**Išrašas**

PATVIRTINTA
VšĮ Kauno miesto greitosios medicinos pagalbos stoties direktoriaus
2021 m. gegužės 24 d. įsakymu Nr. V-90

**INFORMACINĖS SISTEMOS SAUGOS SPECIALISTO PAREIGINĖ INSTRUKCIJA NR. 23-145**

<...>

## II SKYRIUS
## KVALIFIKACINIAI REIKALAVIMAI

4. Informacinės sistemos saugos specialistas turi atitikti šiuos reikalavimus:

4.1. turėti aukštąjį informacinių technologijų išsilavinimą;

4.2. turėti ne mažesnę kaip 2 metų darbo patirtį informacijos saugumo arba kibernetinio saugumo srityje;

4.3. išmanyti darbo saugos reikalavimus ir jų laikytis;

4.4. išmanyti profesinės etikos principus;

4.5. mokėti valstybinę kalbą, sklandžiai dėstyti mintis raštu ir žodžiu;

4.6. mokėti anglų kalbą (raštu ir žodžiu) ne žemesniu kaip Europos kalbų aplanko B2 lygiu;

4.7. išmanyti ir gebėti taikyti Lietuvos Respublikos įstatymus, Lietuvos Respublikos Vyriausybės nutarimus ir kitus teisės aktus, reglamentuojančius informacinių sistemų ir registrų kūrimą, valdymą ir tvarkymą, elektroninius ryšius, elektroninės informacijos saugą ir kibernetinį saugumą;

4.8. išmanyti bendrąjį duomenų apsaugos reglamentą (toliau - BDAR) ir jo principus, turi turėti BDAR kursų baigimo pažymėjimą.

4.9. mokėti dirbti su Windows, Unix/Linux šeimos operacinėmis sistemomis, taip pat Microsoft Windows Server, Active Directory, SQL Server;

4.10. mokėti dirbti kompiuteriu Microsoft Office arba LibreOffice programiniu paketu;

4.11. mokėti administruoti ir vystyti įstaigos duomenų perdavimo tinklą (LAN, WAN, VPN);

4.12. mokėti vystyti ir eksploatuoti Kauno GMPS informacinių technologijų infostruktūrą bei IS;

4.13. turėti patirties administruojant turinio valdymo sistemas;

4.14. išmanyti informacinių ir ryšių technologijų paslaugų administravimo principus;

4.15. atlikti informacinių sistemų saugos įgaliotinio funkcijas, sugebėti savarankiškai planuoti, organizuoti ir atlikti pavestą darbą, rinktis efektyvius darbo metodus, greitai priimti sprendimus, analizuoti ir apibendrinti su vykdomomis funkcijomis susijusią informaciją bei dirbti komandoje;

4.16. turėti šias asmenines savybes: analitinį mąstymą, greitą orientaciją, būti sąžiningas, atsakingas, savarankiškas, kūrybiškas ir iniciatyvus, orientuotis į rezultatus, gebėti dirbti komandoje;

4.17. gerai išmanyti informacijos saugumo, kibernetinio saugumo ir asmens duomenų apsaugos užtikrinimo principus, išmanyti IS administravimą, gerai žinoti elektroninės informacijos saugos principus bei elektroninės informacijos saugos užtikrinimo metodus;

4.18. nenaudoti ir neplatinti nelegalios programinės įrangos ar teisėtai įsigytos programinės įrangos nenaudoti neteisėtai.

5. Informacinės sistemos saugos specialisto ligos, komandiruotės ar pan. atveju, jį pavaduoti gali šios pareiginės instrukcijos 4 punkte išdėstytus kvalifikacinius reikalavimus atitinkantis darbuotojas Kauno GMPS direktoriaus įsakymu.

6. Informacinės sistemos saugos specialistu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieneri metai.

## III SKYRIUS
## FUNKCIJOS

7. Informacinės sistemos saugos specialisto funkcijos:

7.1. teikti pasiūlymus dėl:

7.1.1. IS administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo,

7.2.2. IS saugos dokumentų priėmimo ir keitimo,

7.2.3. IS saugos reikalavimų atitikties vertinimo atlikimo;

7.2. rengti IS informacinių išteklių atitikties vertinimo ir rizikos vertinimo rezultatus ir teikti juos į Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą (ARSIS);

7.3. koordinuoti elektroninės informacijos saugos incidentų informacinėse sistemose tyrimą ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais.

7.4. teikti administratoriui ir IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

7.5. ne rečiau kaip kartą per metus, jeigu kiti teisės aktai nenustato kitaip, organizuoti IS rizikos įvertinimą;

7.6. IS rizikos įvertinimą išdėstyti rizikos įvertinimo ataskaitoje. IS rizikos įvertinimo ataskaita rengti atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos IS elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Dalyvauti rizikos įvertinimo ataskaitos parengime, jei vertinimą atlieka trečioji šalis.

7.7. periodiškai organizuoti IS naudotojų mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoti juos apie elektroninės informacijos saugos problemas (priminimai elektroniniu paštu, teminiai seminarai, atmintinės naujiems darbuotojams ir kt.);

7.8. vykdyti kitų su elektroninės informacijos sauga susijusių teisės aktų nustatytas ir IS valdytojo pavestas funkcijas;

7.9. pagal poreikį dalyvauti įstaigos administracijos organizuojamuose pasitarimuose ir susitikimuose, darbuotojų ir darbo grupės susirinkimuose;

7.10. saugoti asmens duomenis, išskyrus tuos atvejus, kai tokios informacijos pateikimą numato Lietuvos Respublikos teisės aktai;

7.11. dalintis praktine patirtimi ir įgūdžiais su kitais kompiuterinių sistemų specialistais;

7.12. vykdyti kitus Kauno GMPS direktoriaus žodinius ir (ar) raštiškus pavedimus tiesioginių pareigų kompetencijos klausimais;

7.13. nagrinėti, analizuoti ir spręsti informacijos saugumo įvykius, incidentus ir kibernetinius incidentus, administruoti elektroninių įvykių ir incidentų žurnalus;

7.14 atlikti kasmetinį informacijos klasifikavimą;

7.15 inicijuoti ir vykdyti veiklos tęstinumo planą bei atstatymo plano testavimą;

7.16 vykdyti IS administruojamų informacinių sistemų ir registrų saugos įgaliotinio funkcijas, priskirtas IS administruojamų IS ir registrų duomenų saugos nuostatuose ir kituose Lietuvos Respublikos teisės aktuose;

7.17 koordinuoti ir kontroliuoti Lietuvos Respublikos teisės aktų, reglamentuojančių kibernetinį saugumą, reikalavimų įgyvendinimą ir laikymąsi IS;

7.18 atlikti IS, informacijos saugumo, kibernetinio saugumo ir asmens duomenų apsaugos organizacinių ir techninių priemonių veiksmingumo matavimus;

7.19 pagal kompetenciją įgyvendinti Bendrojo duomenų apsaugos reglamento (ES) 2016/679 reikalavimus;

7.20 koordinuoti ir kontroliuoti Lietuvos Respublikos teisės aktų, reglamentuojančių kibernetinį saugumą, reikalavimų įgyvendinimą ir laikymąsi IS;

7.21. vykdyti kibernetinio saugumo specialisto funkcijas:

7.21.1. vykdyti nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas“ (toliau – Pratybos) koordinatoriaus funkcijas ir dalyvauti Pratybų procedūrinėje dalyje;

7.21.2. rengti ir su Nacionaliniu kibernetinio saugumo centru (toliau – NKSC) derinti kibernetinio saugumo politiką ir jos įgyvendinimą IS reglamentuojančius vidaus teisės aktus;

7.21.3. koordinuoti ir kontroliuoti organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimą IS;

7.21.4. NKSC ir kitoms atsakingoms institucijoms pranešti apie IS kibernetinius incidentus;

7.21.5. bendradarbiauti su kompiuterinių sistemų specialistais, organizuoti kibernetinių incidentų imitavimo pratybas ir atsižvelgdamas į jų rezultatus tobulina veiklos tęstinumo planus;

7.21.6. bendradarbiauti su kompiuterinių sistemų specialistais, organizuoti grėsmių ir pažeidžiamumų, galinčių turėti įtakos KGMPS administruojamų IS ir registrų kibernetiniam saugumui, vertinimą;

7.21.7. bendradarbiauti Lietuvos Respublikoje už kibernetinio saugumo politikos formavimą ir įgyvendinimą atsakingomis institucijomis: Lietuvos Respublikos Vyriausybe, Lietuvos Respublikos krašto apsaugos ministerija, Lietuvos Respublikos vidaus reikalų ministerija, Lietuvos Respublikos ryšių reguliavimo tarnyba, NKSC, Valstybine duomenų apsaugos inspekcija ir Policijos departamentu prie Lietuvos Respublikos vidaus reikalų ministerijos;

8. Informacinės sistemos saugos specialistas negali vykdyti IS administratoriaus funkcijų.

<...>