**cu privire la aprobarea Regulamentului de organizare și funcționare a sistemului digital de radiocomunicații speciale critice în standardul TETRA**

**------------------------------------------------------------**

În temeiul art. 6 lit. h) din Legea nr. 136/2017 cu privire la Guvern (Monitorul Oficial al Republicii Moldova, 2017, nr. 252, art. 412), cu modificările ulterioare, GuvernulHOTĂRĂȘTE:

1. Se aprobă Regulamentul de organizare și funcționare a sistemului digital de radiocomunicații speciale critice în standardul TETRA, (se anexează).

2. La data intrării în vigoarea a prezentei hotărâri, entitățile publice care dispun de stații radio în standard TETRA, în termen de 6 luni, urmează să notifice Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne.

3. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

**Prim-ministru DORIN RECEAN**

Contrasemnează:

Ministrul afacerilor interne Ana Revenco

Aprobat

prin Hotărârea Guvernului nr.\_\_\_\_\_\_

din \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023

**REGULAMENT**

**de organizare și funcționare a sistemului digital de radiocomunicații speciale critice în standardul TETRA**

**I. DISPOZIȚII GENERALE**

**1.** Regulamentul de organizare și funcționare sistemului digital de radiocomunicații speciale critice în standardul TETRA (în continuare – *Regulament*) stabilește obiectul, scopul și domeniul de aplicare a Sistemului TETRA, prevederi generale privind structura, arhitectura și funcțiile sistemului digital de radiocomunicații speciale critice în standardul TETRA (în continuare – *sistem TETRA*), modul de organizare și conținutul informațional al acestuia, atribuțiile, drepturile, obligațiile și responsabilitățile subiecților raporturilor juridice, atribuțiile Consiliului coordonator, asigurarea integrității și securității sistemului TETRA și a confidențialității informației procesate de sistemul TETRA.

**2 .** Obiectul Regulamentului îl constituie stabilirea condițiilor și accesul la rețelele şi resursele de telecomunicații radio aflate în proprietatea Ministerului Afacerilor Interne în vederea asigurării unor servicii mobile private care să asigure sporirea interoperabilității autorităților naționale cu atribuții în domeniul gestionării situațiilor de urgență.

**3.** Scopul Sistemului constă în asigurarea transmiterii fiabile și securizate a mesajelor vocale și de date între abonați, prin infrastructură de comunicații (centre de comutare, celule radio, dispecerate, sisteme de management, magistrale de comunicații și terminale de utilizator), care implică un complex de mijloace tehnice (Hardware) și produse de program (Software) unificate în standard TETRA (TErrestrial Trunked RAdio).

**4.** Domeniul de aplicare constituie asigurarea funcționării rețelei de servicii radio, mobile voce şi date, criptate în cadrul Sistemului TETRA, pentru necesitățile autorităților şi instituțiilor statului în interiorul tării şi în cadrul cooperării transfrontaliere.

**5.** În sensul prezentului Regulament se definesc următoarele noțiuni:

*1) comunicații în standard TETRA* – transmisii, emisii sau recepții de semne, semnale, scrieri, imagini, sunete sau informații de orice natură prin fir, radio, sistem optic sau prin alte sisteme electromagnetice;

*2) claster* – reprezintă o conectivitate a 7 zone interconectate prin canale securizate de comunicații;

*3) echipamente MSO (Main Switch Office)* – complex de echipamente care constituie nodul central al sistemului TETRA și sunt necesare pentru procesarea apelurilor din interiorul unei zone, dar şi din afara acesteia, în cazul apelurilor între zone, dar şi cele folosite pentru managementul de rețea, configurarea sistemului și interconectarea cu rețeaua de telefonie fixă;

*4) Consiliul coordonator în domeniul radiocomunicațiilor în standard TETRA* – este organul colegial superior, format din reprezentanți ai autorităților administrative si instituțiilor din subordinea Ministerului Afacerilor Interne și altor autorități publice centrale care dețin dreptul de a gestiona sisteme speciale, care asigură coordonarea politicilor, precum și aprobarea deciziilor tehnico-administrative privind menținerea, dezvoltarea și acordarea accesului în cadrul sistemului la nivel departamental și interinstituțional;

*5) consola dispecer* – echipament complex tehnic și de program, care coordonează traficul și asigură monitorizarea, gestionarea şi organizarea resurselor de utilizatori în cadrul unei rețele de radiocomunicații;

*6) stația de bază* – reprezintă un echipament de infrastructură care asigură acoperirea cu semnal radio într-o arie geografică limitată;

*7) spațiul informațional* – mediu de activitate (digital, cibernetic, mediatic) asociat cu formarea, crearea, transformarea, transmiterea, difuzarea, utilizarea și stocarea informațiilor, care produce efecte la nivel de conștiință individuală şi/sau socială, de infrastructură informațională şi de informație.

*8) terminal radio* – echipament fix, mobil sau portabil care funcționează în standard TETRA şi asigură recepția/emisia semnalului radio;

*9) Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D)*  – standard de comunicații deschis definit de Institutul European de Standardizare în Telecomunicații (ETSI), axat în principal pe sectoare critice precum serviciile de urgență (poliție, pompieri, ambulanțe), destinat comunicațiilor și transmisia de date.

*10) zonă* – reprezintă un segment al sistemului acoperit de MSO, numărul de zone într-un sistem fiind determinat de numărul MSO disponibile.

**6.** Sistemul este creat și menținut cu respectarea următoarelor principii:

1) *cel mai bun efort* – care presupune că administratorul sistemului TETRA/prestatorul serviciilor de comunicații TETRA va depune toată diligența în vederea administrării sistemului TETRA și prestării serviciilor de comunicații TETRA la cea mai înaltă calitate posibilă;

2) *legalitate* – care presupune administrarea sistemului TETRA și prestarea serviciilor de comunicații TETRA în strictă conformitate cu prevederile prezentului Regulament și ale legislației aplicabile;

3) *calitate* – care presupune asigurarea prestării serviciilor TETRA fără întreruperi, eficiența economică la prestarea serviciilor de comunicații TETRA, punându-se accent pe adaptarea acestora la necesitățile utilizatorilor serviciilor sistemului TETRA;

4) *securitate şi confidențialitate –* care presupune garantarea caracterului privat, confidențialitatea, autenticitatea, integritatea şi nonrepudierea informațiilor prelucrate și disponibile în cadrul sistemului TETRA, precum și a sistemului TETRA.

5) *modularității și scalabilității*, care semnifică posibilitatea dezvoltării Sistemului fără modificarea componentelor create anterior.

**7.** Obiectivele sistemului TETRA sunt:

1) garantarea unui mediu de comunicații securizat şi fiabil care să ofere mijloace de comunicare atât subdiviziunilor din cadrul Ministerului Afacerilor Interne, cât şi altor autorități publice;

2) sporirea eficienței serviciilor specializate de urgență în scopul garantării unui nivel sporit de siguranță şi protecție a persoanei şi a bunurilor;

3) asigurarea acoperirii naționale a comunicațiilor în standard TETRA;

4) reducerea timpului de reacție la apelurile de urgență.

**II. STRUCTURA ȘI FUNCȚIILE SISTEMULUI**

**8.** Organizarea sistemului TETRA implică configurarea arhitecturii și managementul componentelor acestuia.

**9.** Sistemul TETRA îndeplinește următoarele funcții de bază:

1) formarea bazei de date a sistemului;

2) asigurarea informațională;

3) administrarea informațională;

4) asigurarea calității informațiilor din contul creării și menținerii calitative a componentelor sistemului;

5) protecția și securizarea informațiilor la toate etapele de formare a băncii de date a sistemului;

6) asigurarea comunicațiilor voce/date de înaltă calitate / securizate / criptate;

7) asigură confidențialitatea serviciilor între sistemul radio şi abonați;

8) asigurarea bunei funcționări a sistemului.

**10.** Sistemul TETRA are următoarele componente:

1) Terminal radio;

2) Consola Dispecer;

3) Stația de Bază;

4) Echipamente MSO;

5) Zonă;

6) Claster.

**11.** Sistemul TETRA furnizează următoarele tipuri de servicii:

1) Servicii vocale

2) Servicii de date

3) Servicii suplimentare a sistemului, în funcție de necesarul utilizatorilor și a capacitații infrastructurii.

Regulile și condițiile de acordare a accesului la sistem sunt aprobate de către Consiliul coordonator.

**12.** Sistemul TETRA are următoarea arhitectură:

1) infrastructura de comunicații (centre de comutare, celule radio, interfețe către alte sisteme de comunicații analogice/digitale, dispecerate, sisteme de management şi magistrale de comunicații);

2) terminale radio.

**13.** Termenul de păstrare a înregistrărilor în sistemul TETRA este de 6 luni, după care se radiază automat, în ordinea în care au fost stocate pe server.

**14.** Termenul de stocare a înregistrărilor din sistemul TETRA poate fi prelungit în temeiul:

1) actului procedural al agentului constatator, în legătură cu necesitatea folosirii acestora în calitate de probe în cazul unor eventuale contestații împotriva procesului-verbal cu privire la contravenție;

2) demersului motivat al organului de urmărire penală;

3) încheierii instanței judecătorești în legătură cu judecarea cauzei;

4) demersului motivat al subiecților care efectuează activitatea specială de investigații, în condițiile legii.

**15.** Termenul de stocare al înregistrărilor audio (voce) din sistemul TETRA nu poate fi prelungit decât pentru perioada necesară atingerii scopului urmărit, cu indicarea exactă a perioadei de timp.

**III. SPAȚIUL INFORMAȚIONAL**

**16.** Datele conținute în sistemul TETRA se gestionează și se clasifică conform Nomenclatorului informațiilor atribuite la secret de stat, aprobat de către Guvern, regulamentelor interne și standardelor, specificației tehnice a resurselor și sistemelor informaționale utilizate în contextul gestionării automatizate, aprobate în acest sens de către Consiliul coordonator al sistemului.

**17.** Spațiul informațional creat de sistemul TETRA este parte componentă a resurselor informaționale departamentale ale Ministerului Afacerilor Interne.

**IV. RAPORTURILE JURIDICE ÎN DOMENIUL CREĂRII, ADMINISTRĂRII, UTILIZĂRII SISTEMULUI TETRA ȘI PRESTĂRII SERVICIILOR DE COMUNICAȚII TETRA**

**Secțiunea 1**

**Subiecții raporturilor juridice**

**18.** Subiecții raporturilor juridice sunt:

1) proprietarul;

2) posesorul;

3) administratorii;

4) utilizatorii;

**19.** Proprietarul sistemului TETRA este statul, care își realizează dreptul de proprietate, gestionare și utilizare a informațiilor din acesta.

**20.** Posesorul sistemului TETRA este Ministerul Afacerilor Interne, care atribuie roluri și drepturi persoanelor autorizate pentru a exploata sistemul, în funcție de obligațiile de serviciu ale acestora.

**21.** Administratorii sistemului TETRA sunt Serviciul Tehnologii Informaționale a Ministerului Afacerilor Interne și Inspectoratul General al Poliției de Frontieră a Ministerului Afacerilor Interne.

**22.** Utilizatorii sistemului TETRA sunt reprezentanții autorităților administrative și a instituțiilor din subordinea Ministerului Afacerilor Interne sau a altor autorități publice, cărora li se asigură servicii de voce/date în cadrul sistemului, cu drept de acces intern deplin sau partajat în sistemul TETRA.

**Secțiunea a 2-a**

**Atribuțiile, drepturile şi obligațiile subiecților raporturilor juridice**

**23.** Posesorul sistemului TETRA are următoarele atribuții:

1) asigură condițiile organizatorice și financiare pentru funcționarea sistemului;

2) coordonează cu Serviciul de Informații și Securitate proiectele de creare a Sistemului, sarcinile tehnice de proiectare, construcție și reconstrucție a obiectelor, de elaborare a tehnologiilor și mostrelor de tehnică specială, în procesul exploatării sau aplicării cărora sânt vehiculate informații importante pentru stat;

3) stabilește scopurile și sarcinile funcționale ale sistemului;

4) asigură securitatea și protecția datelor din sistem prin intermediul structurilor specializate din componența sa sau instituțiilor și organizațiilor din subordine;

5) aprobă și coordonează cu administratorul sistemului executarea modificărilor și/sau rectificărilor solicitate în cererile privind erorile de sistem ale Sistemului, erorile cauzate de factorul uman în sistem, incidentele de infrastructură care afectează funcționalitatea sistemului;

6) după consultarea cu Consiliul coordonator în domeniul radiocomunicațiilor în standard TETRA (în continuare – *Consiliul coordonator*), încheie acorduri cu alte autorități administrative pentru acordarea dreptului de utilizator al sistemului;

7) exercită alte atribuții necesare asigurării bunei funcționări a sistemului.

**24.** Administratorii sistemului TETRA au următoarele atribuții:

1) actualizează necesarul de servicii şi resurse de comunicații la nivelul rețelei comune şi emite recomandări cu caracter tehnic către utilizatori pentru respectarea parametrilor de performanță ai acesteia;

2) promovează măsurile tehnice pentru asigurarea securității comunicațiilor în cadrul Sistemului, elaborate de custodele algoritmilor de criptare AIE (*Air Interface Encryption*);

3) asigură servicii pentru acțiunile de cooperare, pe baza informațiilor şi solicitărilor primite de la utilizatori;

4) emite reglementări şi certificări cu privire la compatibilitatea terminalelor, serviciilor şi aplicațiilor cu infrastructura sistemului;

5) asigură suport tehnic, la solicitarea utilizatorilor pentru elaborarea specificațiilor tehnice pentru echipamentele de infrastructură şi pentru terminalele TETRA, astfel încât acestea să fie compatibile cu infrastructura şi serviciile sistemului;

6) execută lucrări de instalare, întreținere şi exploatare pentru echipamentele care alcătuiesc infrastructura de comunicații aflată în administrare proprie şi pentru terminalele proprii;

7) modernizează serviciile de voce/date şi extinde aria de serviciu cu acordul Consiliului coordonator;

8) optimizează utilizarea resurselor de comunicații;

9) emite norme de exploatare şi măsuri de securitate pentru terminalele definite în cadrul sistemului propriu;

10) determină obiectele informaționale supuse înregistrării în sistem și conținutul acestora;

11) monitorizează și, după caz, ajustează cerințele de securitate și conformitate a sistemului la domeniul securității cibernetice, opțional la domeniul protecției datelor cu caracter personal;

12) monitorizează procesul de înregistrare și prelucrare a datelor în sistem;

13) gestionează activitatea de exploatare și ținere a conținutului informațional al sistemului;

14) stabilește măsurile tehnice și organizatorice de protecție și securitate a Sistemului;

15) să înainteze posesorului propuneri privind modificarea actelor normative care reglementează sistemul TETRA.

**25.** Administratorii poate avea şi calitatea de utilizatori ai serviciilor de voce și date în cadrul sistemului TETRA, pentru utilizatorii proprii.

**26.** Administratorii deține o infrastructură proprie, agreată de Consiliul coordonator şi integrată în cadrul sistemului TETRA.

**27.** Utilizatorii interni și externi ai sistemului TETRA au următoarele atribuții:

1) solicită lucrări de întreținere şi reparații pentru terminalele proprii;

2) actualizează necesarul propriu de servicii de comunicații;

3) solicită servicii pentru acțiunile de cooperare;

4) raportează administratorului problemele ce țin de funcționarea echipamentelor, infrastructurii și/sau a incidentelor de securitate în cadrul Sistemului;

5) respectă normele de exploatare şi măsurile de securitate impuse de către posesor și administrator pentru echipamentele terminale;

**28.** Utilizatorii interni și externi ai sistemului TETRA au următoarele drepturi:

1) să solicite Consiliului coordonator acordarea și modificarea drepturilor de acces la sistem, în limitele competențelor funcționale;

2) să înainteze Consiliului coordonator propuneri privind dezvoltarea Sistemului;

3) să propună modificări la cadrul normativ al sistemului;

4) să solicite administratorului verificarea compatibilității echipamentelor propuse spre integrare în Sistem;

5) să solicite Consiliului coordonator și administratorului asigurarea interoperabilității între utilizatorii sistemului TETRA;

6) să solicite administratorului operarea în Sistem a modificărilor privind politica de securitate şi drepturile de acces.

**29.** Utilizatorii interni și externi ai sistemului TETRA au următoarele obligații:

1) să respecte politica de securitate în cadrul sistemului;

2) să înainteze propuneri pentru includerea în Planul anual de mentenanță şi dezvoltare a sistemului;

3) să răspundă prompt şi deplin la solicitările Consiliului coordonator şi administratorului privind asigurarea bunei funcționări a sistemului;

4) să remedieze imediat defecțiunile tehnice din cadrul infrastructurii deținute;

5) să informeze în termeni utili pe alți utilizatori ai sistemului despre lucrările de mentenanță planificate;

6) să mențină şi să consolideze baza tehnico-materială pentru infrastructura deținută;

7) să respecte şi să execute deciziile Consiliului coordonator;

8) să execute necondiționat cerințele tehnice ale administratorului.

**30.** Fiecare utilizator trebuie să prevadă în statul de personal o funcție responsabilă de administrare a echipamentelor periferice, care sunt parte componentă a sistemului sau să desemneze această persoană prin act administrativ normativ. Numele, prenumele și datele de contact ale persoanelor angajate în aceste funcții, precum și orice modificări cu privire la datele acestora se comunică administratorului.

**Secțiunea a 3-a. Consiliul coordonator**

**31.** Realizarea funcțiilor de gestionare a sistemului TETRA este exercitată prin delegarea atribuțiilor corespunzătoare dintre Consiliul coordonator și Administratorii sistemului.

**32.** Componența şi numărul membrilor Consiliului coordonator se aprobă prin ordinul ministrului afacerilor interne și are următoarele atribuții:

1) elaborează conceptul de dezvoltare a sistemului;

2) aprobă proiectele tehnice de dezvoltare a sistemului, propuse de utilizatorii acestuia;

3) elaborează planul anual de mentenanță şi achiziții pentru sistem, în baza propunerilor utilizatorilor sistemului;

4) aprobă certificatele de testare tehnică a echipamentului supus testului de acceptanță a echipamentelor spre integrare în cadrul sistemului;

5) aprobă deciziile tehnico-administrative privind menținerea, dezvoltarea și acordarea accesului la sistem;

6) autorizează acordurile privind includerea altor instituții în sistem;

7) coordonează proiectele de acte normative ce vizează organizarea și funcționarea sistemului.

**33.** Consiliul coordonator are următoarele drepturi:

1) să solicite utilizatorilor sistemului informații referitoare la buna funcționare a acestuia;

2) să solicite de la utilizatorii sistemului, prezentarea propunerilor pentru întocmirea planului anual de mentenanță şi dezvoltare a sistemului;

3) să solicite revocarea dreptului de utilizator al sistemului prin rezilierea acordului de participare, în caz de abatere de la principiile de asigurare a securității în cadrul acestuia sau de la prevederile prezentului regulament;

4) să dispună utilizatorilor sistemului executarea sarcinilor tehnice şi de politici, în limitele competenței instituționale;

5) să inițieze elaborarea sau modificarea cadrului normativ pentru asigurarea funcționării şi dezvoltării sistemului, să propună utilizatorilor acestuia modificarea cadrului normativ instituțional;

6) să emită şi să formuleze decizii pentru executare către utilizatorii sistemului.

7) acces la informația referitoare la activitatea sistemului, cu respectarea principiului confidențialității şi prevederilor legislației privind protecția datelor cu caracter personal;

8) stabilește regulile de prestare şi utilizare a serviciilor sistemului.

**34.** Membrii Consiliului coordonator:

1) au obligația să respecte Regulamentul sistemului, să contribuie la realizarea funcțiilor şi atribuțiilor acestuia, să participe la ședințele Consiliului coordonator;

2) au obligația să participe la identificarea direcțiilor prioritare de dezvoltare ale sistemului, la evaluarea rapoartelor şi la revizuirea performanțelor.

**35.** Consiliul coordonator se convoacă după necesitate, la inițiativa Președintelui sau a vicepreședintelui Consiliului coordonator.

**36.** Ședința Consiliului coordonator este deliberativă în prezența majorității membrilor. Înștiințarea membrilor privind desfășurarea ședințelor Consiliului coordonator se efectuează din timp, cu cel puțin 3 zile lucrătoare anterior ședinței, de către secretarul Consiliului coordonator, în scris (prin scrisoare remisă în original sau prin e-mail), cu indicarea datei, timpului şi locului desfășurării acestora, ordinii de zi, cu anexarea materialelor aferente.

**37.** În lipsă de cvorum, în cel mult 5 zile lucrătoare, se convoacă ședința repetată a Consiliului coordonator. Membrii Consiliului coordonator vor fi informați despre ședința repetată cu cel puțin 2 zile lucrătoare până la data ședinței.

**38.** Hotărârile Consiliului coordonator se adoptă cu majoritatea minimă de voturi.

**39.** Ședințele Consiliului coordonator se consemnează în procesul-verbal, care reflectă în mod obligatoriu chestiunile examinate în cadrul ședinței şi informația privind înștiințarea membrilor Consiliului coordonator, lista participanților prezenți şi a celor absenți, luările de cuvânt, rezultatul votării fiecărei chestiuni din ordinea de zi.

**40.** Lucrările de secretariat ale Consiliului coordonator sunt executate de secretarul Consiliului.

**41.** Secretarul Consiliului este responsabil pentru păstrarea documentelor Consiliului coordonator, informarea membrilor Consiliului despre ședințele acestuia, participarea la ședințe şi întocmirea proceselor-verbale ale acestora.

**V. REGIMUL JURIDIC DE UTILIZARE A DATELOR**

**42.** Temei pentru obținerea dreptului de acces la sistemul TETRA (utilizarea terminalului radio) îl constituie solicitarea utilizatorului, transmisă administratorului sistemului.

**43.** Accesul la sistemul TETRA se acordă de către administrator conform atribuțiilor și funcțiilor deținute și regimul juridic al informației accesate. Nivelul de acces la informație pentru fiecare utilizator corespunde funcției de serviciu și/sau profilului de acces.

**44.** Resursele informaționale ale sistemului TETRA sunt segmentate pentru utilizatori interni și externi, având aceleași atribuții la utilizarea acestora.

**45.** Utilizatorii interni ai Sistemului sânt posesorul, administratorul, autoritățile administrative și instituțiile din subordinea Ministerului Afacerilor Interne, ale căror drepturi de acces sânt definite în acte administrative normative.

**46.** Utilizatorii externi ai sistemului TETRA sânt alte autorități publice, în conformitate cu cadrul normativ.

**47.** Administratorii gestionează datele din sistemul TETRA, în scopul prestării serviciilor de administrare, inclusiv mentenanță adaptivă și perfectivă a sistemului.

**48.** Furnizarea informațiilor din sistemului TETRA se efectuează exclusiv de către administrator, fiind documentată şi supusă unei analize riguroase privind necesitatea comunicării şi compatibilitatea între scopul în care se face comunicarea şi scopul pentru care aceste date au fost colectate inițial.

**49.** Cu excepția cazurilor de exercitare a drepturilor subiecților operațiunilor de monitorizare video, datele constituite din imagini se divulgă prin transmitere, dar nu mai târziu de 15 zile lucrătoare:

1) Centrului Național pentru Protecția Datelor cu Caracter Personal;

2) organelor abilitate cu atribuții în domeniul asigurării ordinii publice, securității statului, apărării naționale, urmăririi penale şi activităților speciale de investigații în condițiile legii;

3) instanțelor judecătorești.

**50.** În contextul dispozițiilor prevăzute la pct. 49, entitățile vizate au obligația de a prezenta în adresa administratorului solicitarea cu indicarea informațiilor relevante privind:

1) scopurile şi temeiurile legale ce atestă dreptul de acces la datele constituite din imagini;

2) intervalul de timp concret de înregistrare a datelor constituite din imagini la care se referă demersul;

3) specificarea amplasării mijloacelor de supraveghere video, care se constituie în calitate de surse de colectare a datelor constituite din imagini.

**51.** Datele se vor transmite doar în volumul şi condițiile specificate în demers și reieșind din posibilitățile tehnice a sistemului.

**52.** Exploatarea componentelor sistemului TETRA fără autorizare nominală este strict interzisă și urmează a fi considerată ca acces neautorizat la un sistem special de comunicații.

**53.** Dreptul de acces la sistemul TETRA nu este unul permanent, acesta poate fi suspendat sau revocat. Introducerea și/sau modificarea datelor în sistemul TETRA de pe un nume sau profil de utilizator străin este strict interzisă, urmând a fi considerată ca acces neautorizat. Utilizatorul asigură confidențialitatea profilului.

**54.** Revocarea dreptului de acces la sistemul TETRA se efectuează la cererea/demersul utilizatorului sistemului către administrator, în una dintre următoarele situații:

1) la încetarea/suspendarea raporturilor de muncă ale angajaților responsabili;

2) la intervenirea modificărilor raporturilor de muncă când noile atribuții nu impun accesul la sistem;

3) la inițiativa administratorului, ca urmare a constatării încălcării securității informaționale de către utilizator;

4) în alte cazuri, în conformitate cu cadrul normativ.

**55.** Lucrările profilactice planificate în complexul de mijloace software și hardware se efectuează după notificarea de către administrator, în scris sau prin e-mail, a părților interesate, în baza planului coordonat cu posesorul sau utilizatorul, cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil.

**56.** Lucrările neplanificate se efectuează la solicitarea utilizatorului în situația nefuncționării sau funcționării necorespunzătoare a complexului de mijloace software și hardware.

**57.** Funcționarea sistemului TETRA se suspendă de către administrator în următoarele cazuri:

1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware ale sistemului;

2) la apariția circumstanțelor de forță majoră;

3) la încălcarea securității informaționale, dacă aceasta prezintă pericol pentru funcționarea Sistemului;

4) la încălcarea legislației, inclusiv, cu privire la protecția datelor cu caracter personal.

**58.** În cazul apariției impedimentelor justificatoare, precum și a dificultăților tehnice în funcționarea complexului de mijloace software și hardware se suspendă temporar funcționarea sistemului cu notificarea ulterioară a utilizatorilor conectați.

**VI. ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI**

**59.** Datele din sistemului TETRA fac parte din categoria datelor oficiale cu accesibilitate limitată. Asigurarea securității, confidențialității și a integrității datelor prelucrate în cadrul sistemului se efectuează de către subiecții cu drepturi de acces la sistem cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

**60.** Măsurile de protecție și securitate a datelor din sistemul TETRA reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a sistemului și se actualizează de către toți subiecții sistemului.

**61.** Obiecte ale asigurării protecției și securității datelor din sistemul TETRA se consideră tot complexul de mijloace software și hardware care asigură realizarea proceselor informaționale:

1) baza de date, sistemele informaționale, sistemele operaționale, sistemele de gestiune a bazelor de date, sistemele de evidență și alte aplicații care asigură funcționarea sistemului;

2) sistemele de telecomunicații, rețelele, serverele, calculatoarele și alte mijloace tehnice de prelucrare a datelor.

**62.** Securitatea informațională a sistemului TETRA se efectuează prin aplicarea metodelor și efectuarea acțiunilor descrise în Planul de continuitate al sistemului și, după caz, a procedurilor operaționale, aprobate în acest sens de către Consiliul coordonator.

**63.** Protecția datelor din sistemului TETRA se efectuează prin următoarele metode:

1) prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor.

2) utilizarea obligatorie a produselor de program licențiate aprobate, iar orice solicitare de instalare a unui produs de program trebuie coordonată cu administratorul;

**64.** Subiecții la utilizarea și exploatarea sistemului TETRA asigură implementarea normelor de securitate, aceasta urmând să conțină acte ce confirmă:

1) identitatea persoanei responsabile de implementarea normelor de securitate și împuternicirile acesteia;

2) implementarea principalelor măsuri tehnico-organizatorice necesare asigurării funcționării Sistemului;

3) informarea utilizatorilor și instruirea acestora cu privire la modalitățile și mecanismele de asigurare a securității informaționale;

4) procedurile de control intern ale subiectului sistemului privind respectarea condițiilor de securitate informațională.

**65.** Pentru îndeplinirea sarcinilor privind asigurarea securității informaționale a sistemului TETRA sânt folosite următoarele mecanisme:

1) autentificarea și autorizarea;

2) dirijarea accesului;

3) înregistrarea acțiunilor și auditul securității;

4) criptarea informației.

**66.** Sistemul complex al securității informaționale asigură:

1) integritatea logică a informației;

2) integritatea fizică a informației;

3) protecția infrastructurii informaționale în cazul tentativelor de deteriorare sau de modificare a funcționării sistemului.

**67.** Schimbul informațional se efectuează cu utilizarea mijloacelor software și hardware, doar prin canale securizate, asigurând integritatea și securitatea datelor.

**68.** Autoritatea/instituția utilizator al sistemului TETRA desemnează o persoană subordonată nemijlocit conducătorului instituției, responsabilă de implementarea și monitorizarea respectării prevederilor normelor de securitate informațională.

**69.** Normele de securitate informațională se aduc la cunoștința fiecărui utilizator și se semnează de acesta. Fiecare utilizator este obligat să cunoască normele securității informaționale, procedurile pe care trebuie să le respecte în strictă concordanță cu politica de securitate.

**70.** Utilizatorii asigură instruirea angajaților privind metodele și procedeele de contracarare a pericolelor informaționale.

**71.** În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, sânt prevăzute şi asigurate surse de alimentare cu energie electrică de lungă durată, care sânt folosite în cazul deconectării pentru perioade îndelungate şi necesității continuării îndeplinirii de către sistemele informaționale a sarcinilor funcționale stabilite.

**VII. UNIFICAREA ȘI CERTIFICAREA ECHIPAMENTELOR**

**72.** Orice echipament, mijloc de comunicații, ansamblu sau subansamblu înainte de a fi integrat în cadrul sistemului, urmează a fi supus procedurii de verificare/testare a compatibilității cu sistemul pentru fiecare parametru tehnic.

**73.** Procedura de verificare este adaptată în funcție de de schimbările survenite în domeniul de standardizare şi de dezvoltare a echipamentelor sau schimbării tehnologiilor în cadrul sistemului.

**74.** Pentru solicitarea de integrare a echipamentului tehnic în sistem, utilizatorii sistemului sunt obligați să dețină un act confirmativ eliberat de administratorul sistemului.

**75.** Certificate pentru un anumit tip (model) de echipamente, care deja a trecut testarea sunt considerate publice şi sunt publicate pe pagina web oficială a posesorului sistemului, nefiind necesară testarea repetată a echipamentului în cauză.

**76.** Orice utilizator al sistemului TETRA, care solicită integrarea în sistem a echipamentului dar nu deține o confirmare a compatibilității, poate fi refuzat de administratorul sistemului fără expunerea motivului detaliat de refuz.

**77.** Costurile aferente procedurii de testare a echipamentelor cu scopul emiterii certificatului de omologare sunt suportate de către entitatea care a inițiat procedura.

**78.** Pentru proceduri de achiziții a echipamentului în standard TETRA, în cadrul documentației de procedură, este obligatoriu de a cere anexarea de către ofertant a certificatelor de omologare eliberate de administratorul sistemului.

**VIII. CONTROLUL ȘI RĂSPUNDEREA**

**79.** Sistemul este supus controlului intern și extern. Controlul intern privind organizarea și funcționarea sistemului se efectuează de către posesor. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea sistemului se efectuează de către instituții abilitate și certificate în domeniul auditului.

**80.** Responsabilitatea pentru organizarea funcționării sistemului aparține posesorului, administratorilor și utilizatorilor acestuia.

**81.** Toți subiecții sistemului TETRA poartă răspundere în conformitate cu cadrul normativ, pentru prelucrarea, divulgarea, transmiterea informației din Sistem persoanelor terțe.

**82.** Pentru asigurarea funcționalității eficiente și neîntrerupte a sistemului, schimbul informațional de date din cadrul sistemului este asigurat în regim non-stop.