

MINISTERUL AFACERILOR INTERNE
INSTITUȚIA PREFECTULUI – JUDEȚUL BISTRIȚA-NĂȘĂUD

Serviciul financiar contabil, resurse umane, achiziții, informatic și administrativ

Atribuțiile aferente funcției publice de execuție de consilier, grad profesional asistent din cadrul Compartimentului structura de securitate

- asigură măsurile de securitate, pe linie INFOSEC, conform normelor în vigoare;
 - solicită acreditarea/reacreditarea Sistemelor Informatice și de Comunicații (SIC) la Autoritatea Afacerilor Interne de Acreditare de Securitate (AAIAS);
 - solicită asistență de specialitate din partea AAIAS și Autoritatea Afacerilor Interne de Securitate pentru Informatică și Comunicații (AAISIC) pentru stabilirea cerințelor de securitate și procedurilor de aplicare necesare și respectarea de către furnizorii de echipamente, pe durata întregului proces de dezvoltare, instalare și testare SIC;
 - răspunde de alegerea, implementarea, justificarea și controlul facilităților de securitate, de natură tehnică, care reprezintă parte componentă a SIC;
 - asigură exploatarea în condiții de securitate a SIC;
 - realizează legătura între contractant, AAISIC și AAIAS;
 - participă la selecționarea, organizarea și realizarea pregătirii personalului cu atribuții în domeniul INFOSEC;
 - organizează și desfășoară convocări de instruire cu personalul din subordine și utilizatorii din SIC;
 - stabilește responsabilitățile personalului din subordine;
 - verifică periodic sau în timp real implementarea măsurilor de protecție în SIC, din cadrul instituției, pentru a se asigura că securitatea acestuia este în concordanță cu cerințele de securitate aprobate de AAIAS;
 - ține evidența echipamentelor SIC, proprietate privată, autorizate să funcționeze în incinta instituției, în condițiile capitolului XI din OMAI nr. 810/2005;
 - cercetează incidentele de securitate și raportează rezultatele, ierarhic, AAIAS și AAISIC, concomitent cu aplicarea unor măsuri de reducere a consecințelor;
 - asigură arhivarea și predarea, pe bază de proces-verbal, a tuturor documentelor conform nomenclatorului arhivistic.
1. În calitate de administrator de securitate a SIC îndeplinește următoarele atribuții principale:
- elaborează și actualizează Procedurile Operaționale de Securitate, denumite în continuare PrOpSec;
 - monitorizează permanent toate aspectele de securitate specifice SIC;
 - - participă la elaborarea și actualizarea documentelor "Cerințele de Securitate Specifice", "Cerințele de Securitate Comune" și "Cerințele de Securitate Specifice pentru protecția informațiilor în format electronic într-un SIC" pentru sistemele de care răspunde;
 - actualizează și ține evidența tuturor utilizatorilor autorizați;
 - aplică măsurile adecvate de control al accesului la SIC;
 - verifică elemente de identificare a utilizatorilor;
 - asigură evidența evenimentelor legate de securitatea sistemului și a sesiunilor de lucru;

- evaluează implicațiile, în planul securității, privind modificările software, hardware, firmware și procedurale propuse pentru SIC;
 - verifică dacă modificările de configurație a SIC afectează securitatea și dispune măsurile în consecință;
 - verifică dacă personalul cu acces autorizat la SIC cunoaște responsabilitățile care revin în domeniul protecției informațiilor clasificate;
 - verifică modul de executare a întreținerii și actualizării software-ului pentru a nu se periclita securitatea sistemului;
 - asigură un control riguros al mediilor de stocare a informațiilor și documentației sistemului, verificând concordanța între clasa sau nivelul de secretizare a informațiilor stocate și marcajul de secretizare al mediilor stocate;
 - ia măsuri tehnice și organizatorice pentru protecția mediilor de stocare a informațiilor față de câmpurile electromagnetice și accesul neautorizat la informații clasificate;
 - execută controale privind modul de utilizare a mediilor de stocare a informațiilor;
 - asigură păstrarea și consultarea documentației și a datelor de evidență și control, referitoare la securitate, în conformitate cu PrOpSec;
 - stabilește proceduri de verificare pentru utilizarea în SIC numai a software-ului autorizat;
 - asigură, împreună cu administratorul de sistem/rețea, aplicarea celor mai eficiente proceduri de creare a copiilor de rezervă și de recuperare software;
 - asigură instruirea și pregătirea corespunzătoare a administratorilor de securitate în zona terminalelor izolate;
 - raportează conducătorului instituției orice breșe de securitate, vulnerabilități și încălcări ale măsurilor de securitate.
2. În calitate de administrator COMSEC îndeplinește următoarele atribuții principale:
- verifică și răspunde de instalarea echipamentelor SIC folosite în transmiterea informațiilor clasificate în conformitate cu cerințele COMSEC;
 - verifică și răspunde de aplicarea în mod corespunzător a măsurilor de securitate a emisilor - EMSEC și a transmisiilor - TRANSEC;
 - ține evidența echipamentelor și sistemelor folosite la transmiterea informațiilor clasificate.
3. În calitate administrator EMSEC îndeplinește următoarele atribuții principale:
- asigură măsurile tehnice de instalare a echipamentelor din SIC, în conformitate cu cerințele de securitate stabilite;
 - supraveghează ca executarea întreținerilor și modificările aduse echipamentelor protejate TEMPEST să se execute de personal calificat, utilizându-se numai piese de schimb și componente avizate și aprobate de DGPI;
 - solicită efectuarea controalelor periodice pe linie TEMPEST sau când apar premise de scurgere a informațiilor prin radiații electromagnetice compromițătoare.
4. În calitate administrator TRANSEC îndeplinește următoarele atribuții principale:
- asigură implementarea procedurilor de securitate și eficacitatea măsurilor de securitate a transmisiilor, în timpul testării SIC, precum și pe durata desfășurării exercițiilor și aplicațiilor;
 - coordonează elaborarea programelor TRANSEC;
 - elaborează, verifică și aprobă rapoarte TRANSEC;
 - prezintă probleme de specialitate în cadrul ședințelor de pregătire pe tema vulnerabilității unui sistem de comunicații deschis, neprotejat și pe alte teme TRANSEC.
5. În calitate administrator CRIPTO îndeplinește următoarele atribuții principale:

- ține evidența sistemelor criptografice deținute de CSTIC din entitatea din care face parte;
- distribuie materialele criptografice numai personalului autorizat;
- solicită asigurarea cu echipamente și materiale criptografice necesare funcționării sistemului de asigurare a protecției informațiilor clasificate;
- distruge materialele criptografice, în conformitate cu prevederile legale în vigoare;
- raportează administratorului COMSEC și șefului CSTIC toate aspectele de insecuritate legate de gestionarea sistemelor criptografice.

6. În calitate de administrator de securitate local al componentei distante a SIC SIOCWEB îndeplinește următoarele atribuții principale:

- elaborează Procedurile Operaționale de Securitate de la nivelul componentei proprii a SIC SIOCWEB;
- cooperează cu administratorul de securitate a SIC SIOCWEB cu privire la orice aspect legat
- aplică măsurile cuprinse în Programul de prevenire a scurgerii de informații clasificate, referitoare la managementul securității SIC SIOCWEB;
- acționează pentru îndeplinirea, întocmai și în termenele stabilite, a sarcinilor și atribuțiilor din documentele de planificare, implementare și dezvoltare a SIC SIOCWEB;
- asigură corecta aplicare a măsurilor de securitate fizică și buna funcționare a acestora la nivelul locațiilor proprii în care sunt dispuse resursele SIC SIOCWEB;
- asigură verificarea periodică a integrității resurselor SIC SIOCWEB prin verificarea sigiliilor de securitate aplicate la nivelul acestora;
- informează șeful structurii de securitate și AOSIC cu privire la aspectele de interes pentru asigurarea securității SIC SIOCWEB;
- 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;
- asigură pe plan local, evidența și actualizarea fișelor de pregătire individuală a persoanelor autorizate să acceseze informații clasificate naționale și a administratorului de securitate local/înlocuitor;
- primește cererile de vizitare a locației proprii a SIC SIOCWEB, coordonând toate activitățile aferente;
- asigură instruirea și pregătirea utilizatorilor terminalului distant al SIC privind securitatea informațiilor, resurselor și serviciilor sistemului;
- asigură reluarea semestrială a procesului de analiză de risc la nivelul componentei proprii a SIC SIOCWEB, rezultatele urmând a fi transmise AOSIC;
- informează șeful structurii de securitate și cooperează cu administratorul de securitate a sistemului (componenta centrală) cu privire la aspectele de interes pentru asigurarea securității SIC SIOCWEB;
- notifică SRI, imediat, cu privire la orice eveniment informatic sau incident de securitate survenit sau care este posibil a avea loc;
- 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.
- respectă prevederile Regulamentului de organizare și funcționare precum și cel intern al instituției ;
- îndeplinește orice alte sarcini, care au legătură cu natura postului, stabilite de către prefect.