G U V E R N U L R O M Â N I E I

OFICIUL REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

O R D I N

pentru aprobarea Directivei privind structurile cu responsabilități în domeniul INFOSEC – INFOSEC 1

În temeiul:

- art.1 alin.(4) lit.b) şi art.3 alin.(6) din Ordonanța de urgență a Guvernului nr.153/2002 privind organizarea şi funcționarea Oficiului Registrului Național al Informațiilor Secrete de Stat, aprobată prin Legea nr.101/2003, cu modificările şi completările ulterioare,

- art.55 alin.(1) din Regulamentul privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea şi prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum şi a altor documente, în vederea adoptării/aprobării, aprobat prin Hotărârea Guvernului nr.561/2009,

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

emite prezentul

O R D I N:

Art.1 – Se aprobă Directiva privind structurile cu responsabilități în domeniul INFOSEC – INFOSEC 1, prevăzută în anexa care face parte integrantă din prezentul ordin.

Art.2 - La data intrării în vigoare a prezentului ordin se abrogă Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 482/2003 pentru aprobarea Directivei privind structurile cu responsabilități în domeniul INFOSEC – INFOSEC 1, publicat în Monitorul Oficial al României, Partea I, nr. 874 din 9 decembrie 2003.

Art.3 – Oficiul Registrului Național al Informațiilor Secrete de Stat va duce la îndeplinire prevederile prezentului ordin.

DIRECTOR GENERAL

MARIUS PETRESCU

București,
Nr. 86/2013

Anexă

DIRECTIVA PRIVIND STRUCTURILE CU RESPONSABILITĂȚI ÎN DOMENIUL INFOSEC – INFOSEC 1

CAPITOLUL I
INTRODUCERE

Art.1 - Prezenta directivă stabileşte şi defineşte structurile şi funcţiile cu atribuţii în domeniul INFOSEC, precum şi principalele responsabilităţi ale acestora, la nivel naţional, în scopul asigurării protecţiei corespunzătoare a informaţiilor clasificate.

Art.2 - În cuprinsul prezentei directive, în cazul în care nu se fac precizări suplimentare, prin informaţii clasificate se definesc informaţii naţionale clasificate secret de stat, informaţii NATO clasificate, informaţii UE clasificate sau informaţii clasificate care fac obiectul unor tratate, acorduri sau înţelegeri internaţionale la care România este parte.

CAPITOLUL II
Structuri cu responsabilităţi în domeniul INFOSEC

Art.3 - Protecţia informaţiilor clasificate stocate, procesate sau transmise în sisteme informatice, de comunicaţii şi alte sisteme electronice, denumite în continuare SIC, este coordonată la nivel naţional de către Oficiul Registrului Naţional al Informaţiilor Secrete de Stat (ORNISS) prin intermediul Agenţiei de Acreditare de Securitate (AAS), Agenţiei de Securitate pentru Informatică şi Comunicaţii (ASIC) şi al Agenţiei pentru Distribuirea Materialului Criptografic (ADMC).

Art.4 - Responsabilităţile generale ale ORNISS în domeniul INFOSEC sunt următoarele:

a) asistarea structurilor/funcţionarilor de securitate din cadrul persoanelor juridice de drept public sau privat naţionale pentru asigurarea securităţii informaţiilor clasificate stocate, procesate sau transmise prin intermediul SIC;

b) efectuarea de inspecţii periodice privind măsurile de securitate pentru protecţia informaţiilor clasificate stocate, procesate sau transmise în SIC naţionale, pentru a determina dacă aceste măsuri sunt adecvate şi în conformitate cu prevederile NATO, UE şi naţionale în vigoare, referitoare la domeniul INFOSEC, sau care fac obiectul unor tratate, acorduri sau înţelegeri internaţionale la care România este parte;

c) asigurarea pe plan naţional a cadrului de reglementare privind accesul la informaţiile clasificate stocate, procesate sau transmise în SIC, în conformitate cu prevederile politicilor de securitate NATO, UE şi naţionale în vigoare, referitoare la domeniul INFOSEC, sau care fac obiectul unor tratate, acorduri sau înţelegeri internaţionale la care România este parte;

d) asigurarea, prin reglementări şi acreditări, a compatibilizării sistemelor naționale de protecție a informațiilor clasificate, stocate, procesate sau transmise în SIC cu sisteme din statele membre NATO sau UE, ori din state cu care România a încheiat tratate, acorduri sau înțelegeri.

Art.5 - Agenția de Acreditare de Securitate (AAS) este o structură componentă a ORNISS, specializată în principal în gestionarea procesului de acreditare de securitate pentru SIC naționale care vehiculează informații clasificate şi a entităților care sprijină procesul de acreditare de securitate.

Art.6 - Principalele responsabilități ale AAS sunt:

a) acordarea de consultanță cu privire la implementarea standardelor INFOSEC autorităților operaționale ale SIC, funcționarilor/structurilor de securitate, managerilor de proiect, autorităților responsabile cu achizițiile, entităților care sprijină procesul de acreditare de securitate;

b) gestionarea procesului de acreditare de securitate pentru SIC care procesează, stochează sau transmit informații clasificate;

c) stabilirea strategiei de acreditare de securitate, care detaliază criteriile, etapele şi termenele aferente procesului de acreditare de securitate. Procedurile de acreditare de securitate pot să difere în funcție de situație, dar trebuie să fie întotdeauna în conformitate cu politicile NATO, UE şi națională de securitate, precum şi cu prevederile tratatelor, acordurilor sau înțelegerilor internaționale la care România este parte;

d) verificarea, evaluarea şi formularea de propuneri cu privire la aprobarea documentației care susține procesul de acreditare de securitate a SIC;

e) verificarea implementării şi menținerii măsurilor de securitate în cadrul SIC supuse acreditării de securitate, în principal prin inspecții periodice, desfăşurate conform strategiei de acreditare de securitate;

f) formularea de propuneri care stau la baza deciziei privind acreditarea de securitate a SIC;

g) acordarea de consultanță autorităților operaționale ale SIC în ceea ce priveşte evaluarea riscului de securitate, reluarea periodică a procesului de management al riscului de securitate şi acceptarea riscului rezidual;

h) acordarea de consultanță autorităților operaționale ale SIC şi structurilor/funcționarilor de securitate în procesul de investigare a incidentelor INFOSEC, estimarea prejudiciului creat, adoptarea de măsuri corective;

i) acordarea de consultanță autorităților operaționale ale SIC cu privire la implicațiile oricăror propuneri de modificare a arhitecturii SIC, din punct de vedere al riscurilor de securitate şi al măsurilor de securitate corespunzătoare;

j) asigurarea dialogului cu alte autorități de acreditare de securitate în cazul interconectării SIC, situație în care stabileşte, împreună cu aceste autorități, documentația de securitate necesară interconectării;

k) aprobarea sau, după caz, participarea la aprobarea comună a interconectării SIC;

l) gestionarea procesului de acreditare a structurilor interne INFOSEC din cadrul Autorităților Desemnate de Securitate, denumite în continuare ADS;

m) stabilirea modului de derulare a unor activități specifice procesului de acreditare de securitate a SIC, de către structurile interne INFOSEC, din cadrul ADS, acreditate de ORNISS;

n) gestionarea procesului de acreditare a entităților care sprijină procesul de acreditare de securitate a SIC;

o) păstrarea evidenței şi raportarea incidentelor de securitate din SIC acreditate către structurile abilitate din cadrul NATO, UE sau către structurile prevăzute de tratatele, acordurile sau înțelegerile internaționale la care România este parte;

p) gestionarea evidenței SIC acreditate, în curs de acreditare sau cu acreditare expirată.

Art.7 - Agenția de Securitate pentru Informatică şi Comunicații (ASIC) este o structură componentă a ORNISS specializată în reglementarea şi verificarea implementării mecanismelor de protecție a informațiilor clasificate stocate, procesate sau transmise în SIC naționale.

Art.8 - Principalele responsabilități ale ASIC sunt:

a) asigurarea faptului că sistemele, produsele şi mecanismele criptografice utilizate pentru protecția informațiilor clasificate, altele decât cele din categoria cifrului de stat, sunt selectate, operate, utilizate şi întreținute în mod adecvat;

b) coordonarea dialogului pe problematica securității comunicațiilor şi a altor aspecte tehnice din domeniul INFOSEC cu structurile NATO, UE şi naționale abilitate;

c) elaborarea şi promovarea de politici de securitate şi reglementări privind domeniul INFOSEC şi monitorizarea eficienței acestora;

d) asigurarea concordanței dintre măsurile INFOSEC selectate şi implementate pentru protecția informațiilor clasificate şi politicile relevante care reglementează aceste măsuri;

e) coordonarea activității de formare şi dezvoltare a culturii de securitate în domeniul protecției informațiilor vehiculate prin SIC;

f) aprobarea măsurilor de securitate TEMPEST aplicate pentru protecția informațiilor clasificate;

g) emiterea certificatelor de conformitate pentru produsele criptografice destinate protecției informațiilor naționale clasificate, altele decât cele din categoria cifrului de stat;

h) certificarea produselor INFOSEC destinate protecției informațiilor clasificate, altele decât cele precizate la lit. g), conform reglementărilor naționale în domeniu;

i) analizarea cauzelor provocatoare de incidente INFOSEC şi gestionarea bazei de date privind vulnerabilităţile din SIC, necesară pentru evaluarea modului de realizare a managementului riscului de securitate al SIC;

j) recomandarea de măsuri de securitate care să conducă la diminuarea riscurilor de securitate identificate;

k) derularea, împreună cu AAS, de inspecţii de securitate periodice sau inopinate, pentru verificarea modului de implementare şi menţinere a măsurilor de securitate în cadrul SIC supuse acreditării de securitate, pe întreg ciclul de viaţă al SIC.

Art.9 - Agenţia pentru Distribuirea Materialului Criptografic (ADMC) este o structură componentă a ORNISS specializată în managementul şi distribuirea materialelor criptografice NATO, UE sau a celor care fac obiectul unor tratate, acorduri sau înţelegeri internaţionale la care România este parte.

Art.10 - Principalele responsabilităţi ale ADMC sunt:

a) asigurarea managementului şi evidenţei centralizate a materialelor criptografice;

b) verificarea modului de implementare a măsurilor de securitate criptografică în locaţiile destinate păstrării şi/sau utilizării materialelor criptografice;

c) asigurarea distribuirii materialelor criptografice către destinatarii finali;

d) raportarea incidentelor de securitate criptografică la ASIC, precum şi la structurile specializate din cadrul NATO, UE sau prevăzute de tratatele, acordurile sau înţelegerile internaţionale la care România este parte.

Art.11 - Autoritatea Desemnată de Securitate (ADS) este instituţia abilitată prin lege să stabilească, pentru domeniul său de activitate şi responsabilitate, structuri şi măsuri proprii privind coordonarea şi controlul activităţilor referitoare la protecţia informaţiilor secrete de stat, inclusiv a celor stocate, procesate sau transmise în SIC.

Art.12 - Principalele responsabilităţi ale ADS în domeniul INFOSEC sunt următoarele:

a) organizarea sistemelor de protecţie a informaţiilor clasificate în instituţie;

b) organizarea şi executarea auditului intern al sistemelor de securitate;

c) gestionarea, prin intermediul structurilor interne INFOSEC acreditate de ORNISS, a procesului de acreditare de securitate a SIC care stochează, procesează sau transmit informaţii naţionale clasificate secret de stat, aflate în administrare proprie;

d) elaborarea de norme şi măsuri specifice de securitate;

e) derularea periodică a procesului de management al riscului la adresa securităţii informaţiilor clasificate procesate, stocate sau transmise prin intermediul SIC;

f) cooperarea cu ORNISS pentru asigurarea unui nivel adecvat de protecţie a informaţiilor clasificate, în conformitate cu prevederile legislaţiei naţionale, ale standardelor NATO şi UE în domeniu, precum şi ale tratatelor, acordurilor sau înţelegerilor internaţionale la care România este parte.

Art.13 - Structura/funcţionarul de securitate reprezintă punctul de contact pe problematica INFOSEC dintre organizaţia în cadrul căreia îşi desfăşoară activitatea şi ORNISS.

Art.14 - Structura/funcţionarul de securitate are următoarele responsabilităţi în domeniul INFOSEC:

a) elaborarea normelor interne privind protecţia informaţiilor clasificate, care trebuie să includă şi prevederi referitoare la domeniul INFOSEC;

b) coordonarea activităţii interne de protecţie a informaţiilor clasificate în toate componentele acesteia, care includ şi domeniul INFOSEC;

c) asigurarea relaţionării cu agenţiile din cadrul ORNISS abilitate să coordoneze activitatea în domeniul INFOSEC şi asigurarea controlului măsurilor referitoare la protecţia informaţiilor clasificate vehiculate în SIC;

d) monitorizarea internă privind aplicarea normelor de protecţie a informaţiilor clasificate vehiculate în SIC şi a modului de respectare a acestora;

e) asigurarea consultanţei pentru conducerea organizaţiei din care face parte, în domeniul securităţii informaţiilor clasificate;

f) informarea conducerii organizaţiei din care face parte cu privire la riscurile de securitate asociate SIC şi propunerea de măsuri pentru diminuarea acestora;

g) organizarea de programe de pregătire specifică a persoanelor care au acces la informaţii clasificate, care să includă şi problematica specifică domeniului INFOSEC;

h) efectuarea de controale privind modul de aplicare a măsurilor de protecţie a informaţiilor clasificate care includ şi domeniul INFOSEC;

i) stabilirea autorităţii operaţionale a SIC care răspunde de implementarea şi exploatarea operaţională a SIC din organizaţia în cadrul căreia îşi desfăşoară activitatea.

Art.15 - Autoritatea Operaţională a SIC, denumit în continuare AOSIC, este compartimentul care răspunde de implementarea şi menţinerea măsurilor de securitate, precum şi de exploatarea operaţională a SIC.

Art.16 (1) - Principalele responsabilităţi ale AOSIC sunt următoarele :

a) elaborarea şi actualizarea documentaţiei de securitate aferentă procesului de acreditare de securitate a SIC din responsabilitatea sa;

b) propunerea de măsuri INFOSEC în vederea implementării acestora în SIC din responsabilitatea sa, în cooperare cu structura de planificare a SIC şi asigurarea faptului că măsurile INFOSEC sunt implementate şi menţinute;

c) stabilirea, încă de la începutul ciclului de viaţă a sistemului, a resurselor necesare aplicării standardelor INFOSEC;

d) participarea la selectarea şi testarea măsurilor de securitate asociate SIC din responsabilitate şi supravegherea punerii lor în aplicare, pentru a se asigura că instalarea,

configurarea, exploatarea şi întreținerea acestora se realizează în conformitate cu documentația de securitate aprobată;

e) asigurarea formării şi dezvoltării culturii de securitate în domeniul protecției informațiilor vehiculate prin SIC;

f) asigurarea derulării eficiente a procesului de acreditare de securitate a SIC; solicitarea reacreditării de securitate, în conformitate cu cerințele stabilite de către AAS;

g) asigurarea implementării şi menținerii măsurilor de securitate asociate SIC în conformitate cu documentația de securitate aprobată;

h) verificarea periodică a implementării şi menținerii măsurilor de securitate asociate SIC, pentru a se asigura că acestea sunt în conformitate cu documentația de securitate aprobată;

i) investigarea cazurilor de încălcare sau a celor în care se suspectează încălcarea măsurilor de securitate, evaluarea prejudiciului cauzat şi raportarea concluziilor către structura de planificare a SIC şi către AAS;

j) asigurarea managementului materialului criptografic şi asigurarea custodiei elementelor criptografice şi celor controlate şi, dacă este cazul, asigurarea generării variabilelor criptografice.

(2) În funcție de complexitatea SIC, AOSIC poate conține, pe lângă administratorul de securitate al SIC şi administratorul de sistem, şi alte persoane, cum ar fi administratorul de securitate al componentei de comunicații a SIC, administratori de securitate pentru zonele terminalelor SIC etc., care pot avea atribuții similare cu cele ale administratorului de securitate al SIC, corespunzătoare domeniului lor de responsabilitate.

(3) AOSIC asigură controlul şi evidența activităților desfăşurate de utilizatorii SIC. În cazul în care SIC este interconectat cu alte SIC aflate sub controlul altor AOSIC, aceasta trebuie să colaboreze cu celelalte AOSIC pentru a se asigura că securitatea SIC propriu nu este afectată.

(4) În cazul interconectării mai multor SIC, trebuie încheiat un acord oficial între AOSIC implicate, acord care să stabilească limitele de responsabilitate ale fiecărei părți, cerințele de securitate şi cerințele privind acreditarea de securitate pentru fiecare dintre SIC interconectate.

Art.17 – (1) Structura de planificare a SIC răspunde de planificarea, la nivelul organizației, a întregii activități referitoare la un SIC, de exemplu durata etapelor, resursele financiare, resursele materiale şi resursele umane necesare asigurării securității SIC, pe durata întregului ciclu de viață a acestuia.

(2) Responsabilitățile structurii de planificare a SIC, referitoare la domeniul INFOSEC, corespunzătoare fiecărei etape a ciclului de viață a unui SIC, sunt cele specificate în Directiva principală privind domeniul INFOSEC - INFOSEC 2.

CAPITOLUL III

Funcţii cu responsabilităţi în domeniul INFOSEC

Art.18 - Toate SIC, indiferent de complexitatea lor, trebuie să aibă un administrator de securitate al SIC. Administratorul de securitate răspunde de aspectele de securitate asociate SIC, inclusiv de administrarea zilnică a securităţii acestuia.

Art.19 – (1) Atribuţiile administratorului de securitate al SIC trebuie să includă următoarele:

a) elaborarea şi actualizarea documentaţiei de securitate a SIC din responsabilitate şi asigurarea diseminării acesteia către ceilalţi administratori ai sistemului şi către utilizatori, în părţile care îi privesc;

b) păstrarea evidenţei privind luarea la cunoştinţă, de către administratorii şi utilizatorii SIC, a documentaţiei de securitate;

c) asigurarea formării şi dezvoltării culturii de securitate în domeniul protecţiei informaţiilor vehiculate prin SIC, pentru administratorii şi utilizatorii SIC. Acest proces este periodic şi poate fi realizat în următoarele moduri:

- prin afişarea pe ecranele staţiilor de lucru ale utilizatorilor SIC a unor mesaje de avertizare de tip banner, la deschiderea sesiunilor de lucru pe sistem;
- prin distribuirea unor afişe de conştientizare privind securitatea SIC;
- prin efectuarea unor demonstraţii practice privind măsurile tehnice şi procedurale de securitate aplicate în SIC.

d) Menţinerea evidenţei persoanelor autorizate să utilizeze SIC, a autorizaţiilor/certificatelor de acces la informaţii clasificate deţinute de acestea, a necesităţii de a cunoaşte informaţiile stocate, procesate sau transmise prin intermediul SIC;

e) controlarea şi emiterea de parole sau alte elemente ale sistemului de control al accesului şi asigurarea faptului că administratorii şi utilizatorii gestionează în mod adecvat aceste elemente;

f) verificarea implementării şi menţinerii măsurilor de securitate aprobate pentru componentele hardware, firmware şi software ale SIC, pentru a se asigura că acestea sunt în conformitate cu documentaţia aprobată;

g) asigurarea aplicării corecte a măsurilor de securitate a transmisiei, emisiei şi criptografice, inclusiv a celor referitoare la gestionarea, întreţinerea şi protecţia materialului criptografic conform reglementărilor în vigoare;

h) asigurarea gestionării adecvate a mediilor de stocare ale SIC;

i) asigurarea faptului că mediile de stocare conţinând informaţii clasificate sunt utilizate numai în SIC acreditate în mod corespunzător;

j) executarea, la intervale stabilite, a unor verificări prin sondaj privind existența fizică a mediilor de stocare clasificate şi corectitudinea marcării acestora, precum şi păstrarea unei evidențe a verificărilor efectuate;

k) verificarea faptului că mediile de stocare sunt declasificate prin mecanisme aprobate;

l) verificarea informațiilor de audit privind activitățile utilizatorilor;

m) verificarea şi testarea copiilor de siguranță (back-up), precum şi a altor elemente relevante pentru restaurarea sistemului;

n) gestionarea aspectelor de management al configurației din perspectiva modificărilor relevante pentru securitate şi a documentelor asociate;

o) raportarea către AOSIC a oricăror incidente/suspiciuni de incidente/prejudicii/ vulnerabilități/anomalii în ceea ce priveşte securitatea SIC;

p) asigurarea implementării şi menținerii măsurilor de securitate aplicate locațiilor în care sunt instalate elementele componente ale SIC;

r) acordarea de consultanță celorlalți administratori şi utilizatorilor SIC;

s) asigurarea faptului că activitățile de întreținere a SIC se efectuează fără a fi afectată securitatea acestuia;

t) participarea, împreună cu AAS şi ceilalți membri ai AOSIC, la investigarea cazurilor de încălcare a securității sau a încercărilor de încălcare a securității SIC, care privesc informațiile clasificate.

(2) În cazul în care administratorul de securitate are drepturi de administrare depline, acesta trebuie să dețină certificat de securitate sau autorizație de acces la informații clasificate de nivel superior nivelului de clasificare a informațiilor procesate, stocate sau transmise în SIC.

Art.20 - Toate SIC, indiferent de complexitatea lor, trebuie să aibă un administrator de sistem. Administratorul de sistem răspunde de funcționarea sistemului în conformitate cu documentația de securitate aprobată.

Art.21 (1) - Principalele responsabilități ale administratorului de sistem sunt următoarele:

a) implementarea măsurilor de securitate aplicabile configurației hardware şi software, activitate realizată sub coordonarea administratorului de securitate;

b) crearea/blocarea/dezactivarea conturilor;

c) implementarea modificărilor şi îmbunătățirilor configurației SIC, astfel încât obiectivele securității SIC să nu fie afectate;

d) asigurarea utilizării echipamentelor SIC în condiții optime;

e) gestionarea şi repartizarea capacităților hardware şi software;

f) asigurarea întreținerii şi reparării echipamentelor SIC;

g) actualizarea evidențelor privind funcționarea SIC;

h) raportarea către AOSIC a oricăror incidente/suspiciuni de incidente/prejudicii/vulnerabilități/anomalii în ceea ce privește funcționarea sistemului.

(2) În cazul în care administratorul de sistem are drepturi de administrare depline, acesta trebuie să dețină certificat de securitate sau autorizație de acces la informații clasificate de nivel superior nivelului de clasificare a informațiilor procesate, stocate sau transmise în SIC.

Art.22 - În funcție de complexitatea SIC, poate fi numit și un administrator COMSEC. Administratorul COMSEC al SIC răspunde de aspectele referitoare la securitatea echipamentelor de comunicații ale SIC. De asemenea, administratorul COMSEC răspunde și de aplicarea și respectarea normelor privind securitatea emisiilor (TEMPEST) pentru echipamentele și locațiile SIC.

Art.23 - Principalele responsabilități ale administratorului COMSEC privind securitatea echipamentelor de comunicații ale SIC sunt următoarele:

a) participarea la elaborarea și actualizarea documentației de securitate, potrivit domeniului său de responsabilitate;

b) acordarea de consultanță pentru AOSIC și utilizatorii SIC, privind securitatea echipamentelor de comunicații ale SIC;

c) garantarea faptului că întregul personal care are acces la echipamentele de comunicații ale SIC deține certificat de securitate corespunzător, cunoaște regulile de securitate locală și este supravegheat pe durata desfășurării activității;

d) păstrarea evidenței tuturor persoanelor autorizate să utilizeze echipamentele de comunicații ale SIC și a punctelor de unde pot să le utilizeze;

e) garantarea faptului că în cadrul SIC se asigură:

- securitatea echipamentelor de comunicații ale SIC în conformitate cu prevederile legale în vigoare;

- proceduri și mecanisme pentru identificarea și autentificarea corespondentului;

- controlul accesului;

- auditul activităților;

f) participarea la pregătirea și finalizarea acordurilor privind interconectarea SIC, din punct de vedere al securității echipamentelor de comunicații ale SIC;

g) asigurarea implementării modificărilor și îmbunătățirilor hardware, firmware și software ale echipamentelor de comunicații ale SIC, în scopul asigurării faptului că obiectivele securității SIC nu sunt afectate;

h) păstrarea evidenței înlocuirilor, modificărilor și defectelor hardware, firmware și software ale echipamentelor de comunicații și analizarea periodică a evidenței acestora;

i) asigurarea faptului că activitățile de întreținere a echipamentelor de comunicații ale SIC se efectuează fără a fi afectată securitatea acestora;

j) păstrarea şi analizarea jurnalelor privind funcționarea echipamentelor de comunicații ale SIC. Aceste jurnale trebuie să conțină suficiente detalii privind activitățile SIC care să permită reconstituirea istoricului evenimentelor, inclusiv monitorizarea şi înregistrarea activităților (ora şi data) care afectează securitatea echipamentelor de comunicații ale SIC;

k) realizarea şi gestionarea adecvată a copiilor de siguranță (back-up) aferente echipamentelor de comunicații ale SIC;

l) monitorizarea aspectelor privind managementul configurației, referitoare la schimbările hardware, firmware sau sofware, precum şi ale documentației asociate, care pot afecta securitatea echipamentelor de comunicații ale SIC;

m) raportarea către AOSIC a oricăror incidente/suspiciuni de incidente /prejudicii/ vulnerabilități/anomalii în ceea ce priveşte securitatea comunicațiilor;

n) participarea, împreună cu AAS şi ceilalți membri ai AOSIC, la investigarea cazurilor de încălcare sau a încercărilor de încălcare a securității echipamentelor de comunicații ale SIC;

o) păstrarea legăturii cu AAS, prin intermediul AOSIC, privind toate aspectele referitoare la securitatea echipamentelor de comunicații ale SIC.

Art.24 - Principalele responsabilități ale administratorului COMSEC privind securitatea emisiilor (TEMPEST) sunt următoarele:

a) acordarea de consultanță structurii de planificare a SIC, managerului de proiect şi AOSIC privind măsurile de securitate a emisiilor (TEMPEST) necesar a fi aplicate şi criteriile de selectare şi instalare a echipamentelor SIC în locațiile acestuia;

b) gestionarea proceselor de implementare a măsurilor de securitate a emisiilor (TEMPEST), a procesului de zonare a locațiilor în care urmează să fie instalate echipamentele sistemului şi a procesului de selectare, evaluare, certificare şi instalare a echipamentelor TEMPEST;

c) executarea de verificări periodice în scopul asigurării faptului că nu au fost instalate echipamente şi dispozitive neautorizate sau că echipamentele SIC nu au fost supuse încercărilor de acces neautorizat;

d) asigurarea măsurilor de securitate fizică în vederea contracarării unor fenomene electromagentice, de exemplu: ecranare prin panouri/paravane/armătură, EMI/EMP, bariere RFI (garnituri/manşoane RFI), sigilii etc.;

e) asigurarea faptului că echipamentele utilizate temporar, pe durata unor activități specifice, nu încalcă regulile de securitate a emisiilor existente şi nu perturbă funcționarea celorlalte echipamente permanente ale SIC;

f) păstrarea evidenței tuturor derogărilor de la măsurile TEMPEST care au fost aprobate pentru SIC;

g) Păstrarea evidenței tuturor echipamentelor protejate TEMPEST implementate în sistem, evidență care să includă sigiliile TEMPEST aplicate şi valabilitatea certificatului fiecărui echipament.

Art.25 - În funcție de complexitatea SIC, poate fi numit şi un administrator TRANSEC. Administratorul TRANSEC al SIC poate fi numit, de exemplu, numai pentru SIC interconectate şi răspunde de aspectele referitoare la securitatea transmisiei informațiilor prin intermediul sistemelor electromagnetice, indiferent de formatul acestora (ex.: audio, date, mesaje, grafică).

Art.26 - Principalele responsabilități ale administratorului TRANSEC sunt următoarele:

a) participarea la elaborarea şi actualizarea documentației de securitate, potrivit domeniului său de responsabilitate;

b) asigurarea implementării şi menținerii măsurilor de securitate a transmisiilor;

c) acordarea de consultanță pentru AOSIC şi utilizatorii SIC referitoare la aspecte de securitate a transmisiilor;

d) elaborarea rapoartelor referitoare la securitatea transmisiilor;

e) prezentarea/expunerea problemelor de specialitate în cadrul pregătirii/instruirii personalului SIC;

f) raportarea către AOSIC a oricăror incidente/suspiciuni de incidente/prejudicii/ vulnerabilități/anomalii în ceea ce priveşte securitatea transmisiilor.

Art.27 - În cazul în care în SIC este folosit material criptografic NATO sau UE, trebuie numit şi un administrator CRIPTO. Administratorul CRIPTO răspunde de aspectele referitoare la securitatea materialului criptografic deținut.

Art.28 - Principalele responsabilități ale administratorului CRIPTO privind securitatea criptografică în cadrul SIC sunt următoarele:

a) asigurarea nemijlocită a managementului şi controlului materialului criptografic pe care îl are în custodie (înregistrat în evidențele sale);

b) asigurarea primirii, verificării, păstrării, transferului, protecției şi distrugerii materialului criptografic, păstrarea şi actualizarea evidenței rapoartelor referitoare la materialul criptografic din custodia sa, în conformitate cu prevederile instrucțiunilor în vigoare pentru domeniul criptografic;

c) aplicarea procedurilor de folosire a materialului criptografic;

d) realizarea periodică a inventarierii materialului criptografic;

e) distrugerea materialul criptografic;

f) asigurarea faptului că materialul criptografic este pus numai la dispoziția persoanelor autorizate corespunzător, ale căror sarcini de serviciu implică accesul la acesta. Administratorul CRIPTO le va face cunoscută obligația de a proteja materialul pe perioada de timp cât se află în posesia acestuia.

g) raportarea către ADMC a tuturor aspectelor referitoare la încălcarea sau încercările de încălcare a securității criptografice (probabile, posibile sau efective), care au legătură cu gestionarea materialului criptografic în conformitate cu prevederile legale în vigoare.

Art.29 - Înlocuitorul administratorului CRIPTO participă, alături de administratorul CRIPTO, la toate activitățile de management al materialului criptografic NATO sau UE şi asigură continuitatea acestora în absența administratorului CRIPTO.

Art.30 - Atribuțiile înlocuitorului administratorului CRIPTO sunt următoarele:

a) cunoaşterea activității zilnice specifice, pentru a fi în măsură să preia şi să-şi asume responsabilitățile administratorului CRIPTO atunci când este cazul, fără a provoca întreruperi în activitatea criptografică;

b) îndeplinirea tuturor responsabilităților administratorului CRIPTO pe perioada absenței acestuia.

Art31 - Pentru gestionarea de material criptografic UE, administratorul CRIPTO şi înlocuitorul acestuia trebuie să dețină certificat de acces la informații clasificate de nivel minim SECRET UE/EU SECRET. În cazul în care în cadrul contului COMSEC sunt gestionate zece sau mai multe titluri scurte de material criptografic SECRET UE/EU SECRET, administratorul CRIPTO şi înlocuitorul acestuia trebuie să dețină certificat de acces la informații TRES SECRET UE/EU TOP SECRET.

Art.32 - Pentru gestionarea de material criptografic NATO, administratorul CRIPTO şi înlocuitorul acestuia trebuie să dețină certificat de acces la informații clasificate corespunzător nivelului maxim de clasificare a materialelor deținute în contul COMSEC. În cazul în care în cadrul contului COMSEC sunt gestionate zece sau mai multe titluri scurte de material criptografic NATO SECRET, administratorul CRIPTO şi înlocuitorul acestuia trebuie să dețină certificat de acces la informații COSMIC TOP SECRET.

Art.33 - Administratorul CRIPTO şi înlocuitorul acestuia trebuie să urmeze un program de pregătire specifică pentru desfăşurarea activității criptografice.

Art.34 - Administratorul de securitate al obiectivului SIC este responsabil de asigurarea implementării şi menținerii măsurilor de securitate fizică referitoare la domeniul INFOSEC, aplicabile locațiilor SIC. De asemenea, este responsabil de raportarea către AOSIC a oricăror încălcări ale măsurilor de securitate fizică.

Art.35 - Responsabilitățile unui administrator de securitate al obiectivului SIC pot fi îndeplinite de către structura/funcționarul de securitate al instituției respective, ca parte a îndatoririlor sale profesionale.

Art.36 - Administratorul de securitate al obiectivului SIC are următoarele responsabilități:

a) participarea la elaborarea şi actualizarea documentației de securitate, potrivit domeniului său de responsabilitate;

b) monitorizarea permanentă a tuturor aspectelor privind securitatea fizică specifice SIC;

c) implementarea şi menţinerea măsurilor de securitate fizică, aprobate prin documentaţia de securitate a SIC;

d) asigurarea accesului în locaţiile SIC numai pentru personalul autorizat;

e) păstrarea şi actualizarea evidenţei tuturor persoanelor care au autorizaţie de acces în locaţiile SIC;

f) aplicarea măsurilor adecvate de control al accesului în obiectivul SIC, controlarea şi/sau furnizarea elementelor de identificare a personalului referitoare la accesul în locaţiile SIC;

g) asigurarea implementării, testării şi întreţinerii sistemului de securitate fizică aferent locaţiilor SIC;

h) păstrarea evidenţei evenimentelor referitoare la securitatea fizică a SIC;

i) supravegherea modului de efectuare a oricăror modificări care privesc securitatea fizică a locaţiilor SIC;

j) asigurarea faptului că întregul personal al SIC îşi cunoaşte responsabilităţile cu privire la securitatea fizică a locaţiilor SIC;

k) asigurarea faptului că evidenţele şi înregistrările conţinând informaţii referitoare la acces şi controlul accesului în locaţiile SIC sunt păstrate şi consultate în conformitate cu prevederile documentaţiei de securitate;

l) asigurarea verificării periodice a modului de acţiune în situaţii de urgenţă;

m) asigurarea instruirii şi pregătirii corespunzătoare a administratorilor de securitate ai zonei terminalelor, conform domeniului său de competenţă;

n) raportarea către AOSIC a oricăror incidente/suspiciuni de incidente/prejudicii/ vulnerabilităţi/anomalii în sistemul de securitate fizică al SIC.

Art.37 - În cazul în care un SIC are terminale sau alte echipamente aflate la distanţă (de exemplu, în alte clădiri sau în zone separate de locaţia principală), se poate numi câte un administrator de securitate pentru fiecare astfel de zonă.

Art.38 - Administratorul de securitate al zonei terminalelor SIC are următoarele responsabilităţi principale:

a) implementarea politicii de securitate a SIC în zona de care răspunde;

b) aplicarea măsurilor de securitate specifice terminalelor şi celorlalte echipamente aferente aflate în zona sa de responsabilitate;

c) raportarea către AOSIC a oricăror incidente/suspiciuni de incidente/prejudicii/ vulnerabilităţi/anomalii privind zona sa de responsabilitate.

Art.39 - Utilizatorii SIC au obligaţia de a respecta prevederile documentaţiei de securitate a sistemului, în părţile care îi privesc.

Art.40 - Utilizatorii au următoarele responsabilităţi principale:

a) însuşirea şi respectarea procedurilor de securitate;

b) raportarea imediată către administratorul de securitate al SIC a oricăror incidente/suspiciuni de incidente/prejudicii/vulnerabilități/anomalii privind SIC.

Art.41 - Managerul de proiect este persoana care răspunde de proiectul SIC pe durata întregului ciclu de viață a sistemului.

Art.42 - Responsabilitățile managerului de proiect referitoare la domeniul INFOSEC, corespunzătoare fiecărei etape generice a ciclului de viață a unui SIC sunt cele specificate în Directiva principală privind domeniul INFOSEC - INFOSEC 2.