale.
Programul de prevenire a scurgerii de informații clasificate **integrează toate măsurile de protecție** implementate la nivelul unui obiectiv gestionar de astfel de date.

ATENȚIE! În absența acestui document procedural avizat de SRI, nu se poate vorbi de un sistem protectiv viabil.

DE CE ESTE NECESARĂ AUTORIZAREA ACCESULUI LA INFORMAȚII SECRETE DE STAT ÎN CAZUL FACTORILOR DECIZIONALI?

Autorizația de acces la informații secrete de stat/certificatul de securitate este documentul eliberat - cu aprobarea ORNISS, în funcție de avizul Autorității Desemnate de Securitate - de către conducătorul persoanei juridice deținătoare de astfel de informații, prin care se confirmă că, în exercitarea atribuțiilor profesionale, posesorul poate avea acces la informații de un anumit nivel de secretizare, cu respectarea principiului necesității de a cunoaște.
Conducătorii unităților de informații secrete de stat sunt răspunzători de aplicarea măsurilor de protecție a acestora, una din componentele sistemului protectiv reprezentând-o "protecția personalului" care în exercitarea atribuțiilor de serviciu necesită acces la astfel de date.
În lipsa autorizării accesului la informații secrete de stat, conducătorul unei entități care gestionează astfel de informații este în imposibilitatea de a îndeplini obligațiile ce-i revin potrivit legislației în materie.


TOP SECRET

EXISTĂ DIFERENȚE ÎNTRE ATRIBUȚIILE STRUCTURII DE SECURITATE ȘI CELE ALE COMPARTIMENTULUI SPECIAL PENTRU EVIDENȚA, PĂSTRAREA, PROCESAREA, MULTIPLICAREA, MANIPULAREA, TRANSPORTUL, TRANSMITEREA ȘI DISTRUGEREA INFORMAȚIILOR CLASIFICATE?

Da. Responsabilitățile structurii / funcționarului de securitate sunt prevăzute la art. 31 alin. (1) din Standardele naționale aprobate prin HG nr. 585/2002, iar cele ale Compartimentului special derivă din dispozițiile art. 40 și următoarele din același act normativ.

ATENȚIE! Șeful structurii/funcționarul de securitate trebuie să fie adjunct al conducătorului unității sau membru al consiliului de administrație, având și atribuții de coordonare a activității Compartimentului special.

CUM POATE FI PUS ÎN EXECUTARE UN CONTRACT ÎN DERULAREA CĂRUIA SUNT GESTIONATE INFORMAȚII SECRETE DE STAT?

Condițiile în care poate fi pus în executare un astfel de contract sunt prevăzute în Capitolul VII din Standardele naționale, aprobate prin HG nr. 585/2002 și presupun:

- **întocmirea**, de către partea contractantă care pune la dispoziție informații secrete de stat, a **anexei de securitate** la contract, în care vor fi inserate clauzele și procedurile de protecție a datelor în cauză - art. 201-202 din Standarde;
- **obținerea** de către contractant, după adjudecarea contractului, a **certificatului de securitate industrială**, în vederea punerii în executare a acestuia.

Obiectivele industriale care participă **la procedura de negociere** a unor contracte în derularea cărora sunt gestionate informații secrete de stat **trebuie să dețină autorizație de securitate industrială** eliberată de ORNISS - art. 206 din Standarde.

UNDE SE REALIZEAZĂ PREDAREA/PRIMIREA CORESPONDENȚEI CLASIFICATE LA/DE LA ECHIPELE DE CURIERI MILITARI?

Doar în punctele de colectare-distribuire stabilite la nivelul entității, care trebuie să fie organizate ca zone de securitate/administrative, în funcție de clasa/nivelul de secretizare a informațiilor predate/primite.

PUNCTELE DE COLECTARE-DISTRIBUIRE A CORESPONDENȚEI CLASIFICATE:

- sunt menționate în solicitarea de includere în sistemul de transport al corespondenței clasificate, prevăzută de anexa nr. 2 la HG nr. 1349/2002;
- figurează în lista cu obiectivele, sectoarele și locurile care prezintă importanță deosebită pentru protecția informațiilor clasificate.

Predarea/primirea și gestionarea informațiilor clasificate în afara zonelor de securitate/administrative reprezintă incident de securitate.

CUM SE PROCESEAZĂ INFORMAȚIILE SECRETE DE STAT ÎN FORMAT ELECTRONIC?

Pe **sisteme informatice acreditate de ORNISS**, amplasate în zone de securitate.

PROCEDURA DE ACREDITARE PRESUPUNE:

- desemnarea structurii de acreditare – AOSIC și a componentei de securitate pentru tehnologia informației și a comunicațiilor – CSTIC;
- întocmirea documentației cu Cerințele de Securitate Specifice (CSS), Managementul de risc, Procedurile Operaționale de Securitate (PrOpSec);
- existența unor norme interne prin care s-au instituit reguli de utilizare a sistemelor informatice și de comunicații, conectarea SIC la alte rețele informatice (ex.: Internet / Intranet).

MĂSURILE DE PROTECȚIE A INFORMAȚIILOR CLASIFICATE ÎN FORMAT ELECTRONIC:

- sunt similare celor pe suport de hârtie;
- previn materializarea amenințărilor și a oricăror acțiuni care pot aduce atingere confidențialității și integrității lor.

www.sri.ro