Anexă

NORME CADRU PRIVIND SECURITATEA FIZICĂ A INFORMAȚIILOR UE CLASIFICATE

1. DISPOZIȚII GENERALE

Art. 1 – Securitatea fizică reprezintă ansamblul măsurilor de protecție aplicate incintelor în care sunt gestionate informații UE clasificate ce trebuie protejate împotriva accesului neautorizat, deteriorării, distrugerii, pierderii sau compromiterii.

Art. 2 – În sensul prezentelor norme, termenii şi expresiile utilizate se definesc după cum urmează:

a) Container – dulap metalic special destinat păstrării informațiilor clasificate şi protecției împotriva accesului neautorizat la acestea;
b) Forță de securitate – forță specializată alcătuită din personalul permanent de pază şi o forță de intervenție rapidă;
c) Contractant – parte la un contract, care are calitatea de executant de lucrări sau prestator de servicii;
d) Chei de securitate – combinații ale unui sistem cu cifru sau chei de la încăperi speciale de securitate ori de la încuietorile containerelor destinate protecției informațiilor UE clasificate.

2. PRINCIPII DE ORGANIZARE A MĂSURILOR DE SECURITATE FIZICĂ

Art. 3 – Măsurile de securitate fizică urmăresc:

a) să prevină pătrunderea neautorizată a persoanelor, prin efracție sau în alt mod fraudulos, în spațiile protejate;

b) să prevină, să descopere şi să împiedice acțiunile ostile ale personalului neloial, inclusiv cele de spionaj, de natură să afecteze securitatea informațiilor UE clasificate;

c) să permită accesul la informații UE clasificate exclusiv persoanelor autorizate, pe baza unei certificări de securitate corespunzătoare şi a aplicării principiului „nevoia de a cunoaşte'';

d) să descopere şi să combată, în mod operativ, orice încălcare a măsurilor de protecție a informațiilor UE clasificate.

Art. 4 – Amploarea măsurilor de protecție fizică a informațiilor UE clasificate se stabileşte în funcție de:

a) nivelul de clasificare şi categoria informațiilor protejate;

b) volumul informațiilor şi natura suportului de stocare a acestora;

c) modul de păstrare a informațiilor;

d) natura amenințărilor la adresa securității informațiilor clasificate, determinate de activitățile serviciilor de informații care au ca țintă UE sau state membre ale acesteia, precum şi de acţiuni de natură teroristă, subversivă, sabotaj sau de alte activităţi infracţionale.

Art. 5 – (1) Măsurile de protecţie fizică trebuie completate cu măsuri de securitate a personalului, securitate a informaţiilor şi INFOSEC.

(2) Stabilirea celor mai eficiente metode de contracarare a ameninţărilor şi de compensare a vulnerabilităţilor printr-o combinaţie a măsurilor protective din domeniile de la alin. (1) se realizează printr-un management corespunzător al riscurilor de securitate.

Art. 6 – Pentru o incintă dată, măsurile de securitate fizică sunt cuprinse în Planul de securitate fizică.

Art. 7 – Implementarea măsurilor de securitate fizică se va baza pe principiul „apărării în adâncime”, urmărindu-se stabilirea:

a) incintei care trebuie protejată;
b) unui dispozitiv exterior de securitate destinat să delimiteze zona protejată şi să descurajeze accesul neautorizat;
c) unui dispozitiv intermediar de securitate destinat să descopere tentativele sau accesul neautorizat în zona protejată şi să alerteze forţa de securitate;
d) unui dispozitiv interior de securitate destinat să întârzie acţiunile eventualilor intruşi şi să ofere suficient timp pentru ca aceştia să fie reţinuţi de forţa de securitate.

3. MĂSURI DE SECURITATE FIZICĂ

Art. 8 – (1) Informaţiile cu nivelul de clasificare UE CONFIDENTIEL sau superior se gestionează numai în interiorul unei zone de securitate.

(2) Zona de securitate reprezintă perimetrul delimitat, amenajat şi protejat, special destinat gestionării informaţiilor UE clasificate care trebuie să corespundă uneia din următoarele categorii:

a) zona de securitate clasa I, organizată astfel încât intrarea unei persoane într-o asemenea zonă permite accesul direct la orice informaţii UE clasificate gestionate aici, ca urmare a modului specific de păstrare a acestora (expuse la vedere pe rafturi, afişate pe pereţi etc.) şi care presupune:

i. controlul tuturor intrărilor şi ieşirilor;
ii. un sistem de control al intrării care să permită accesul doar acelor persoane care au certificarea de securitate corespunzătoare şi sunt special autorizate să intre într-o asemenea zonă;
iii. specificarea nivelurilor de clasificare ale informaţiilor UE gestionate aici;

b) zona de securitate clasa II, organizată astfel încât o persoană prezentă într-o asemenea zonă are acces exclusiv la informaţiile UE clasificate pentru care este autorizată, ca urmare a modului specific de păstrare a acestora şi care presupune:

i. controlul tuturor intrărilor şi ieşirilor;

ii. un sistem de control al intrării care să permită accesul neînsoţit doar acelor persoane care au certificare de securitate corespunzătoare şi sunt special autorizate să intre într-o asemenea zonă. Pentru toate celelalte persoane trebuie să existe reguli de însoţire pentru a preveni accesul neautorizat la informaţii UE clasificate.

Art. 9 – (1) În jurul zonelor de securitate poate fi stabilită o zonă administrativă. O asemenea zonă implică un perimetru vizibil delimitat, în cadrul căruia sunt create condiţii pentru controlul persoanelor şi al vehiculelor.

(2) Informaţiile UE clasificate gestionate în zona administrativă vor avea cel mult nivelul de clasificare RESTREINT UE.

Art. 10 – Incintele în care nu se lucrează 24 de ore din 24 vor fi inspectate imediat după terminarea programului de lucru, pentru a se verifica dacă protecţia informaţiilor clasificate este asigurată în mod corespunzător.

Art. 11 – (1) Pentru eficientizarea sistemelor de pază şi apărare împotriva pătrunderii neautorizate pot fi utilizate măsuri de securitate fizică specifice (gardul de perimetru, sisteme de detectare a intruziunilor - SDI, iluminat, televiziune cu circuit închis - TVCI).

(2) În cazurile în care acest lucru este posibil, zona ce trebuie protejată va fi delimitată de un gard de perimetru.

(3) Porţile de acces permanent trebuie să ofere cel puţin acelaşi nivel de protecţie ca şi gardul; celelalte porţi vor fi încuiate şi asigurate.

Art. 12 – Iluminatul de securitate va fi realizat astfel încât să ofere un grad mai mare de detectare a unui potenţial intrus atât direct de către pază, cât şi indirect prin intermediul sistemului TVCI.

Art. 13 – Sistemele de detectare a intruziunilor vor fi utilizate pentru a spori nivelul de securitate oferit de gard sau vor fi folosite în camere şi clădiri pentru a ajuta sau a substitui personalul de pază.

Art. 14 – Televiziunea cu circuit închis va fi utilizată pentru verificarea incintelor şi alarmelor SDI.

Art. 15 – Atunci când se folosesc SDI, TVCI sau alte dispozitive destinate supravegherii şi protecţiei informaţiilor UE clasificate, trebuie să existe o sursă de alimentare de rezervă.

Art. 16 – (1) Controlul accesului personalului permanent în zonele de securitate se efectuează de personal de pază sau prin sisteme electronice, avându-se în vedere următoarele:

a) accesul fiecărui angajat se realizează prin locuri anume stabilite, pe baza permisului de acces;
b) permisul de acces nu va specifica în clar identitatea organizației emitente sau locul în care deținătorul are acces;
c) permisele de acces care acordă accesul fără escortă în interiorul zonelor de securitate în care sunt manipulate sau depozitate informații UE clasificate se emit numai persoanelor care au certificare de securitate corespunzătoare; cererea pentru acces în zonă trebuie să fie bine întemeiată și bazată pe principiul „nevoia de a cunoaște".

(2) La nivelul fiecărei persoane juridice care gestionează informații UE clasificate se pot stabili reguli suplimentare proprii privind accesul, cu respectarea prezentelor cerințe minime.

Art. 17 – Accesul vizitatorilor în zonele de securitate se realizează conform regulilor proprii aprobate de conducătorul instituției, ținând cont de certificarea de securitate și cu aplicarea principiului „nevoia de a cunoaște", înregistrându-se datele personale ale vizitatorilor, precum și ora intrării și ieșirii acestora prin punctele de control.

Art. 18 – (1) Pentru accesul angajaților agenților economici contractanți care efectuează lucrări de construcții, reparații și întreținere a clădirilor, instalațiilor sau utilităților în zonele de securitate, conducătorii instituțiilor beneficiare vor elibera, pe baza actelor de identitate, la solicitarea reprezentanților autorizați ai agenților în cauză, documente de acces temporar.

(2) Documentul de acces temporar este valabil doar pe durata executării lucrărilor și se restituie emitentului la terminarea acestora.

Art. 19 – Accesul în zonele de securitate al personalului însărcinat cu păstrarea curățeniei se face conform regulilor proprii stabilite de conducătorul instituției beneficiare.

Art. 20 – Accesul personalului care asigură întreținerea sistemelor de informatică și comunicații (SIC) se va realiza în conformitate cu prevederile Ordinului directorului general al ORNISS nr. 488/2003 privind aprobarea Ghidului pentru elaborarea documentației cu cerințele de securitate (DCS) pentru sisteme informatice și de comunicații (SIC) - DS 1, publicat în Monitorul Oficial al României, Partea I, nr. 866 din 5 decembrie 2003.

Art. 21 – Forța de securitate va fi asigurată de structuri specializate ale autorităților publice sau de societăți autorizate de pază și protecție.

Art. 22 – Forța de intervenție rapidă are rolul de a interveni în situații de urgență și poate fi constituită din personal propriu sau poate fi asigurată pe bază de contract.

Art. 23 – Timpul de reacție al forței de intervenție rapidă se testează periodic și se menționează în Planul de securitate fizică.

Art. 24 – (1) Sarcinile personalului permanent de pază, precum şi necesitatea şi frecvența patrulărilor vor fi stabilite în funcție de nivelul riscului şi de celelalte sisteme sau echipamente de securitate instalate.

(2) În incintele în care nu se lucrează 24 de ore din 24, intervalul de timp dintre patrulările efectuate în afara orelor de program nu va depăşi două ore.

(3) Personalul de pază va primi instrucțiuni scrise cu privire la modul de îndeplinire a atribuțiilor specifice în cadrul instituției respective şi va fi înarmat, respectându-se legislația în vigoare.

(4) Personalul de pază care asigură paza incintelor în care sunt gestionate informațiile UE clasificate, trebuie să dețină certificare de securitate corespunzătoare informațiilor gestionate în zona în care poate avea acces pentru îndeplinirea atribuțiilor ce-i revin.

Art. 25 – Birourile sau zonele în care, în mod uzual, se poartă discuții în cadrul cărora sunt vehiculate informații UE clasificate de nivel CONFIDENTIEL UE sau superior vor fi protejate împotriva ascultării neautorizate.

Art. 26 – Echipamentele de telecomunicații şi echipamentele electrice sau electronice de birou, de orice tip, folosite în timpul şedințelor în care se vehiculează informații clasificate de nivel CONFIDENTIEL UE sau superior vor fi verificate de către unități specializate la cererea structurii/funcționarului de securitate.

Art. 27 – Copiatoarele şi faxurile vor funcționa în încăperile speciale de securitate, la ele având acces doar persoanele autorizate.

Art. 28 – (1) Informațiile UE clasificate se păstrează în încăperi speciale de securitate şi/sau containere speciale ori mobilier de birou.

(2) Dispozițiile Ordinului directorului general al ORNISS nr. 475/2005 privind aprobarea Cerințelor minime de securitate fizică pentru încăperile speciale de securitate destinate protecției informațiilor NATO clasificate şi a celor echivalente, potrivit legii, publicat în Monitorul Oficial al României, Partea I, nr. 1035 din 22 noiembrie 2005, se aplică în mod corespunzător şi în privința încăperilor speciale de securitate destinate protecției informațiilor UE clasificate.

(3) Containerele speciale se clasifică astfel:

a) clasa A, containere autorizate la nivel național pentru depozitarea informațiilor TRÈS SECRET UE/UE TOP SECRET în zone de securitate de Clasa I sau Clasa II;
b) clasa B, containere autorizate la nivel național pentru depozitarea informațiilor SECRET UE şi CONFIDENTIEL UE în zone de securitate de Clasa I sau Clasa II;
c) clasa C, mobilier de birou adecvat numai pentru depozitarea informațiilor RESTREINT UE.

Art. 29 – Încuietorile folosite la containerele în care sunt păstrate informații UE clasificate se împart în 3 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.

Art. 30 – Prevederile Ordinului directorului general al ORNISS nr. 443/2003 privind aprobarea Cerințelor minime pentru containerele destinate protecției informațiilor clasificate, pentru mecanismele de închidere, sistemele cu cifru şi încuietorile acestora, publicat în Monitorul Oficial al României, Partea I, nr. 781 din 6 noiembrie 2003, completat prin Ordinul directorului general al ORNISS nr. 182/2004, publicat în Monitorul Oficial al României, Partea I, nr. 383 din 30 aprilie 2004, se aplică în mod corespunzător şi în privința containerelor destinate protecției informațiilor UE clasificate, mecanismelor de închidere, sistemelor cu cifru şi încuietorilor acestora.

Art. 31 – (1) Combinațiile cifrului şi cheile de la containerele şi încăperile speciale de securitate trebuie protejate adecvat pentru a se evita intrarea acestora în posesia unor persoane neautorizate.

(2) Cheile de la containerele şi încăperile de securitate se păstrează într-o zonă de securitate.

(3) Cheile de rezervă se păstrează de către şeful structurii/funcționarul de securitate, care trebuie să țină evidența utilizării acestora. Ele se introduc în unul sau mai multe plicuri mate, care se sigilează şi se păstrează într-un container de securitate prevăzut cu încuietoare cu cifru.

Art. 32 – (1) În cadrul zonelor de securitate pot fi stabilite zone sigure din punct de vedere tehnic.

(2) Aceste zone vor fi ținute încuiate atunci când nu sunt ocupate, iar toate cheile vor fi considerate chei de securitate.

(3) Zonele sigure din punct de vedere tehnic vor fi inspectate periodic sau în urma unei intrări neautorizate ori atunci când există suspiciuni privind o intrare neautorizată.

Art. 33 – Pentru echipamentele şi mobilierul din dotarea acestor zone se va păstra un inventar detaliat care să asigure urmărirea circulației acestora. Orice piesă de mobilier sau echipament va fi introdusă într-o asemenea zonă numai după ce a fost atent inspectată de către personalul de securitate specializat în detectarea dispozitivelor de ascultare. Ca regulă generală, se va evita instalarea liniilor de comunicații în zonele securizate din punct de vedere tehnic.

Art. 34 – Este interzisă folosirea, în zonele sigure din punct de vedere tehnic, a telefonului mobil şi/sau a altor echipamente care pot fi utilizate pentru înregistrarea şi redarea informațiilor UE clasificate.

Art. 35 – (1) Toate încăperile în care se gestionează sau în care este posibil accesul la informații UE clasificate vehiculate prin SIC trebuie să se afle într-o zonă de securitate.

(2) Toate SIC sau alte medii de gestionare similare (servere, sisteme de rețea etc.) în care se gestionează informații UE clasificate se instalează în încăperi speciale de securitate, în conformitate cu nivelul de clasificare al informațiilor şi cu nevoile specifice de protecție a acestora.

(3) Măsurile de protecție a informațiilor UE clasificate gestionate în SIC se stabilesc prin proceduri INFOSEC.

Art. 36 – (1) La nivelul persoanelor juridice care gestionează informații UE clasificate se întocmeşte Planul de securitate fizică ce va cuprinde descrierea tuturor măsurilor de securitate fizică implementate pentru protecția acestor informații, structurat astfel:

a) delimitarea, marcarea şi configurația zonelor de securitate;
b) sistemul de pază şi apărare;
c) sistemul de avertizare şi alarmare;
d) controlul accesului, al cheilor şi combinațiilor de cifru;
e) modul de acțiune în situații de urgență;
f) modul de raportare, investigare şi evidență a încălcării măsurilor de securitate;
g) responsabilitățile şi modul de implementare a măsurilor de pregătire şi instruire pe linie de securitate fizică;
h) responsabilitățile şi modalitățile de realizare a verificărilor, inspecțiilor şi controalelor sistemului de securitate;
i) măsuri suplimentare de protecție fizică.

(2) În cazul în care la nivelul persoanei juridice există un plan de securitate al obiectivului pentru protecția informațiilor clasificate, elaborat şi implementat conform legislației în vigoare, acesta va fi completat în mod corespunzător cu măsurile de securitate fizică specifice pentru protecția informațiilor UE clasificate.