Atribuțiile postului pentru funcția publică de execție de consilier, clasa I, grad profesional asistent, din cadrul Compartimentului Structura de Securitate

a) implementează metodele, mijloacele și măsurile necesare protecției informațiilor în format electronic;

b) are atribuții privind exploatarea operațională a SPAD și RTD-SIC în condiții de securitate;

c) coordonează cooperarea dintre unitatea deținătoare a SPAD sau RTD-SIC și autoritatea care asigură acreditarea;

d) implementează măsurile de securitate și protecția criptografică ale SPAD sau RTD-SIC;

e) solicită acreditarea/reacreditarea SIC de la A.A.I.A.S. pentru următoarele activități:

1. planificarea dezvoltării sau achiziția unui SIC care stochează, procesează sau transmit informații clasificate;
2. propunerea privind schimbarea configurației de sisteme existente;
3. propunerea privind conectarea cu un alt SIC;
4. propunerea pivind schimbările modului de operare al SIC;
5. propunerea privind modificările sau înlocuitorilor software-ului pentru optimizarea securității SIC;
6. inițierea procedurilor de modificare a clasei sau nivelului de securitate ale SIC care au fost deja acreditate;
7. planificarea sau propunerea privind desfășurarea oricărei alte activități în scopul oricărei alte activități în scopul îmbunătățirii securității SIC care au fost deja acreditate.

f) solicită asistența de specialitate din partea A.A.I.A.S. și A.A.I.S.I.C. pentru stabilirea cerințelor de scuritate și procedurilor de aplicare necesare și respectării de către furnizorii de echipamente, pe durata întregului proces de dezvoltare, instalare și testare SIC;

g) răspunde de alegerea, implementarea, justificarea și controlul facilităților de securitate, de natură tehnică, care reprezintă parte componentă a SIC;

h) asigură exploatarea în condiții de securitate a SIC;

i) realizează legătura între contractant A.A.I.S.I.C. și A.A.I.A.S.;

j) participă la selecționarea, organizarea și realizarea pregătirii personalului cu atribuții în domeniul INFOSEC;

k) organizează și desfășoară convocări de instruire cu personalul din subordine și utilizatorii din SIC;

l) stabilește responsabilitățile personalului din subordine;

m) verifică periodic sau în timp real, implenentarea măsurilor de protecție a SIC din cadrul unității/structurii, pentru a se asigura că securitatea acestuia este în concordanță cu cerințele de securitate aprobate de A.A.I.A.S.;

n) ține evidența echipamentelor SIC, proprietate privată, autorizate să funcționeze în incinta unități, în condițiile capitolului XI la O.m.a.i.nr. 810/2005, pentru aprobarea

Normelor de aplicare a Standardelor naționale de protecție a informațiilor clasificate în sistemele informatice și de comunicații –INFOSEC în instituțiile M.A.I.;

o) cercetează incidentele de securitate și raportează rezultatele, ierarhic A.A.I.A.S. și A.A.I.S.I.C, concomitent cu aplicarea unor măsuri de reducere a consecințelor;

p) în calitate de administrator de securitate al SIC îndeplinește urmatoarele atribuții principale:

1. Elaborează și actualizează Procedurile operaționale de securitate (PrOpSec);
2. Monitorizează permanent toate aspectele de securitate specifice SIC;
3. Participă la elaborarea și actualizarea documentelor "Cerințe de Securitate Specifice",

"Cerințe de Securitate Comune" și "Cerințe de Securitate Specifice pentru Protecția Informațiilor în format electronic într-un SIC" pentru sistemele de care răspunde;

4. Actualzează și ține evidența tuturor utilozatorilor autorizați;
5. Aplică măsurile adecvate de control al accesului la SIC respectiv;
6. Verifică elementele de identificare a utilizatorilor;
7. Asigură evidența evenimentelor legate de securitatea sistemului și a sesiunilor de lucru;
8. Evaluează implicațiile, în planul securității, privind modificările software, hardware, firmware și procedurile propuse SIC;
9. Verifică dacă personalul cu acces la SIC cunoaște responsabilitățile care revin în domeniul protecției informațiilor;
10. Verifică dacă personalul cu acces autorizat la SIC cunoaște responsabilitățile care revin în domeniul protecției informațiilor;
11. Verifică modul de executare a întreținerii și actualizării software-ului pentru a nu se periclita securitatea sistemului;
12. Asigură un control riguros al mediilor de stocare a informațiilor și documentației sistemului verificând concordanța între clasa și nivelul de secretizare și a informațiilor stocate și marcajul de securitate a informațiilor stocate;
13. Ia măsuri tehnice și organizatorice pentru protecția mediilor de stocare a informațiilor față de câmpurile electromagnetice și accesul la informațiile clasificate;
14. Execută controale privind modul de utilizare a mediilor de stocare a informațiilor;
15. Asigură păstrarea și consultarea documentației și a datelor de evidență și control, refritoare la securitate, în conformitate cu PrOpSec;
16. Stabilește proceduri de verificare pentru utilizarea în SIC numai a software-ului autorizat;
17. Asigură, împreună cu administratorul de sistem/rețea, aplicarea celor mai eficiente proceduri de creare a copiilor de rezervă și de recuparere software;
18. Asigură instruirea și pregătirea corespunzătoare a administratorilor de securitate în zona terminalelor izolate;
19. Raportează conducătorului instituției orice breșe de securitate, vulnerabilități și încălcări ale măsurilor de scuritate;

q) În calitate de administrator de securitate al COMSEC îndeplinește urmatoarele atribuții principale:

1. Verifică și răspunde de instalarea echipamentelor SIC folosite în tranmiterea informațiilor clasificate în conformitate cu cerințele COMSEC ;
2. Verifică și răspunde de aplicarea în mod corespunzător a măsurilor de securitate a emisiilor-EMSEC și a transmisiilor-TRANSEC;
3. Ține evidența echipamentelor și sistemelor folosite la transmiterea informaților clasificate;
4. Cercetează incidentele de securitate și raportează rezultatele, ierarhic A.A.I.A.S. și A.A.I.S.I.C, concomitent cu aplicarea unor măsuri de reducere a consecințelor;

r) În calitate de administrator TRANSEC îndeplinește urmatoarele atribuții principale:

1. Asigură implementarea procedurilor de securitate și eficacitatea măsurilor de securitate a transmisiilor, în timpul testării SIC, precum și pe durata desfășurării exercițiilor și aliplicațiilor;
2. Coordonează elaborarea programelor TRANSEC;
3. Elaborează, verifică și aprobă rapoarte TRANSEC;
4. Prezintă probleme de specialitate în cadrul sedințelor de pregătire pe tema vulnerabilității unui sistem de comunicații deschis, neprotejat pe alte teme TRANSEC.

s) În calitate de administrator EMSEC îndeplinește urmatoarele atribuții principale:

1. Asigură măsurile tehnice de instalare a echipamntelor din SIC, în conformitate cu cerințele de securitate stabilite;
2. Supravechează ca executarea întreținerilor și modificările aduse echipamentelor protejate TEMPEST să se execute de personal calificat utilizându-se numai piese de schimb și component avizate de șeful INFOSEC și aprobate de funcționarul de securitate M.A.I.;
3. Solicită efectuarea controalelor periodice pe linie de TEMPEST sau când apar premise de scurgere a informațiilor prin radiații electromagnetice compromițătoare;

t) În calitate de custode cripto îndeplinește urmatoarele atribuții principale:

1. Ține evidența sistemelor criptografice deținute de CSTIC din structura/unitate din care face parte;
2. Distribuie materilele criptografice numai persoanelor autorizate;
3. Solicită asigurarea cu echipamente și materiale criptografice necesare funcționării sistemului de asigurare a protecției informațiilor clasificate;
4. Distruge materialele criptografice în conformitate cu prevederile legale în vigoare;

În baza prevederilor Standardelor naționale de protecție a informațiilor clasificate aprobate prin Hotărârea Guvernului României nr.585 din 13.06.2002, ale Ghidului privind structura și conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru Sistemele Informatice și de Comunicații – DS 2, aprobat de Directorul General al Oficiului Registrului Național al Informațiilor Secrete de Stat, fișa postului se completează cu următoarele atribuții și sarcini specifice ale titularului postului care decurg din calitatea de înlocuitor al administratorului de Securitate Local al componentei distante a SIC SIOCWEB din cadrul Ministerului Afacerilor Interne, Instituția Prefectului județul Hunedoara, după cum urmează:

În calitate de înlocuitor al administratorului de securitate local al SIC SIOCWEB are următoarele responsabilități:

a) elaborează Procedurile Operaționale de Securitate de la nivelul componentei proprii a SIC SIOCWEB;
b) cooperează cu administratorul de securitate a SIC SIOCWEB cu privire la orice aspect legat de securitatea componentei proprii a sistemului;
c) aplică măsurile cuprinse în Programul de prevenire a scurgerii de informații clasificate, referitoare la managementul securității SIC SIOCWEB;
d) acționează pentru îndeplinirea, întocmai și în termenele stabilite, a sarcinilor și atribuțiilor din documentele de planificare, implementare și dezvoltare a SIC SIOCWEB;
e) asigură corecta aplicare a măsurilor de securitate fizică și buna funcționare a acestora la nivelul locațiilor proprii în care sunt dispuse resursele SIC SIOCWEB;
f) asigură verificarea periodică a integrității resurselor SIC SIOCWEB prin verificarea sigiliilor de securitate aplicate la nivelul acestora;
g) informează șeful structurii de securitate și AOSIC cu privire la aspectele de interes pentru asigurarea securității SIC SIOCWEB;
h) aplică măsurile de control al accesului în locația terminalului propriu aferent SIC SIOCWEB și la terminalul SIC SIOCWEB, potrivit Programului de prevenire a scurgerii de informații clasificate și Procedurilor Operaționale de Securitate de la nivelul componentei proprii a SIC SIOCWEB
i) asigură, pe plan local, evidență și actualizarea fișelor de pregătire individuală a persoanelor autorizate să acceseze informații clasificate naționale și a administratorului de securitate local/înlocuitor;
j) primește cererile de vizitare a locației proprii a SIC SIOCWEB, coordonând toate activitățile aferente,
k) asigură instruirea și pregătirea utilizatorilor terminalului distant al SIC privind securitatea informațiilor, resurselor și serviciilor sistemului;
l) asigură reluarea semestrială a procesului de analiză de risc la nivelul componentei proprii a SIC SIOCWEB, rezultatele urmând a fi transmise AOSIC:
m) informează șeful structurii de securitate și cooperează cu administratorul de securitate al sistemului (componenta centrală) cu privire la aspectele de interes pentru asigurarea securității SIC SIOCWEB;
n) notifică SRI, imediat, cu privire la orice eveniment informatic sau incident de securitate survenit sau care este posibil a avea loc;
o) verifică anual modul de acțiune în situații de urgență, în conformitate cu prevederile capitolului VI al Procedurilor Operaționale de Securitate de la nivelul componentei proprii a SIC SIOCWEB;