PATVIRTINTA
Viešosios įstaigos Joniškio
ligoninės direktoriaus
2023 m. birželio 19 d. įsakymu Nr. V-75

VIEŠOSIOS ĮSTAIGOS JONIŠKIO LIGONINĖS SAUGAUS ELEKTRONINĖS IR ASMENINĖS / JAUTRIOS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Viešosios įstaigos Joniškio ligoninės ***saugaus elektroninės ir asmeninės / jautrios informacijos tvarkymo taisyklių*** (toliau – Taisyklės) **tikslas – nustatyti tvarką, užtikrinančią** saugų Joniškio ligoninės informacinių sistemų (toliau – IS) techninės, programinės įrangos funkcionavimą**, saugų duomenų tvarkymą** ir jų teikimą kitoms institucijoms, bei asmenims pagal teisės aktų nustatytus reikalavimus.

2. Taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“.

3. Šios **Taisyklės yra privalomos visiems Joniškio ligoninės darbuotojams**, dirbantiems pagal darbo sutartis, arba paslaugų teikimo sutartį, naudojantiems kompiuterinę įrangą darbo užduotims atlikti.

4. Taisyklėse vartojamos sąvokos:

4.1. **Joniškio ligoninės informacinės sistemos** (toliau – IS arba Informacinės sistemos) – informacinių technologijų pagrindu veikiančios sistemos, užtikrinančios kompiuterizuotą Joniškio ligoninės duomenų, dokumentų ir kitos informacijos kūrimą, tvarkymą ir saugojimą, tenkinančios kitus Joniškio ligoninės informacinius poreikius. Informacines sistemas sudaro techninė įranga (tarnybinės stotys, darbo vietų kompiuteriai, duomenų saugyklos, kompiuterių tinklo ir elektroninio ryšio priemonės, duomenų apsaugos priemonės), programinė įranga (operacinės sistemos, pagalbinės programos, taikomosios programinės įrangos), kompiuterizuotai tvarkoma Joniškio ligoninės veiklos informacija (elektroniniai dokumentai, įvairūs duomenys, duomenų bazės) ir kita informacija;

4.2**. Saugos įgaliotinis** – Joniškio ligoninės direktoriaus paskirtas darbuotojas, dirbantis pagal darbo sutartį, arba paslaugų teikimo sutartį, įgyvendinantis elektroninės informacijos saugą Joniškio ligoninės Informacinėse sistemose;

4.3. **Informacinių sistemų administratorius** (toliau – Administratorius) – Joniškio ligoninės darbuotojas, dirbantis pagal darbo sutartį, arba paslaugų teikimo sutartį, atliekantis Informacinių sistemų priežiūrą;

4.4. **Informacinių sistemų naudotojas** (toliau – Naudotojas) –darbuotojas, dirbantis pagal darbo sutartį, arba paslaugų teikimo sutartį, turintis teisę naudotis Informacinių sistemų ištekliais numatytoms funkcijoms atlikti;

4.5. kitos Taisyklėse vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimus, Saugos dokumentų turinio gaires ir Elektroninės informacijos, sudarančios

valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gaires, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 (Žin., 2013, Nr. 86-4310) ir kituose Lietuvos Respublikos teisės aktuose vartojamas sąvokas.

5. Už IS duomenų saugų tvarkymą atsakingi **Naudotojai, Administratorius**.

6. Už Taisyklių įgyvendinimo organizavimą ir kontrolę atsakingas **Saugos įgaliotinis**.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

7. Saugiam elektroninės informacijos tvarkymui užtikrinti naudojamos kompiuterinės įrangos, programinės įrangos, fizinės, techninės ir organizacinės duomenų saugos priemonės.

8. Prieiga prie Informacinės sistemos suteikiama tik **autorizuotiems Naudotojams**. Kiekvienas Naudotojas Informacinėje sistemoje turi patvirtinti savo tapatybę vardu ir slaptažodžiu. Slaptažodis turi būti sudarytas iš ne mažiau kaip 8 simbolių, būtinai panaudojant bent vieną skaitmenį, mažąją ir didžiąją raides. Slaptažodžiai negali būti atskleidžiami kitiems asmenims.

9. Prieiga Naudotojams suteikiama tik prie tų išteklių, kurie yra būtini tiesioginėms pareigoms vykdyti.

10. Prieigos prie tarnybinių stočių (serverių) kontrolė užtikrinama, suteikiant prieigos prie tarnybinių stočių teises tik Administratoriui. Asmenys, nesusiję su Informacinės sistemos administravimu, patekti į šias patalpas gali tik lydimi Administratoriaus arba jį pavaduojančio darbuotojo.

11. Naudojama legali sisteminė ir taikomoji programinė įranga.

12. Programinės įrangos diegimą atlieka tik **Administratoriai** ar kiti įgalioti asmenys.

13. Naudojamos antivirusinės programos Naudotojų kompiuteriuose, antivirusinės programos elektroninio pašto tarnybinėje stotyje, programinės ugniasienės Naudotojų kompiuteriuose ir tinklo tarnybinėse stotyse apsaugai nuo virusų, šnipinėjimui skirtos programinės įrangos, nepageidaujamo elektroninio pašto ir pan.

14. Siekiant apsaugoti nuo žalingos programinės įrangos, reguliariai turi būti atliekamas nuolatinis Naudotojų ir tarnybinių stočių operacinių sistemų atnaujinimas.

15. Antivirusinių programų duomenų bazės turi būti atnaujinamos periodiškai – ne rečiau kaip kartą per dieną, jei atnaujinimą pateikia antivirusinės programos gamintojas.

16. Nuolat stebima Informacinės sistemos serverių, duomenų perdavimo tinklo mazgų ir ryšio linijų techninė būklė.

17. Tarnybinių stočių kompiuterinės įrangos dubliavimas ir šios kompiuterinės įrangos techninės būklės nuolatinė stebėsena.

18. Tarnybinės stotys, naudotojų kompiuterinė įranga ir duomenų perdavimo tinklo mazgai eksploatuojami griežtai laikantis gamintojo rekomendacijų.

19. Saugiam elektroninės informacijos teikimui ir (ar) gavimui iš kitų valstybės institucijų užtikrinti naudojamas Saugus valstybės duomenų perdavimo tinklas.

20. Duomenys nuo jų praradimo, iškraipymo, sunaikinimo, neteisėto panaudojimo galimybių apsaugomi techninėmis, organizacinėmis, programinėmis priemonėmis.

21. Techninė įranga apsaugoma nuo elektros srovės svyravimų, nuo neteisėtos prieigos prie techninės įrangos, jos sugadinimo ar neteisėto poveikio jai. Naudojami specialūs maitinimo šaltiniai, nenutrūkstamo maitinimo šaltinis su automatine apsauga nuo įtampos svyravimų.

22. Patalpa, kurioje veikia tarnybinės stotys, atitinka priešgaisrinės saugos reikalavimus, joje yra gaisro gesinimo priemonės. Periodiškai atliekama gaisro gesinimo priemonių patikra. Įrengta oro kondicionavimo sistema.

23. Kiekvienas Informacinės sistemos Naudotojas unikaliai identifikuojamas – patvirtina savo tapatybę Informacinės sistemos Naudotojo vardu ir slaptažodžiu. **Baigus darbą, Informacinės sistemos Naudotojas turi užtikrinti, kad jautri informacija būtų apsaugota slaptažodžiu.**

III SKYRIUS
SAUGUS ELEKTRONINĖS IR ASMENINĖS/JAUTRIOS INFORMACIJOS TVARKYMAS

24. Informacinių sistemų **duomenų keitimą, atnaujinimą ir naujų duomenų įvedimą turi teisę atlikti tik autorizuoti Naudotojai, turintys teisę tai atlikti**.

25. Informacinių sistemų elektroninės informacijos pakeitimai registruojami IS veiksmų žurnale, nurodant IS Naudotojo vardą, pavardę, duomenų keitimo laiką, duomenų tvarkymo veiksmus.

26. Už Informacinių sistemų duomenų atsarginių duomenų kopijų darymą, saugojimą ir duomenų atkūrimą iš atsarginių duomenų kopijų atsako Administratorius.

27. Atsarginės duomenų kopijos daromos periodiškai, bet ne rečiau kaip kartą per mėnesį, o kopijos tarnybinėse stotyse – automatiniu būdu į išorinius informacijos kaupiklius kiekvieną dieną.

28. Informacinių sistemų duomenų bazės yra kopijuojamos ir saugomos taip, kad įvykus nenumatytai situacijai Informacinių sistemų veikla būtų visiškai atkurta per 48 valandas.

29. Informacinės sistemos duomenų atkūrimo bandymai atliekami vieną kartą per metus, ne darbo valandomis ir prieš tai informavus visus Informacinės sistemos Naudotojus.

30. **Naudotojas yra atsakingas už savo kompiuteryje saugomų duomenų atsarginių kopijų saugojimą.**

31. **Naudotojas yra atsakingas už rizikas, kurios gali kilti iš jo naudojamų asmeninio pašto žinučių ar socialinių tinklų tikrinimą darbiniame kompiuteryje.**

32. **Naudotojas yra atsakingas ir už atspausdintos ar ranka užpildytos informacijos saugojimą ir duomenų neatskleidimą popieriniuose dokumentuose.**

33. Duomenų mainai tarp IS ir kitų susijusių valstybės ar žinybinių registrų ir valstybės informacinių sistemų vykdomi su šių susijusių valstybės ar žinybinių registrų ir valstybės informacinių sistemų valdytojais sudarytose duomenų teikimo sutartyse numatytais būdais, terminais ir numatytos apimties.

34. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarką, priklausomai nuo konkretaus atvejo, derina Administratorius.

35. Operacinių sistemų ir taikomosios programinės įrangos keitimai turi būti valdomi: planuojami ir ištestuojami, numatomos atstatomosios procedūros nesėkmingų keitimų atvejams, įvertinamas keitimų poveikis saugumui.

36. Administratorius, užtikrindamas Informacinės sistemos duomenų vientisumą, privalo naudoti visas įmanomas fizines, programines ir organizacines priemones, skirtas Informacinei sistemai ir joje tvarkomiems duomenims apsaugoti nuo neteisėtų veiksmų.

37. **Naudotojas, įtaręs, kad su IS duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai Administratoriui**. Administratorius, įtaręs, kad su IS duomenimis vykdomi neteisėti veiksmai, privalo apie tai pranešti Saugos įgaliotiniui. Saugos įgaliotinis, gavęs pranešimą apie vykdomus neteisėtus veiksmus su IS arba su IS tvarkomais duomenimis, inicijuoja elektroninės informacijos saugos incidento valdymo procedūras.

38. Stacionarūs, nešiojamieji kompiuteriai ir mobilieji įrenginiai turi būti apsaugoti saugiais slaptažodžiais, sudėtingumu atitinkančiais Naudotojų administravimo taisyklių reikalavimus, saugomi ir negali būti palikti be priežiūros.

39. Už mobiliųjų įrenginių ir jame tvarkomų ar saugomų duomenų saugą teisės aktų nustatyta tvarka **atsako Naudotojas**, kuriam šis įrenginys yra skirtas.

40. Darbuotojui nesant darbo vietoje, jis turi užtikrinti jo darbo vietoje disponuojamos informacijos saugumu, nepaliekant dokumentų ant stalo, atrakinto kompiuterio ar neužrakinto kabineto.

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINIŲ SISTEMŲ PASLAUGŲ TEIKĖJAMS

41. Administratorius suteikia prieigos prie Informacinių sistemų duomenų teisę (peržiūrėti duomenis, atlikti užklausas, vykdyti veiksmus su duomenimis ir kt.) bei fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nurodytam laikotarpiui jam nustatytoms funkcijoms atlikti.

42. Administratorius suteikia priežiūros paslaugų teikėjams tik tokias prieigos prie Informacinės sistemos programinių, techninių ir kitų išteklių teises, kokios yra būtinos norint teikti priežiūros paslaugas.

43. Reikalavimai priežiūros paslaugų teikėjams ir jų teikiamoms priežiūros paslaugoms nustatomi šių paslaugų teikimo sutartyse. Paslaugų teikimo sutartyse turi būti nurodoma, kad paslaugų teikėjai, kurdami ar modifikuodami Informacinės sistemos ar jos posistemių taikomąją programinę įrangą turi naudoti informacijos saugumo nuo nesankcionuoto poveikio sisteminei, taikomajai programinei įrangai ir patalpoms priemones. Naudoti tik sertifikuotą sisteminę programinę įrangą.

44. Perkant paslaugas ar įrangą, pirkimo sutartyje turi būti iš anksto nustatyta, kad paslaugų teikėjas ar įrangos tiekėjas užtikrina atitiktį kibernetinio saugumo reikalavimams, nustatytiems Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše.

45. Pasibaigus sutartyje nurodytam laikotarpiui, Administratorius panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie Informacinių sistemų duomenų teisę ir apie tai jį informuoja.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

46. Šios Taisyklės yra privalomos visiems darbuotojams, naudojantiems kompiuterinę įrangą darbo užduotims atlikti.

47. Naudotojai, pažeidę šių Taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____