Atribuțiile postului: Îndeplineşte sarcinile specifice şefului CSTIC, iar prin cumul și cele prevăzute pentru:

- administratorul de securitate ;
- administratorul COMSEC ;
- administratorul TRANSEC ;
- administratorul EMSEC ;
- custodele cripto ;
- protecţia informaţiilor clasificate (PIC),

1. **Atribuții în calitate de șef CSTIC**
   a) Solicită acreditarea/reacreditarea SIC de la A.A.I.A.S. pentru următoarele activități:
      - planificarea dezvoltării sau achiziția unui SIC care stochează, procesează sau transmite informații clasificate;
      - propunerea schimbării configurației de sistem existente;
      - propunerea conectării cu un alt SIC;
      - propunerea de schimbare a modului de operare protejată ale SIC;
      - propunerea de modificare sau înlocuire a software-ului pentru optimizarea securității SIC;
      - inițierea procedurii de modificare a clasei sau nivelului de secretizare ale SIC care au fost deja acreditate.
   b) Solicită asistență de specialitate din partea A.A.I.A.S. și A.A.I.S.I.C. pentru stabilirea cerințelor de securitate și procedurilor de aplicare necesare și respectării de către furnizorii de echipamente, pe durata întregului proces de dezvoltare, instalare și testare SIC;
   c) Raspunde de alegerea, implementarea, justificarea și controlul facilităților de securitate, de natură tehnică, care reprezintă parte componentă a SIC;
   d) Asigură exploatarea în condiții de securitate a SIC;
   e) Realizează legătura între contractant, A.A.I.S.I.C și A.A.I.A.S;
   f) Participă la selecționarea, organizarea și realizarea pregătirii personalului cu atribuții în domeniul INFOSEC;
   g) Organizează și desfășoară convocări de instruire cu personalul din subordine și utilizatorii din SIC;
   h) Stabilește responsabilitățile personalului din subordine;
   i) Verifică periodic sau în timp real, implementarea măsurilor de protecție în 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;
   j) Ține evidența echipamentelor SIC, proprietate privată, autorizate să funcționeze în incinta unității;
   k) Cercetează incidentele de securitate și raportează rezultatele, ierarhic, A.A.I.A.S și A.A.I.S.I.C, concomitant cu aplicarea unor măsuri de reducere a consecințelor.

2. **Atribuții în calitate de administrator de securitate**
   a) Elaborează și actualizează Procedurile Operaționale de Securitate, denumite PrOpSec;

b) Monitorizează permanent toate aspectele de securitate specifice SIC;
c) 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;
d) Actualizează și ține evidența tuturor utilizatorilor autorizați;
e) Aplică măsurile adecvate de control al accesului la SIC respectiv;
f) Verifică elemente de identificare a utilizatorilor;
g) Asigură evidența evenimentelor legate de securitatea sistemului și a sesiunilor de lucru;
h) Evaluează implicațiile în planul securității, privind modificările software, hardware, firmware și procedurale propuse pentru SIC;
i) Verifică dacă modificările de configurație a SIC afectează securitatea și dispune măsurile în consecință;
j) Verifică dacă personalul cu acces autorizat la SIC cunoaște responsabilitățile care revin în domeniul protecției informațiilor;
k) Verifică modul de executare a întreținerii și actualizării software-ului pentru a nu se periclita securitatea sistemului;
l) 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;
m) Ia măsuri tehnice și organizatorice pentru protecția mediilor de stocare a informațiilor față de câmpurile electromagnetice și accesul neautorizat la informațiile clasificate;
n) Execută controale privind modul de utilizare a mediilor de stocare a informațiilor;
o) Asigură păstrarea și consultarea documentației și a datelor de evidență și control, referitoare la securitate, în conformitate cu PrOpSec;
p) Stabilește proceduri de verificare pentru utilizarea în SIC numai a software-ului autorizat;
q) Asigură aplicarea celor mai eficiente proceduri de creare a copiilor de rezervă și de recuperare software;
r) Asigură instruirea și pregătirea corespunzătoare a administratorilor de securitate în zona terminalelor izolate;
s) Raportează șefului C.S.T.I.C orice breșe de securitate, vulnerabilități și încălcări ale măsurilor de securitate.

3. Atribuții în calitate de administrator COMSEC

a) Verifică și răspunde de instalarea echipamentelor SIC folosite în transmiterea informațiilor clasificate în conformitate cu cerințele COMSEC;

b) Verifică și răspunde de aplicarea în mod corespunzător a măsurilor de securitate a emisiilor – EMSEC și a transmisiilor - TRANSEC;

c) Ține evidența echipamentelor și sistemelor folosite la transmiterea informațiilor clasificate.

4. **Atribuții în calitate de administrator TRANSEC**

a) Asigură implementarea procedurilor de securitate și eficacitatea măsurilor de securitate a transmisiilor, în timpul testării SIC, precum și pe durata desfășurării exercițiilor și aplicațiilor;

b) Coordonează elaborarea programelor TRANSEC;

c) Elaborează, verifică și aprobă rapoarte TRANSEC;

d) Prezintă probleme de specialitate în cadrul ședințelor de pregătire pe tema vulnerabilității unui sistem de comunicații deschis, neprotejat și pe alte teme TRANSEC.

5. **Atribuții în calitate de administrator EMSEC**

a) Asigură măsurile tehnice de instalare a echipamentelor din SIC, în conformitate cu cerințele de securitate stabilite;

b) 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 de șeful INFOSEC și aprobate de funcționarul de securitate M.A.I;

c) Solicită efectuarea controalelor periodice pe linie de TEMPEST sau când apar premise de scurgerea informațiilor prin radiații electromagnetice compromițătoare.

6. **Atribuții în calitate de custode cripto**

a) Ține evidența sistemelor criptografice deținute de C.S.T.I.C din structura/unitatea din care face parte;

b) Distribuie materialele criptografice numai persoanelor autorizate;

c) Solicită asigurarea cu echipamente și materiale criptografice necesare funcționării sistemului de asigurare a protecției informațiilor clasificate;

d) Distruge materialele criptografice, în conformitate cu prevederile legale în vigoare;

e) Raportează administratorului COMSEC și șefului C.S.T.I.C. toate aspectele de insecuritate legate de gestionarea sistemelor criptografice.

7. **Atribuţii pe linia protecţiei informaţiilor clasificate:**

a) Elaborează şi supune aprobării conducerii instituţiei normele interne privind protecţia informaţiilor clasificate, elaborate sau păstrate de instituţie, ulterior monitorizând aplicarea acestor norme la nivelul instituţiei;

b) Consiliază conducerea instituţiei în legătură cu toate aspectele privind securitatea informaţiilor clasificate;

c) În baza propunerilor formulate de către structurile de specialitate, elaborează şi actualizează Programul de prevenire a scurgerii de informaţii clasificate, pe care îl supune avizării Ministerului Afacerilor Interne şi aprobării conducerii instituţiei;

d) Organizează activitatea de pregătire specifică a persoanelor care au acces la informaţii clasificate;

e) Organizează şi asigură respectarea regulilor generale privind primirea, evidenţa, întocmirea, păstrarea, manipularea, multiplicarea, transportul şi repartizarea lucrărilor ce conţin informaţii clasificate;

f) Organizează activitatea de evidenţă a ordinelor şi instrucţiunilor ministrului afacerilor interne, precum şi a ştampilelor şi sigiliilor din dotarea Instituţiei Prefectului Județului Brăila;

g) Efectuează, cu aprobarea prefectului, controale privind modul de aplicare a măsurilor legale de protecţie a informaţiilor clasificate, în baza planificării;

h) Asigură păstrarea, evidenţa şi actualizarea certificatelor de securitate, a autorizaţiilor de acces la informaţii clasificate, a permiselor de acces în zonele de securitate şi a listelor informaţiilor clasificate;

i) Asigură relaţionarea cu instituţia abilitată să coordoneze activitatea şi să controleze măsurile privitoare la protecţia informaţiilor clasificate, potrivit legii;

j) Acordă sprijin reprezentanţilor autorizaţi ai instituţiilor publice abilitate, potrivit competenţelor legale, pe linia verificării persoanelor pentru care se solicită accesul la informaţii clasificate;

k) Asigură protecţia datelor şi a informaţiilor gestionate şi ia măsuri de prevenire a scurgerii de informaţii clasificate;

l) Asigură relaţionarea cu instituţia abilitată să presteze servicii de pază și protecție a obiectivului Instituția Prefectului Județului Brăila;

m) Arhivează și păstrează în condiții corespunzătoare documentele care conțin informații clasificate, potrivit nomenclatorului arhivistic al instituției.

8. Acționează în vederea îndeplinirii de către prefect, în condițiile legii, a atribuțiilor ce revin acestuia în domeniul organizării și desfășurării alegerilor locale, parlamentare, europarlamentare și prezidențiale, precum și a referendumului național ori local;

9. Constituie dosarele cu documentele create de compartiment, legate, numerotate, sigilate și parafate pe bază de inventare, pe termene de păstrare, conform nomenclatorului arhivistic și le predă compartimentului de arhivă pe bază de procese verbale de predare – primire, pe care le semnează;

10. Întocmește procedurile formalizate pentru activitățile aferente atribuțiilor postului;