DECIZIA (UE) 2022/640 A COMISIEI

din 7 aprilie 2022

privind normele de punere în aplicare referitoare la rolurile și responsabilitățile principalilor actori din domeniul securității

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 249,

având în vedere Decizia (UE, Euratom) 2015/443 a Comisiei din 13 martie 2015 privind securitatea în cadrul Comisiei ([1]),

având în vedere Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate ([2]),

întrucât:

(1) Deciziile (UE, Euratom) 2015/443 și (UE, Euratom) 2015/444 se aplică tuturor departamentelor și sediilor Comisiei.

(2) Atunci când este necesar, trebuie adoptate norme de punere în aplicare pentru completarea sau sprijinirea Deciziei (UE, Euratom) 2015/444, în conformitate cu articolul 60 din aceasta.

(3) Măsurile de securitate pentru protecția informațiilor UE clasificate pe durata ciclului lor de viață ar trebui să fie proporționale, în special, cu clasificarea lor în materie de securitate.

(4) Măsurile de securitate pentru protecția sistemelor informatice și de comunicații în cadrul Comisiei sunt prevăzute în Decizia (UE, Euratom) 2017/46 a Comisiei ([3]), în special la articolul 3 privind principiile de securitate informatică în cadrul Comisiei și la articolul 9 privind proprietarii de sisteme.

(5) Obiectivul normelor de punere în aplicare referitoare la rolurile și responsabilitățile principalilor actori din domeniul securității este de a oferi orientări cu privire la condițiile prealabile și sarcinile care sunt prevăzute pentru rolurile respective în Deciziile (UE, Euratom) 2015/443 și (UE, Euratom) 2015/444.

(6) Articolul 36 alineatul (7) din Decizia (UE, Euratom) 2015/444 stabilește o serie de funcții suplimentare legate de securitate care trebuie exercitate de Autoritatea de securitate a Comisiei. Sarcinile aferente acestor funcții sunt prevăzute în prezenta decizie.

(7) Ofițerii locali de securitate și ofițerii de control al registraturii au responsabilități specifice în ceea ce privește protecția informațiilor clasificate ale UE în cadrul departamentelor lor, în conformitate cu Decizia (UE, Euratom) 2015/444.

(8) La data de 4 mai 2016, Comisia a adoptat o decizie ([4]) de autorizare a membrului Comisiei însărcinat cu probleme de securitate să adopte, în numele Comisiei și sub responsabilitatea acesteia, normele de punere în aplicare prevăzute la articolul 60 din Decizia (UE, Euratom) 2015/444. Ulterior, la 13 aprilie 2021, membrul Comisiei responsabil cu problemele de securitate a adoptat, în numele Comisiei și sub responsabilitatea acesteia, o decizie ([5]) de subdelegare a acestor norme de punere în aplicare directorului general al Direcției Generale Resurse Umane și Securitate,

([1]) JO L 72, 17.3.2015, p. 41.
([2]) JO L 72, 17.3.2015, p. 53.
([3]) Decizia (UE, Euratom) 2017/46 a Comisiei din 10 ianuarie 2017 privind securitatea sistemelor informatice și de comunicații în cadrul Comisiei Europene (JO L 6, 11.1.2017, p. 40).
([4]) Decizia C(2016) 2797 final din 4 mai 2016 privind o abilitare legată de securitate.
([5]) Decizia C(2021) 2684 final din 13 aprilie 2021 de acordare a unei subdelegări de competențe acordate prin Decizia C(2016) 2797 a Comisiei privind o abilitare legată de securitate.

ADOPTĂ PREZENTA DECIZIE:

CAPITOLUL 1

Dispoziții generale

Articolul 1

Obiect și domeniu de aplicare

(1) Prezenta decizie stabilește rolurile și responsabilitățile principalilor actori din domeniul securității care sunt responsabili de protecția informațiilor UE clasificate (IUEC) în cadrul Comisiei în temeiul Deciziilor (UE, Euratom) 2015/443 și (UE, Euratom) 2015/444.

(2) Prezenta decizie se aplică tuturor departamentelor Comisiei și în toate sediile acesteia.

CAPITOLUL 2

Direcția Generală Resurse Umane și Securitate

Articolul 2

Autoritatea de securitate a Comisiei

(1) Directorul Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate este Autoritatea de securitate a Comisiei (*Commission Security Authority* – CSA), menționată la articolul 7 din Decizia (UE, Euratom) 2015/444.

(2) CSA își îndeplinește funcțiile în următoarele domenii, astfel cum se prevede în Decizia (UE, Euratom) 2015/444, în conformitate cu articolele 3-7 din prezenta decizie:

(a) securitatea personalului;

(b) securitatea fizică;

(c) gestionarea IUEC;

(d) acreditarea oricărui sistem informatic și de comunicații (SIC) care gestionează IUEC;

(e) securitatea industrială; și

(f) schimbul de informații clasificate.

(3) CSA furnizează activități de formare obligatorii pentru ofițerii locali de securitate (LSO), adjuncții LSO, ofițerii de control al registrelor (RCO) și adjuncții RCO cu privire la responsabilitățile și atribuțiile lor.

Articolul 3

Autoritatea de asigurare a informațiilor

Autoritatea de asigurare a informațiilor este responsabilă de următoarele activități legate de protecția IUEC:

(a) elaborarea de politici de securitate și de orientări de securitate pentru asigurarea informațiilor și monitorizarea eficacității și pertinenței acestora;

(b) protejarea și gestionarea informațiilor tehnice privind produsele criptografice;

(c) asigurarea conformității măsurilor de asigurare a informațiilor cu politicile de securitate și de achiziții ale Comisiei, după caz;

(d) asigurarea faptului că produsele criptografice sunt selectate în conformitate cu politicile care reglementează eligibilitatea și selecția acestora;

(e) consultarea proprietarilor de sisteme, a furnizorilor de sisteme, a actorilor din domeniul securității și a reprezentanților utilizatorilor în ceea ce privește politicile de securitate și orientările de securitate pentru asigurarea informațiilor.

Articolul 4

Autoritatea de acreditare în materie de securitate

(1) CSA este responsabilă de acreditarea zonelor securizate care îndeplinesc cerințele articolului 18 din Decizia 2015/444 și a SIC pentru gestionarea IUEC.

(2) Departamentele Comisiei consultă autoritatea de acreditare în materie de securitate (AAS), în coordonare cu LSO și LISO ai lor, după caz, ori de câte ori un departament intenționează:

(a) să construiască o zonă securizată;

(b) să implementeze un SIC pentru a gestiona IUEC;

(c) să instaleze orice alt echipament pentru gestionarea informațiilor clasificate, inclusiv conexiuni la un SIC al unei părți terțe.

AAS oferă consiliere cu privire la aceste activități atât în timpul proceselor de planificare, cât și al celor de construcție sau dezvoltare.

(3) IUEC nu pot fi gestionate într-o zonă securizată sau de către un SIC înainte ca autoritatea de acreditare în materie de securitate să emită pentru zona securizată, respectiv pentru SIC, o acreditare la nivelul IUEC corespunzător.

(4) Printre cerințele pentru acreditarea unei zone securizate se numără:

(a) aprobarea planurilor pentru zona securizată;

(b) aprobarea oricăror contracte de lucrări executate de contractanți externi, luând în considerare dispozițiile privind securitatea industrială, cum ar fi orice cerințe de deținere de autorizații de securitate de către contractanți și personalul acestora;

(c) disponibilitatea tuturor declarațiilor și certificatelor de conformitate necesare;

(d) o inspecție fizică a zonei securizate pentru a verifica dacă materialele și metodele de construcție, controalele accesului, echipamentele de securitate și orice alte articole respectă cerințele prevăzute de CSA;

(e) validarea măsurilor de combatere a radiațiilor electromagnetice pentru orice zonă securizată din punct de vedere tehnic;

(f) aprobarea procedurilor operaționale de securitate (SecOP) pentru zona securizată.

(5) Printre cerințele pentru acreditarea unui SIC care gestionează IUEC se numără:

(a) crearea unei strategii de acreditare a sistemelor;

(b) validarea planului de securitate al SIC, pe baza unei abordări de gestionare a riscurilor;

(c) validarea SecOP pentru SIC;

(d) validarea tuturor celorlalte documente de securitate necesare, astfel cum au fost stabilite de autoritatea de acreditare în materie de securitate;

(e) aprobarea oricărei utilizări a tehnologiilor de criptare;

(f) validarea măsurilor de combatere a radiațiilor electromagnetice pentru un SIC care gestionează informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior;

(g) o inspecție a SIC pentru a verifica dacă măsurile de securitate documentate sunt implementate în mod corect.

(6) După constatarea îndeplinirii cu succes a cerințelor de acreditare, autoritatea de acreditare în materie de securitate eliberează o autorizație oficială pentru gestionarea IUEC în zona securizată sau de către SIC, pentru un nivel maxim precizat al IUEC și pentru o perioadă de până la 5 ani, în funcție de nivelurile IUEC gestionate și de riscurile implicate.

(7) După notificarea unei încălcări a securității sau a unei modificări semnificative în ceea ce privește proiectarea sau măsurile de securitate ale unei zone securizate sau ale unui SIC, autoritatea de acreditare în materie de securitate revizuiește și, dacă este necesar, poate revoca autorizația de gestionare a IUEC până la soluționarea oricăror probleme identificate.

Articolul 5

Autoritatea TEMPEST

(1) Se implementează măsuri de securitate TEMPEST pentru a proteja SIC care gestionează informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior și se pot implementa măsuri de securitate și pentru informațiile clasificate RESTREINT UE/EU RESTRICTED.

(2) Autoritatea TEMPEST este responsabilă de aprobarea măsurilor luate pentru protecția împotriva compromiterii IUEC prin emanații electronice neintenționate.

(3) La cererea unui proprietar de sistem al unui SIC care gestionează IUEC, autoritatea TEMPEST emite specificații pentru măsurile de securitate TEMPEST care sunt adecvate nivelului de clasificare al informațiilor.

(4) Autoritatea TEMPEST efectuează teste tehnice în timpul acreditării zonelor securizate și a SIC pentru gestionarea IUEC la nivelul CONFIDENTIAL UE/EU CONFIDENTIAL sau la un nivel superior și, dacă testele au reușit, eliberează un certificat TEMPEST.

(5) Certificatele TEMPEST trebuie să specifice cel puțin:

(a) data efectuării testului;

(b) o descriere a măsurilor de securitate TEMPEST, împreună cu planurile incintelor respective;

(c) data expirării certificatului;

(d) ce modificări vor invalida certificarea;

(e) semnătura autorității TEMPEST.

(6) Un LSO sau o persoană care organizează reuniuni responsabilă de organizarea unei reuniuni clasificate, în coordonare cu LSO, poate solicita autorității TEMPEST să testeze sălile de reuniuni pentru a se asigura că acestea sunt securizate din punct de vedere tehnic.

Articolul 6

Autoritatea de aprobare criptografică

(1) Autoritatea de aprobare criptografică este responsabilă de aprobarea utilizării tehnologiilor de criptare.

(2) Autoritatea de aprobare criptografică emite orientări privind cerințele pentru utilizarea și aprobarea tehnologiilor de criptare.

(3) Autoritatea de aprobare criptografică aprobă utilizarea soluțiilor de criptare pe baza unei cereri din partea proprietarului de sistem. Aprobarea se bazează pe o evaluare satisfăcătoare a cel puțin următoarelor aspecte:

(a) nevoile în materie de securitate aferente informațiilor care trebuie protejate;

(b) o imagine de ansamblu a SIC implicat în soluție;

(c) o evaluare a riscurilor inerente și reziduale;

(d) o descriere a soluției propuse;

(e) SecOP pentru soluția de criptare.

(4) Autoritatea de aprobare criptografică ține un registru al soluțiilor de criptare aprobate.

Articolul 7

Autoritatea de distribuție criptografică

(1) Autoritatea de distribuție criptografică este responsabilă de distribuirea materialelor criptografice utilizate la protecția IUEC (în principal echipamente de criptare, chei și certificate criptografice și autentificatorii aferenți) către:

(a) utilizatorii sau departamentele din cadrul Comisiei pentru SIC care sunt administrate de părți externe;

(b) utilizatorii sau organizațiile din afara Comisiei pentru SIC care sunt administrate de Comisie.

(2) Autoritatea de distribuție criptografică poate delega altor departamente distribuirea de materiale criptografice pentru părți terțe, în conformitate cu articolul 17 alineatul (3) din Decizia 2015/443.

(3) Autoritatea de distribuție criptografică se asigură că toate materialele criptografice sunt trimise prin canale securizate care oferă protecție împotriva oricărei manipulări frauduloase și care prezintă dovezi ale oricărei manipulări frauduloase, în conformitate cu normele de securitate aplicabile pentru nivelul de clasificare a IUEC care vor fi protejate de materialele respective.

(4) Autoritatea de distribuție criptografică oferă orientări LSO și, după caz, responsabilului local cu securitatea informatică din cadrul fiecărui departament al Comisiei care este implicat în producerea, distribuția sau utilizarea materialelor criptografice.

(5) Autoritatea de distribuție criptografică se asigură că sunt instituite SecOP adecvate pentru procesul de distribuție.

CAPITOLUL 3

Departamentele Comisiei

Articolul 8

Șefii de departament

(1) Fiecare șef de departament numește:

(a) un LSO și unul sau mai mulți adjuncți ai acestuia, după caz, pentru departament sau cabinet;

(b) un RCO și unul sau mai mulți adjuncți ai acestuia, după caz, pentru fiecare departament care gestionează o registratură IUEC;

(c) un proprietar de sistem pentru fiecare SIC care gestionează IUEC.

(2) Șeful de departament solicită aprobarea directorului Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate înainte de numirea LSO, a LSO adjuncți, a RCO și a RCO adjuncți.

(3) Șeful de departament identifică toate posturile care necesită autorizare pentru a avea acces la IUEC, în consultare cu LSO. Candidații la astfel de posturi sunt informați în cursul procesului de recrutare cu privire la cerința de a obține o autorizare.

(4) Șeful oricărui departament care deține IUEC este responsabil de activarea planurilor de distrugere și de evacuare de urgență, atunci când este necesar. Planurile trebuie să includă o soluție alternativă pentru situațiile în care șeful de departament nu poate fi contactat.

Articolul 9

Proprietarii de sistem ai SIC care gestionează IUEC

(1) Proprietarul de sistem contactează autoritatea de acreditare în materie de securitate cât mai curând posibil în cadrul unui proiect de implementare a unui SIC care gestionează IUEC pentru a stabili standardele și cerințele de securitate relevante și pentru a începe procesul de acreditare de securitate.

(2) Proprietarul de sistem se asigură că măsurile de securitate îndeplinesc cerințele autorității de acreditare în materie de securitate și că SIC nu gestionează IUEC înainte să fie acreditat.

(3) Proprietarul de sistem contactează autoritatea de aprobare criptografică pentru aprobarea utilizării oricăror tehnologii de criptare. Proprietarii de sistem nu operează tehnologii de criptare în sistemele de producție fără o aprobare prealabilă.

(4) Proprietarul de sistem consultă LISO al departamentului în ceea ce privește aspectele legate de securitatea SIC.

(5) Proprietarul de sistem revizuiește cel puțin o dată pe an măsurile de securitate aplicate unui sistem, inclusiv planul de securitate al acestuia.

(6) În cazul în care are loc un incident de securitate într-un SIC din care reiese faptul că SIC nu mai poate proteja în mod adecvat IUEC, proprietarul de sistem informează LSO și contactează imediat autoritatea de acreditare în materie de securitate pentru a-i oferi consiliere cu privire la modul în care trebuie să procedeze. În acest caz, acreditarea poate fi suspendată, iar sistemul poate fi scos din funcțiune până când se iau măsurile corective corespunzătoare.

(7) Proprietarul sistemului acordă în orice moment sprijin deplin autorității de acreditare în materie de securitate în îndeplinirea sarcinilor acesteia legate de acreditarea SIC.

Articolul 10

Autoritatea operațională de asigurare a informațiilor

Autoritatea operațională de asigurare a informațiilor pentru fiecare SIC:

(a) stabilește documentația în materie de securitate în conformitate cu politicile și orientările privind securitatea, în special cu planul de securitate, SecOP legate de sistem și documentația criptografică din cadrul procesului de acreditare a SIC;

(b) participă la selectarea și testarea măsurilor tehnice de securitate, a dispozitivelor și software-ului specifice sistemului, pentru a supraveghea implementarea lor și pentru a se asigura că instalarea, configurarea și întreținerea lor este securizată în conformitate cu documentația de securitate relevantă;

(c) participă la selectarea măsurilor și dispozitivelor de securitate TEMPEST, dacă acest lucru este impus de planul de securitate, și, în cooperare cu autoritatea TEMPEST, se asigură că acestea sunt instalate și întreținute în mod securizat;

(d) monitorizează implementarea și aplicarea SecOP legate de funcționarea sistemului;

(e) gestionează și manipulează produsele criptografice, în colaborare cu autoritatea de distribuție criptografică, pentru a asigura custodia corespunzătoare a materialelor criptografice și a produselor controlate și, dacă este necesar, asigură generarea variabilelor criptografice;

(f) efectuează analize, revizuiri și teste de securitate, în special pentru a elabora rapoartele de risc relevante, în conformitate cu cerințele autorității de acreditare în materie de securitate;

(g) furnizează cursuri de formare în domeniul asigurării informațiilor specifice SIC-ului;

(h) pune în aplicare și utilizează măsuri de securitate specifice SIC-ului.

CAPITOLUL 4

Ofițerul local de securitate

Articolul 11

Numirea LSO

(1) LSO și LSO adjuncți trebuie să fie funcționari sau agenți temporari.

(2) Toți LSO și LSO adjuncți trebuie să dețină o autorizare de securitate valabilă pentru accesul la IUEC până la nivelul SECRET UE/EU SECRET și până la nivelul TRÈS SECRET UE/EU TOP SECRET, dacă este necesar. LSO și LSO adjunct trebuie să obțină autorizația de securitate înainte de numirea lor.

(3) Reprezentanțele Comisiei pot solicita CSA să acorde o excepție de la cerințele prevăzute la alineatele (1) și (2).

Articolul 12

Proceduri operaționale de securitate pentru zonele securizate

(1) LSO al departamentului în cauză al Comisiei elaborează SecOP pentru fiecare zonă securizată aflată în responsabilitatea sa.

(2) LSO se asigură că SecOP includ următoarele cerințe:

(a) numai membrii personalului care dețin o autorizare de securitate valabilă și o necesitate stabilită de a avea acces la documente clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sunt autorizați să aibă acces neînsoțiți într-o zonă securizată în timpul programului de lucru;

(b) accesul neînsoțit într-o zonă securizată în afara programului de lucru se acordă numai LSO al departamentului, RCO al (ai) zonei securizate, adjuncților acestora și personalului autorizat din cadrul Direcției Securitate a Direcției Generale Resurse Umane și Securitate;

(c) dispozitivele de înregistrare și comunicare, cum ar fi telefoanele mobile, calculatoarele, aparatele foto sau alte dispozitive inteligente, nu sunt permise în interiorul zonelor securizate fără o autorizare prealabilă din partea CSA; orice derogare trebuie solicitată CSA în prealabil; LSO acționează ca punct de contact;

(d) toți membrii personalului intern sau extern care solicită acces la o zonă securizată, dar care nu îndeplinesc criteriile prevăzute la litera (a) de mai sus trebuie să fie însoțiți și supravegheați în permanență de către un membru al personalului autorizat în mod corespunzător; orice astfel de acces într-o zonă securizată trebuie înregistrat într-un registru păstrat la intrarea în zona securizată;

(e) LSO se asigură că sistemele de detectare a intruziunilor care monitorizează o zonă securizată sunt active și funcționează corespunzător în permanență; LSO gestionează toate parolele, cheile, PIN-urile sau alte mecanisme de acces și de autentificare aferente;

(f) alarmele declanșate într-o zonă securizată se raportează Direcției Securitate din cadrul Direcției Generale Resurse Umane și Securitate, care notifică imediat LSO;

(g) LSO al departamentului în care se află zona securizată ține evidența fiecărei intervenții efectuate în urma declanșării unei alarme sau a producerii unui incident de securitate;

(h) trebuie să existe proceduri care să acopere eventualitatea unei alarme sau a unei alte situații de urgență în interiorul zonei securizate, inclusiv evacuarea personalului și asigurarea unui răspuns rapid din partea unei echipe de urgență aflate sub autoritatea CSA și a serviciilor de urgență externe, după caz;

(i) LSO raportează imediat CSA orice încălcare a securității care are loc în interiorul unei zone securizate sau care implică o astfel de zonă, pentru a stabili răspunsul adecvat;

(j) birourile individuale, încăperile și seifurile din interiorul unei zone securizate sunt ținute încuiate ori de câte ori sunt lăsate nesupravegheate;

(k) personalul evită discuțiile despre informații clasificate pe coridoare sau în alte zone comune din zona securizată atunci când în apropierea lor se află persoane care nu dețin autorizarea de securitate.

Articolul 13

Chei și combinații de securitate

(1) LSO are responsabilitatea generală de a asigura manipularea și stocarea corespunzătoare a cheilor și a combinațiilor utilizate în zonele securizate sau pentru accesarea acestora. Cheile și combinațiile se stochează într-un container de securitate și sunt protejate cel puțin la același nivel ca și materialul la care dau acces.

(2) LSO ține un registru al containerelor de securitate și al camerelor tezaur, precum și o listă actualizată a tuturor membrilor personalului care au acces neînsoțit la acestea.

(3) LSO ține un registru al cheilor pentru containerele de securitate și camerele tezaur, inclusiv al membrilor personalului cărora le sunt alocate. Se păstrează o dovadă de primire pentru fiecare cheie eliberată, inclusiv identificarea cheii, destinatarul, data și ora.

(4) Cheile și combinațiile se eliberează numai personalului care are necesitatea de a cunoaște și căruia i-a fost acordată autorizarea corespunzătoare pentru a avea acces la IUEC. LSO recuperează cheile atunci când condițiile menționate mai sus nu mai sunt îndeplinite.

(5) LSO păstrează chei de rezervă și o evidență scrisă a fiecărei combinații în plicuri individuale sigilate, opace, semnate și datate, care trebuie furnizate de membrul personalului responsabil de chei. Plicurile respective sunt păstrate într-un container de securitate căruia i se acordă un nivel de clasificare echivalent cu cel al materialului depozitat în containerul respectiv sau în camera tezaur respectivă cu cel mai înalt nivel de clasificare.

(6) În cazul în care, la schimbarea combinației sau la rotația cheilor, un plic prezintă semne de manipulare frauduloasă sau de deteriorare, LSO tratează acest lucru ca pe un incident de securitate și informează imediat CSA.

(7) Modificarea setărilor combinațiilor containerelor de securitate din zonele securizate se efectuează sub supravegherea LSO. Combinațiile se resetează cel puțin o dată la 12 luni și ori de câte ori:

(a) se primește un nou container sau se instalează o nouă încuietoare (în special, combinațiile implicite trebuie schimbate imediat);

(b) se suspectează o compromitere sau s-a produs o compromitere;

(c) accesul nu mai este necesar pentru o persoană care deține o combinație.

(8) LSO ține evidența datelor la care s-au efectuat modificările combinațiilor menționate la alineatul (7).

Articolul 14

Planuri de evacuare și de distrugere de urgență a IUEC

(1) LSO îl asistă pe șeful de departament la stabilirea planurilor de evacuare și de distrugere de urgență a IUEC, pe baza orientărilor furnizate de Direcția Securitate a Direcției Generale Resurse Umane și Securitate.

(2) LSO se asigură că orice echipament necesar pentru funcționarea planurilor prevăzute la alineatul (1) este disponibil cu ușurință și menținut într-o stare de funcționare bună.

(3) LSO, împreună cu funcționarii desemnați în planurile prevăzute la alineatul (1), reexaminează nivelul de pregătire a planurilor cel puțin o dată la 12 luni și ia toate măsurile necesare pentru actualizarea acestora.

Articolul 15

Autorizările de securitate

(1) LSO ține evidența tuturor posturilor din cadrul departamentului care necesită o autorizare de securitate din partea Comisiei, precum și a personalului care ocupă posturile respective. Cerința deținerii unei autorizări de securitate trebuie specificată în anunțul de post vacant în cursul procesului de recrutare și comunicată candidatului în timpul interviului.

(2) LSO supraveghează toate cererile de autorizări de securitate pentru accesul la IUEC. LSO este punctul de contact din cadrul departamentului și asigură legătura cu CSA pentru autorizările de securitate.

(3) LSO inițiază cererea de lansare a procedurii de autorizare de securitate pentru membrul personalului în cauză și se asigură că membrul personalului returnează prompt CSA chestionarul privind autorizarea de securitate națională.

(4) LSO se asigură că membrii personalului din departament care au primit autorizarea de securitate națională participă la cursul obligatoriu de informare privind IUEC pentru a obține autorizarea de securitate.

(5) LSO colaborează în mod regulat cu serviciul de resurse umane al departamentului pentru a obține informații cu privire la orice modificare a posturilor care necesită o autorizare de securitate și informează fără întârziere CSA cu privire la orice astfel de modificare.

(6) LSO informează CSA atunci când sosește un nou membru al personalului care deține deja o autorizare de securitate pentru a ocupa un post care necesită autorizarea de securitate.

(7) LSO se asigură că membrii personalului din cadrul departamentului finalizează procedura de reînnoire a autorizării de securitate în termenul prevăzut. Orice membru al personalului care refuză să finalizeze procedura este obligat să se transfere pe un post care nu necesită deținerea autorizării de securitate.

Articolul 16

Registratura IUEC

(1) În cazul în care un departament gestionează o registratură IUEC, LSO supraveghează activitățile RCO în ceea ce privește gestionarea IUEC și respectarea normelor de securitate referitoare la protecția IUEC.

(2) LSO efectuează următoarele verificări cel puțin o dată la 12 luni și la schimbarea unui RCO sau a unui RCO adjunct:

(a) o verificare a unui eșantion din documentele din registratura IUEC pentru a confirma statutul acestora și fiabilitatea registrului documentelor clasificate;

(b) o verificare a unui eșantion din confirmările de primire și de transmitere pentru distribuirea IUEC către și din registratura IUEC;

(c) o verificare a unui eșantion din certificatele de distrugere.

(3) Cel puțin o dată pe lună, LSO efectuează verificări prin sondaj ale registrului documentelor clasificate și ale documentelor clasificate primite recent, pentru a se asigura că documentele sunt înregistrate corect.

(4) Toate controalele se înregistrează în fișierul-jurnal al registrului documentelor clasificate.

Articolul 17

Alte responsabilități în materie de securitate

Celelalte responsabilități în materie de securitate ale LSO sunt stabilite într-o comunicare privind securitatea referitoare în special la securitatea fizică a persoanelor, a incintelor și a altor active, precum și a informațiilor.

CAPITOLUL 5

Ofițerul de control al registrului

Articolul 18

Numirea RCO

(1) RCO și RCO adjuncți trebuie să fie funcționari sau agenți temporari.

(2) Toți RCO și RCO adjuncți trebuie să dețină o autorizare de securitate valabilă pentru accesul la IUEC până la nivelul SECRET UE/EU SECRET și până la nivelul TRÈS SECRET UE/EU TOP SECRET, dacă este necesar. RCO și RCO adjunct trebuie să obțină autorizarea de securitate înainte de a fi numiți.

(3) Reprezentanțele Comisiei pot solicita CSA să acorde o excepție de la cerințele prevăzute la alineatele (1) și (2).

Articolul 19

Responsabilități

(1) RCO înregistrează informațiile clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior, în scopuri de securitate, atunci când:

(a) sosesc într-un departament al Comisiei sau pleacă de la un departament al Comisiei; sau

(b) sosesc într-un SIC sau când pleacă dintr-un SIC.

(2) RCO înregistrează toate evenimentele survenite în ciclul de viață al tuturor informațiilor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior. RCO se asigură, de asemenea, că se păstrează o evidență a tuturor informațiilor clasificate RESTREINT UE/EU RESTRICTED sau la un nivel echivalent care sunt transmise unor țări terțe și organizații internaționale, respectiv care sunt primite de la acestea. Acest lucru se face în coordonare cu registratura IUEC gestionată de Secretariatul General.

(3) RCO înregistrează documentele clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior în registrul documentelor clasificate și se asigură că acestea sunt stocate în siguranță în registratura IUEC.

(4) RCO asistă personalul Comisiei la crearea și transmiterea de informații clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior.

(5) Atunci când documente clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior sunt primite de la alte departamente sau de la părți externe, RCO asigură transmiterea corespunzătoare către emitent a confirmării de primire.

(6) Înainte de a permite unui membru al personalului să aibă acces la un document clasificat deținut de registratura IUEC, RCO verifică împreună cu LSO dacă membrul personalului respectiv are autorizare de securitate de la CSA.

(7) RCO înregistrează toți membrii personalului care intră și ies din registratura IUEC și care nu sunt autorizați să aibă acces neînsoțit și îi însoțesc pe întreaga durată a vizitei lor.

(8) Atunci când un membru al personalului scoate din registratura IUEC un document pentru a-l consulta, RCO se asigură că acesta știe care sunt măsurile de securitate compensatorii relevante și că membrul personalului returnează documentul de îndată ce nu mai are nevoie de el. RCO reamintește membrilor personalului să returneze orice astfel de document cât mai curând posibil.

(9) Registratura IUEC eliberează un certificat de curierat dacă documentele clasificate sunt transportate personal în afara țării în care se află registratura.

(10) Instrucțiunile detaliate pentru RCO privind înregistrarea documentelor clasificate sunt prevăzute într-o comunicare de securitate.

Articolul 20

Declasarea și declasificarea

RCO asistă departamentele inițiatoare în procesul de revizuire a IUEC înregistrate pentru a stabili dacă nivelul de clasificare inițial este în continuare adecvat sau dacă documentul poate fi declasat sau declasificat.

Articolul 21

Distrugere

(1) RCO sunt responsabili de distrugerea informațiilor clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL și la un nivel superior, prin mijloace aprobate, dacă este cazul în prezența unor martori care dețin autorizarea de securitate.

(2) RCO înregistrează orice distrugere a informațiilor clasificate la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL și la un nivel superior în registrul documentelor clasificate și păstrează certificatele de distrugere aferente în registratura IUEC.

Articolul 22

Sarcini suplimentare

(1) RCO furnizează LSO toată asistența de care au nevoie atunci când LSO desfășoară activități de supraveghere în registratura IUEC.

(2) RCO raportează orice incident de securitate suspectat sau real către LSO, care, la rândul său, îl raportează CSA.

(3) RCO al registraturii IUEC a unui departament al Comisiei care organizează o reuniune clasificată la nivelul CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior pregătește IUEC care vor fi manipulate în timpul reuniunii și se coordonează cu organizatorul reuniunii pentru a se asigura că toate documentele și confirmările de primire sunt tratate în conformitate cu normele relevante.

CAPITOLUL 6

Dispoziții finale

Articolul 23

Transparența

Prezenta decizie se aduce la cunoștința personalului Comisiei și a tuturor persoanelor cărora li se aplică și se publică în *Jurnalul Oficial al Uniunii Europene*.

Articolul 24

Prezenta decizie intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 7 aprilie 2022.

Pentru Comisie,
Pentru Președinte,
Gertrud INGESTAD
Director general
Direcția Generală Resurse Umane și Securitate