PATVIRTINTA
Direktoriaus 2020 m. birželio 5 d.
Įsakymu Nr.V-95

# VŠĮ ANYKŠČIŲ RAJONO SAVIVALDYBĖS LIGONINĖS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

## I. BENDROSIOS NUOSTATOS

1. VšĮ Anykščių rajono savivaldybės ligoninės (toliau – Ligoninės) saugaus elektroninės informacijos tvarkymo taisyklėse (toliau – Taisyklės) nustatyta tvarka, pagal kurią turi būti saugiai tvarkoma Ligoninės informacinėje sistemoje (toliau – IS) esanti elektroninė informacija.

2. Taisyklės yra privalomos visiems Ligoninės darbuotojams (toliau – informacinės sistemos naudotojams), pareigybių aprašymuose, pareiginėse instrukcijose nustatytoms tiesioginėms funkcijoms vykdyti naudojantiems kompiuterių įrangą. Taisyklėse apibrėžiama IS naudojamos elektroninės informacijos sauga tvarkant duomenis.

3. Taisyklės parengtos vadovaujantis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemos reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin.,1997, Nr. 83-2075; 2003, Nr. 2-45, 2007, Nr.49-1891), Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070) taip pat kitais teisės aktais, reglamentuojančiais duomenų tvarkymo teisėtumą, duomenų tvarkytojų veiklą ir duomenų saugos valdymą.

4. Elektroninės informacijos savybės: konfidencialumas – tai, kad su informacinėje sistemoje tvarkoma elektronine informacija gali susipažinti tik tam įgalioti asmenys; vientisumas – tai, kad elektroninė informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta; prieinamumas – tai, kad elektroninė informacija gali būti tvarkoma reikiamu metu.

5. IS esanti elektroninė informacija skirstoma į kategorijas:

5.1. **Viešai neskelbtina ir neteiktina informacija** – tai neviešo pobūdžio informacija (privati informacija ir kt.), kurios skelbimas ar viešas teikimas ribojamas teisės aktų nustatyta tvarka. Viešai neskelbtiną ir neteiktiną informaciją, išskyrus įstatymų nustatytus atvejus, sudaro:

5.1.1. Ligoninės darbuotojų asmens duomenys, tvarkomi automatiniu būdu (kompiuterinėje duomenų bazėje ir kt.), neautomatiniu būdu – asmens bylose, sąrašuose, sąvaduose, kartotekose, asmens kortelėse, kituose dokumentuose;

5.1.2. informacija, susijusi su Ligoninės darbuotojų tarnybinės veiklos vertinimu;

5.1.3. Ligoninės pretendentų į Ligoninės darbuotojus asmens duomenys ir kita informacija, susijusi su priėmimu į tarnybą;

5.1.4. informacija, susijusi su viešojo pirkimo procedūromis (viešojo pirkimo procedūrose dalyvavusių tiekėjų kvalifikaciniai duomenys, pasiūlymo turinys, informacija, susijusi su tiekėjų pateiktų pasiūlymų vertinimu, nagrinėjimu, aiškinimu ir kt.), kai jos atskleidimas prieštarautų Viešųjų pirkimų įstatymo reikalavimams, visuomenės interesams, pažeistų teisėtus viešuosiuose pirkimuose dalyvaujančių asmenų interesus;

5.1.5. finansų ir apskaitos duomenys;

5.1.6. informacinių sistemų informacija: duomenų perdavimo adresai ir su jų valdymu susijusi informacija, tarnybinių stočių ir tinklinės įrangos konfigūracinės laikmenos (angl. *log files*), vartotojų identifikatoriai, informacinių sistemų aprašymai ir schemos, projektinė dokumentacija, taikomųjų programų, licencijuotos programinės įrangos, operacinių sistemų pirminiai kodai (angl. *source*), kompiuterių tinklų valdymo ir duomenų saugos programinės priemonės, sistemoje naudojamos taikomosios programinės įrangos dokumentacija, skirta vartotojui;

5.1.7. Centralizuoto vidaus audito skyriaus darbo dokumentai, ataskaitos, išvados ir rekomendacijos;

5.1.8. kita informacija, kuri pagal Lietuvos Respublikos įstatymus, kitus teisės aktus nėra vieša informacija (privati informacija, techninė, technologinė, organizacinė, komercinė, profesinė paslaptis ir kt.).

5.2. **Viešoji informacija** – visa informacija, išskyrus viešai neskelbtiną ir neteiktiną informaciją.

5.3. Ligoninės darbuotojai su viešai neskelbtina ir neteiktina informacija gali susipažinti ir naudotis tarnyboje jų pareigybių aprašymuose, pareiginėse instrukcijose nurodytoms funkcijoms atlikti. Susipažinti su asmens duomenimis, tvarkomais asmens bylose, kita viešai neskelbtina ir neteiktina informacija, nurodyta taisyklių 5.1 punkte, galima gavus Ligoninės ar struktūrinio padalinio vadovo, kurio kompetencijai priklauso tvarkoma informacija, leidimą arba įstatymų ir kitų norminių teisės aktų nustatyta tvarka.

## II. TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

6. Kiekvienas kompiuteris turi įjungimo slaptažodį, kiekvienas naudotojas IS unikaliai atpažįstamas – patvirtina savo tapatybę.

7. Informacinės sistemos slaptažodžių valdymo sistema užtikrina saugų individualių slaptažodžių naudojimą.

8. Slaptažodis turi būti sudarytas iš ne mažiau kaip 8 simbolių, būtinai panaudojant bent vieną skaitmenį, mažąją ir didžiąją raides. Slaptažodis keičiamas kas 120 dienų.

9. Slaptažodžiai negali būti atskleidžiami kitiems asmenims.

10. Baigus darbą imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos.

11. Informacinės sistemos kompiuteriais galima naudotis tik Ligoninės patalpose. Naudotojams, kuriems būtina, suteikiama teisė kompiuterius naudoti tiesioginėms pareigoms atlikti ne Ligoninės patalpose. Informacinės sistemos kompiuterius ne Ligoninės patalpose turi teisę naudoti tik saugos įgaliotinio, paskirto Ligoninės vadovo įsakymu, autorizuoti naudotojai. Prašymą, patvirtintą tiesioginio vadovo, naudotojas privalo pateikti saugos įgaliotiniui. Naudotojų, kuriems suteikta teisė naudoti kompiuterius ne patalpose, sąrašas saugomas saugos įgaliotinio. Sąrašas peržiūrimas ir koreguojamas ne rečiau kaip kartą per metus.

12. Naudotojų kompiuterių apsaugai naudojama programinė įranga, efektyviai apsauganti nuo žalingos programinės įrangos (įskaitant antivirusines programas, tačiau jomis neapsiribojama). Antivirusinės programos žalingo kodo aprašai periodiškai atnaujinami. Naudotojui apribota galimybė savavališkai konfigūruoti antivirusinės sistemos nustatymus.

13. Informacinės sistemos elektroninio pašto apsaugai naudojama programinė įranga, apsauganti nuo žalingos programinės įrangos. Žalingo kodo aprašai atnaujinami ne rečiau kaip kartą per dieną.

14. Naudotojams kompiuterių operacinėse sistemose suteikiamos minimalios, tiesioginėms pareigoms vykdyti būtinos teisės.

15. Informacinėje sistemoje naudojama tik legali ir autorizuota programinė įranga.

16. Taikomoji programinė įranga įdiegiama ir konfigūruojama laikantis gamintojo saugos rekomendacijų.

17. Planuojant, įgyvendinant ir konfigūruojant duomenų perdavimo tinklus suteikiama minimali būtina prieiga prie tinklo išteklių ir užtikrinamas minimalus būtinas tinklo funkcionalumas.

18. Informacinės sistemos elektroninės informacijos perdavimo tinklas atskiriamas nuo viešųjų telekomunikacijų tinklų naudojant ugniasienę.

19. Už tinklo ugniasienių administravimą, priežiūrą, operacinės sistemos atnaujinimą ir saugią ugniasienių konfigūraciją atsakingas IS administratorius.

20. Saugos užtikrinimo priemonės Ligoninės bendrosioms patalpoms:

21.1. Patalpos rakinamos (darbuotojai privalo kiekvieną kartą patalpą užrakinti, kai ją palieka be priežiūros).

22. Saugos užtikrinimo priemonės patalpai, kurioje yra tarnybinės stotys ir komutaciniai mazgai:

22.1. Patalpa atskirta nuo bendro naudojimo patalpų, durys rakinamos.

22.2. Patalpos atitinka priešgaisrinės saugos reikalavimus, yra gaisro gesinimo priemonės, vykdoma gaisro gesinimo priemonių patikra.

22.3. Techninė įranga saugoma nuo elektros srovės svyravimų nepertraukiamo maitinimo šaltiniais (UPS). Rezervinis maitinimo šaltinis užtikrina informacinės sistemos pagrindinės kompiuterinės įrangos veikimą ne trumpiau nei 10 min.

23. IS techninės, sisteminės ir taikomosios programinės saugos užtikrinimo priemonės:

23.1. IS posistemes administruoja Ligoninės direktoriaus įsakymu paskirtas posistemių administratorius - Informacinių technologijų skyriaus darbuotojas.

23.2. Kontroliuojamas išorinis prisijungimas prie vidinio duomenų perdavimo tinklo.

23.3. Valdoma informacinės sistemos naudotojų teisė naudotis programine įranga.

23.4. Naudojama sertifikuota ir legali programinė įranga.

23.5. Reguliariai daromos duomenų bazių ir kitos svarbios informacijos kopijos.

23.6. Atsarginės duomenų ir programinės įrangos kopijos saugomos tam skirto kompiuterio, esančio kitoje patalpoje, diske.

23.7. Įranga prižiūrima pagal gamintojo rekomendacijas.

23.8. Gedimus šalina kvalifikuoti specialistai.

23.9. Svarbiausios kompiuterinės įrangos techninė būklė nuolat stebima.

23.10. Informacinės sistemos naudotojai mokomi dirbti su programine įranga.

23.11. Darbo vietos atitinka Lietuvos higienos normą HN 32:2004 „Darbas su videoterminalais. Saugos ir sveikatos reikalavimą“, patvirtintą Lietuvos Respublikos sveikatos apsaugos ministro 2004 m. vasario 12 d. įsakymu Nr. V-65 (Žin., 2004, 32-1027), kituose Lietuvos Respublikos teisės aktuose nustatytus reikalavimus.

23.12. IS naudotojai, pasirašę konfidencialumo pasižadėjimą, užregistruojami IS, suteikiant jiems vartotojų vardus, slaptažodžius ir prieigos teises pagal jų pareigybių aprašymuose, pareiginėse instrukcijose nustatytas funkcijas.

23.13. Pasikeitus darbuotojo statusui (atleidžiamas, perkeliamas, atostogauja, vykdomas informacinės sistemos naudotojo veiklos tyrimas, nebeatlieka turėtų funkcijų ir pan.), vykdomos Ligoninės informacinės sistemos naudotojų administravimo taisyklėse numatytos darbo apskaitos priemonės.

24. Elektros ir duomenų kabeliai apsaugoti nuo neteisėto prie jų prisijungimo ir jų pažeidimo.

25. Parengtas ir nuolat atnaujinamas išsamus veiklos atkūrimo planas.

## III. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

26. Duomenų keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

26.1. IS posistemių elektroninius duomenis įveda, keičia, atnaujina ir naikina IS informacinės sistemos naudotojai pagal prieigos prie IS teisių, rolių, sertifikatų lygmenį, nustatytą pareigybių aprašymuose, pareiginėse instrukcijose reikalingoms funkcijoms atlikti.

26.2. Už elektroninės informacijos turinį atsako duomenis įvedęs IS naudotojas.

26.3. IS posistemių elektroniniuose žurnaluose turi būti registruojamas informacinės sistemos naudotojų darbo laikas, prisijungimo vardas ir atliekami veiksmai. Ši informacija turi būti prieinama tik IS administratoriui ir saugos įgaliotiniui, kad būtų galima nustatyti duomenų vientisumo pažeidimus.

27. Duomenų kopijų darymo tvarka:

27.1. IS atsarginių duomenų kopijos daromos kiekvieną pirmadienį ir keliamos į UAB „Edrana Baltic“ FTP serverį.

27.2. Pakartotinės IS atsarginių duomenų kopijos daromos prieš ir po posistemių programinio atnaujinimo ar įvedus didelį kiekį naujos elektroninės informacijos.

27.3. Atsarginės duomenų kopijos įrašomos ir saugomos tam skirto kompiuterio kietajame diske.

27.4. Naudotojui svarbių duomenų, nesaugomų duomenų bazėse, atsarginės duomenų kopijos daromos programinėmis priemonėmis numatytu laiku ir naudotojui savo nuožiūra pasirinkus pakartotinį kopijų darymą, saugomos tam skirto kompiuterio kietajame diske.

27.5. Saugomos 5 paskutinių dienų atsarginių duomenų kopijos.

27.6. Prarasti ar sunaikinti duomenys yra atkuriami iš atsarginių duomenų kopijų per 48 valandas.

27.7. IS naudotojas yra atsakingas už savo kompiuteryje saugomų duomenų išsaugojimą.

27.8. IS administratorius yra atsakingas už atsarginių duomenų kopijų darymą, duomenų atkūrimą ir atsarginių duomenų kopijų apsaugą.

27.9. Duomenų saugos įgaliotinis atsakingas už atsarginių duomenų saugojimo kontrolę.

28. Duomenų perkėlimo, teikimo kitoms informacinėms sistemoms ir gavimo tvarka:

28.1. IS duomenys kitai informacijos tvarkymo sistemai turi būti perduodami vadovaujantis Širvintų rajono savivaldybės administracijos informacinės sistemos nuostatais, IS duomenų saugos nuostatais, IS saugumo politiką įgyvendinančiais dokumentais, kitais duomenų saugą užtikrinančiais ir reglamentuojančiais teisės aktais.

28.2. Duomenų teikėjai duomenis į IS turi teikti teisės aktų numatytais būdais, apimtimi, reguliarumu ir terminais.

29. Neteisėto duomenų kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) nustatymo tvarka:

29.1. IS informacinės sistemos naudotojas, kilus įtarimui, kad su duomenimis yra vykdoma neteisėta veikla, privalo nedelsdamas apie tai informuoti IS administratorių. IS administratorius nedelsdamas turi imtis visų įmanomų veiksmų, reikalingų neteisėtai veiklai su duomenimis užkirsti.

29.2. IS administratorius privalo naudoti visas turimas ir įmanomas technines, programines ir administracines priemones, skirtas duomenims nuo neteisėtos veiklos apsaugoti.

30. Programinės įrangos diegimo ar atnaujinimo, IS kompiuterių techninės įrangos keitimo ar perkėlimo (toliau – pakeitimai) tvarka:

30.1. IS pakeitimai gali būti atliekami tik IS valdytojui raštiškai pritarus.

30.2. Turi būti laikomasi oficialių įforminimo, testavimo, įgyvendinimo procedūrų atliekant svarbius pokyčius esamoje sistemoje ar diegiant naujus.

30.3. Prieš atliekant IS pakeitimus, kurių metu gali iškilti grėsmė duomenų konfidencialumui, vientisumui ar pasiekiamumui, IS administratorius turi ištestuoti atliekamus pakeitimus esant techninei galimybei.

30.4. Atlikus vykdomų IS pakeitimų testavimą arba jei testavimo darbų dėl programinių ir/ar techninių priežasčių nebuvo galima atlikti, IS administratorius gali pradėti įgyvendinti IS pakeitimus.

30.5. Įgyvendinant IS pakeitimus, kurių metu galimi IS veikimo sutrikimai, IS administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki planuojamų IS pakeitimų vykdymo pradžios informuoti IS naudotojus apie tokių darbų pradžią ir galimus IS veiklos sutrikimus.

30.6. IS administratorius naudotojams privalo pateikti visą reikalingą informaciją apie naudojimosi IS pakitimus, kurių atsiradimas susijęs su įvykdytais arba vykdomais IS pakeitimais.

## IV. REIKALAVIMAI, KELIAMI IS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS

31. IS administratorius atsako už programinių, techninių ir kitų prieigos prie IS resursų organizavimą, suteikimą ir panaikinimą IS techninės ir/ar programinės priežiūros paslaugos (toliau – IS priežiūros paslauga) teikėjui.

32. IS administratorius suteikia IS priežiūros paslaugos teikėjui tik tokią prieigą prie IS resursų, kuri yra būtina norint atlikti arba vykdyti sutartyje numatytus įsipareigojimus.

33. IS administratorius privalo supažindinti IS priežiūros paslaugų teikėją su suteiktos prieigos prie IS saugos reikalavimais ir sąlygomis.

34. Pasibaigus sutarties su IS priežiūros paslaugos teikėju galiojimo terminui ar atsiradus kitoms sutartyje ar IS saugos politiką įgyvendinančiuose dokumentuose įvardytoms sąlygoms, IS administratorius privalo nedelsdamas organizuoti suteiktos prieigos panaikinimą.

## V. BAIGIAMOSIOS NUOSTATOS

35. Asmenys, pažeidę Taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.

_____