

PATVIRTINTA

VšĮ K. Griniaus slaugos ir palaikomojo
gydymo ligoninės direktoriaus
2024 m. vasario 1 d. įsakymu Nr. BP-13

**VŠĮ K. GRINIAUS SLAUGOS IR PALAIKOMOJO GYDYMO LIGONINĖS
INFORMACINIŲ IR KOMUNIKACINIŲ TECHNOLOGIJŲ NAUDOJIMO BEI
DARBUOTOJŲ STEBĖSENOS IR KONTROLĖS DARBO VIETOJE TVARKA,**

priimta pagal 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679
dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo duomenų judėjimo nuostatas

1. Tvarkos tikslas – užtikrinti viešosios įstaigos K. Griniaus slaugos ir palaikomojo gydymo ligoninės, juridinio asmens kodas 135134113, buveinės adresas Kruonio g. 21, LT-45370 Kaunas (toliau – „Ligoninė“), darbuotojo privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis (toliau – „Tvarka“).

2. Ligoninė, atsižvelgiant į darbuotojo einamas pareigas, savo nuožiūra darbuotojams suteikia darbo priemones. Ligoninei priklausančios informacinės ir komunikacinės technologijos, t. y. kompiuteriai, telefonai, prieiga prie interneto, elektroninis paštas, spausdintuvai, duomenų laikmenos ir kiti prietaisai, – yra skirtos išimtinai darbuotojų darbo funkcijoms vykdyti, jeigu Ligoninė su darbuotoju nesusitaria kitaip.

3. Visuose kompiuteriuose, kurie jungiami į kompiuterinį tinklą, turi nuolat veikti antivirusinė programa su naujausia virusų aprašymų duomenų baze.

4. Darbuotojas, palikdamas savo darbo vietą ilgesniam nei 30 minučių laikui, privalo išjungti visas programas, duomenų bazes. Galima palikti tik operacinės sistemos darbalaukį.

5. Darbuotojai naudoja Ligoninės informacines ir komunikacines technologijas Ligoninės ir darbuotojų sudarytų darbo sutarčių pagrindu, laikydamiesi šios Tvarkos, teisės aktų reikalavimų, licencinių ar kitų sutarčių nuostatų, kitų norminių ir Ligoninės lokaliųjų teisės aktų.

6. Darbuotojai turi teisę informacines ir komunikacines technologijas naudoti tik savo darbo funkcijoms Ligoninėje vykdyti. Retas ir trumpas Ligoninės informacinių ir komunikacinių technologijų naudojimas asmeniniais tikslais (išskyrus Ligoninės suteikto el. pašto, kitų elektroninės komunikacijų priemonių naudojimą) galimas tik tuo atveju, jeigu tai yra atliekama darbuotojų poilsio laiku (laisvu nuo darbo laiku), neigiamai neįtakoja darbuotojo darbo našumo ar darbuotojo vykdomų darbo funkcijų ir nepažeidžia šios Tvarkos, teisės aktų reikalavimų ar trečiųjų asmenų teisių ir/ar teisėtų interesų.

7. Ligoninės informacinių ir komunikacinių technologijų naudojimas bet kokių ne Ligoninės teikiamų paslaugų siūlymui ar teikimui, taip pat bet kokių veiksmų, kurie gali pažeisti teisės aktų reikalavimus ir (ar) bet kokių trečiųjų asmenų teises ar teisėtus interesus, atlikimui, visais atvejais yra draudžiamas.

8. Ligoninės techninės ir programinės įrangos konfigūracijas nustato, konfigūruoja, prižiūri ir taiso išskirtinai tik Ligoninės direktorius (arba IT specialistas, arba Ligoninės paslaugų teikimo sutarties pagrindu šias paslaugas teikiantis paslaugos teikėjas) (toliau už IT paslaugas atsakingas darbuotojas). Taip pat programinę įrangą, programas įdiegia, ištrina bet kurio iš Ligoninės darbuotojų kompiuteryje tik už IT paslaugas atsakingas darbuotojas, dėl kurių įdiegimo būtinumo, galimybių ir kitų aspektų sprendžia už IT paslaugas atsakingas darbuotojas, jei kyla neaiškumų, už IT paslaugas atsakingas darbuotojas sprendimą priima pasitaręs su Ligoninės direktoriumi.

9. Prieigas prie informacinių sistemų sukuria Ligoninės IT specialistas direktoriaus pavedimu.

10. Visais atvejais, kai siunčiamame laiške yra ar gali būti asmens duomenų, ar konfidencialios informacijos (išskyrus, kai el. laiškas siunčiamas Ligoninės darbuotojų el. pašto adresais, darbuotojai privalo siųsti 7zip šifravimo programa užšifruotus el. laiškus. Išsiuntus šifruotą el. laišką, nedelsiant kitu laišku informuojama apie pirmiau atsiųstą el. laišką ir jo atidarymo slaptažodį. Rekomenduotinas naudoti antrojo laiško tekstas: „Prieš tai Ligoninė Jums išsiuntė laišką, kuris, siekiant apsaugoti Jūsų ir/ar trečiųjų asmenų asmens duomenų konfidencialumą, užtikrinti tinkamą asmens duomenų apsaugą reglamentuojančių teisės aktų įgyvendinimą, yra užšifruotas. Šiuo laišku siunčiame ankstesniame laiške pateiktos informacijos atidarymo slaptažodį: [*nurodomas slaptažodis*]. Informuokite, prašau, jei nepavyksta perskaityti, atsidaryti prieš tai atsiųsto laiško, jo priedų ir/ar nerandate minėto laiško ar jame esančių priedų. Kitu atveju laikysime, kad prieš tai siųstą laišką ir jo priedus gavote ir Jums sėkmingai pavyko susipažinti su atsiųsta informacija.“. Ligoninė gali nuspręsti naudoti kitokį rekomenduotiną antrojo laiško tekstą, apie jį Ligoninės darbuotojai bus informuojami el. laišku.

11. Ligoninės darbuotojai visus duomenis susijusius su pacientais turi suvesti į paciento ligos istoriją atitinkamoje sistemoje (ir/ar popierinę paciento ligos istorijos kortelę), e.sveikata.lt sistemoje.

12. Administracijos darbuotojai su darbo funkcijų vykdymu susijusius dokumentus privalo saugoti Ligoninės saugykloje. Tuo tarpu nei asmeninio pobūdžio nei bet kokie kiti dokumentai ir/ar informacija negali būti saugomi darbuotojo kompiuteryje. Darbuotojai yra atsakingi už tinkamą duomenų, dokumentų perkėlimą ir išsaugojimą į Ligoninės saugyklą.

13. Rekomenduojama neatidarinėti el. laiškų ir bylų, gautų iš nepažįstamų, su Ligonine, jos veiklos vykdymu nesusijusių asmenų. Kilus bet kokiam įtarimui, kad laiškas gali būti užkrėstas virusu ar kitokia kenkėjiška programa, nedelsiant turi būti kreipiamasi į už IT paslaugas atsakingą darbuotoją.

14. Ligoninės duomenų saugykloje esančiuose aplankuose draudžiama laikyti, saugoti su darbu nesusijusią informaciją, pvz. muzikines, video rinkmenas, instaliacines programas, žaidimus ir pan. Už informacijos, esančios Ligoninės duomenų saugyklos aplankuose legalumą bei atitiktį šios Tvarkos reikalavimams atsako informaciją patalpinęs asmuo.

15. El. pašto sistemos vartotojas atsako už jo vardu siunčiamus elektroninius laiškus, jų turinį. Visi siunčiami elektroniniai laišakai privalo būti su standartiniu parašu: „Šis laiškas yra skirtas išimtinai tik jo adresatui. Laiško turinys ir visi jo priedai yra konfidenciali informacija. Jei laiškas nėra skirtas Jums, prašome nedelsiant apie tai informuoti mus ir ištrinti laišką bei visus jo priedus. Pespėjame, kad negalime garantuoti informacijos, siunčiamos elektroniniu paštu, visiško konfidencialumo.“

16. Ligoninės darbuotojams leidžiama jungtis prie el. pašto, specializuotų duomenų valdymo programų, per atstumą nuotoliniu būdu tik Ligoninės direktoriui priėmus sprendimą (kuris įforminamas direktoriaus įsakymu) dėl tokio jungimosi poreikio, būdo. Visais atvejais jungimasis prie Ligoninės kompiuterių tinklo nuotoliniu būdu yra galimas tik išimtiniais atvejais.

17. Ligoninės darbuotojai, kuriems Ligoninės direktoriaus įsakymu paskirta administruoti Facebook puslapį, privalo laikytis slaptažodžio konfidencialumo. Po paciento kreipimosi dėl registracijos ar kitos informacijos, visas susirašinėjimo pokalbis privalo būti ištrintas. Facebook puslapis pacientams gali būti naudojamas tik registracijai pas gydytoją, jokia konsultacija susijusi su sveikata, gydymu ir pan., negali būti teikiama.

18. Ligoninės direktorius registruoja kiekvienam darbuotojui priskiriamą ar jam laikinai naudojimui suteikiamą Ligoninei priklausančią įrangą, išskyrus telefonus, laikydamasis Ligoninės vidaus teisės aktų nuostatų.

19. Ligoninė vykdo jai priklausančių telefonų, SIM kortelių apskaitą, nustato paslaugų mėnesio limitus ir kontroliuoja, ar jie nėra viršijami vadovaudamasi Ligoninės vidaus teisės aktais.

20. Ligoninės darbuotojams naudojant el. pašto ir interneto resursus asmeniniais tikslais, neįsipareigoja užtikrinti darbuotojų asmeninės informacijos konfidencialumo (slaptumo). Be to, Ligoninė saugo darbuotojų išsiųstus el. laiškus Ligoninės vidaus teisės aktuose nustatytą terminą.

21. Kiekvienas Ligoninės darbuotojas yra asmeniškai atsakingas už savo sukurtų slaptažodžių atitikimą šios Tvarkos nuostatomis, jų periodinį keitimą, slaptažodžių apsaugą ir negali jų atskleisti tretiesiems asmenims (įskaitant ir kitus Ligoninės darbuotojus), išskyrus už IT paslaugas atsakingą darbuotoją.

22. Ligoninės darbuotojas, įjungęs savo darbo vietos kompiuterį suveda jo paties sukurtą slaptažodį, tokiu būdu Ligoninės darbuotojui automatiškai suteikiama prieiga ir prie Ligoninės naudojamų informacinių ir komunikacinių sistemų, pvz. elektroninio pašto.

23. Už IT paslaugas atsakingas darbuotojas užtikrina, kad darbuotojų kompiuteriuose būtų laiku keičiami slaptažodžiai.

24. Ligoninės darbuotojams draudžiama bet kokiems tretiesiems asmenims (įskaitant ir kitus Ligoninės darbuotojus), išskyrus už IT paslaugas atsakingą darbuotoją sudaryti galimybę prisijungti prie jo darbinio kompiuterio ir, pasinaudojus šia prieiga, prisijungti prie Ligoninės saugykloje saugomų aplankų.

25. Bet koks neautorizuotas dokumentų įkėlimas, sukūrimas, keitimas ar naikinimas yra draudžiamas.

26. Ligoninės direktorius ar jo nurodymu įpareigoti darbuotojai vieną kartą per metus (kaip taisyklė, pasibaigus kalendoriams metams) turi patikrinti bylų aplankuose esančių dokumentų reikalingumą ir ištrinti nereikalingus/aktualumą praradusius dokumentus, o tuos, kurie saugotini pagal Ligoninės dokumentacijos planą – Ligoninės nustatyta tvarka perduoti saugojimui.

27. Visa informacija, esanti Ligoninės suteiktuose įrenginiuose, techninėje įrangoje, el. pašte, saugykloje, specializuotose duomenų valdymo programose ir kt. bei susijusi su Ligoninės vykdoma veikla, darbuotojo darbo funkcijų vykdymu, išskyrus informaciją, kuri yra patalpinta pažeidžiant šią Tvarką, nuosavybės teise priklauso Ligoninei. Visos intelektinės nuosavybės teisės į šią informaciją taip pat priklauso Ligoninės i. Visa šiame punkte nurodyta informacija yra laikoma profesine informacija, t. y. sukurta ir/ar įgyta darbuotojams vykdant darbo funkcijas, Ligoninės vardu ir interesais.

28. Darbuotojai privalo naudoti prisijungimo vardus ir slaptažodžius visais atvejais.

29. Jungiantis prie darbuotojo paskyros Ligoninės specializuotose duomenų valdymo programose, slaptažodį turi susidaryti ne iš mažiau kaip 8 simboliai, kuriame privalomai turi būti: bent 1 mažoji raidė; bent 1 skaičius; bent 1 simbolis; bent 1 didžioji raidė.

30. Prie elektroninio pašto sistemos jungiantis ne iš darbo kompiuterio, būtina jungtis per tinklą, jeigu jungiasi naudojantis wi-fi tinklą, privaloma rinktis saugų, kuris apsaugotas slaptažodžiais, draudžiama rinktis laisvą wi-fi prieigą dėl galimo nesaugaus tinklo.

31. Pastebėjus ar įtarus, kad slaptažodis tapo žinomas tretiesiems asmenims, nedelsiant informuoti apie tai Ligoninės direktorių.

32. Už IT paslaugas atsakingas darbuotojas turi teisę jungtis prie darbo kompiuterių per Google remote dekstop programą siekiant darbuotojams sutvarkyti iškilusias problemas su IT sistemomis, programomis.

33. Darbuotojai, kuriems yra suteiktos prieigos prie išorinių trečiųjų asmenų duomenų bazių (pavyzdžiui, įvairių registrų) privalo užtikrinti, kad slaptažodžiai atitiktų sutarčių su atitinkamais trečiaisiais asmenimis reikalavimus, kad jie būtų keičiami šiose sutartyse nurodytais terminais ir tvarka, taip pat užtikrinti prieigos duomenų (vartotojo vardo, slaptažodžio) konfidencialumą. Tais atvejais, kai sutartyse nėra numatyti reikalavimai slaptažodžiams, jų keitimui ir techniškai tai yra įmanoma, slaptažodžiai turi būti sudaromi, keičiami ir saugomi laikantis šios Tvarkos bei kitų Ligoninės vidinių teisės aktų.

34. Slaptažodžiui neturi būti naudojama lengvai įsimenanti frazė ir raidžių bei skaitmenų kombinacija, siekiant sumažinti slaptažodžio atspėjimo riziką. Nerekomenduojama slaptažodžiui

naudoti pavardes, gimimo datas, mėgstamų sporto komandų pavadinimus, dienų, mėnesių pavadinimus ir kt., naudoti tą patį slaptažodį skirtingoms sistemoms, užsirašyti slaptažodžius ir laikyti juos šalia techninės įrangos ar joje.

35. Darbuotojams draudžiama platinti, atskleisti kitiems asmenims jiems suteiktus prieigos vardus, slaptažodžius, kodus ar kitus duomenis, kurie yra suteikti / naudojami darbo funkcijų vykdymo tikslais, išskyrus atvejus, kai keliems darbuotojams Ligoninė paveda naudotis viena prieiga. Už šių duomenų saugumą atsako atitinkamas darbuotojas.

36. Praradus techninę įrangą (pavyzdžiui, kompiuterį, duomenų saugojimo laikmeną, kurioje buvo su Ligoninės veikla susijusios informacijos, įskaitant, bet neapsiribojant asmens duomenų) ar telefoną, darbuotojas nedelsiant, bet ne vėliau, kaip per 3 (tris) valandas privalo imtis visų priemonių ir kreiptis į už IT paslaugas atsakingą darbuotoją, kad jis nedelsdamas imtųsi visų saugumo priemonių informacijos, esančios techninėje įrangoje ar telefone, ištrynimui arba techninės įrangos ar telefono užblokovimui taip, kad tokia informacija būtų nepasiekiamo (jeigu telefono ir/ar paslaugų teikėjo techninės galimybės leidžia atlikti tokius veiksmus). Taip pat per nurodytą terminą darbuotojas privalo informuoti Ligoninės direktorių. Praradęs techninę įrangą ar telefoną, darbuotojas turi nedelsdamas, bet ne vėliau kaip per 2 (dvi) valandas informuoti apie tai Ligoninės mobiliojo ryšio paslaugų teikėją.

37. Ligoninės darbuotojai ne vėliau kaip per 3 (tris) valandas nuo sužinojimo momento privalo informuoti Ligoninės direktorių apie: bet kokius techninės (įskaitant telefonus) ar programinės įrangos praradimo, gedimo, sugadinimo ar pažeidimo incidentus; bet kokią neįprastą veiklą, susijusią su Ligoninės tvarkomais asmens duomenimis, kita informacija, taip pat informacinėmis sistemomis; bet koki žinomą informacinių sistemų ar informacijos saugumo pažeidimą; koki įsilaužimą į Ligoninės informacines sistemas, aptiktą / įtariamą virusą ir pan.

38. Ligoninės pasilieka teisę atjungti ar išjungti techninę įrangą ar telefoną be atskiro darbuotojo įspėjimo.

39. Jeigu darbuotojas atleidžiamas iš darbo ar bet kokiais kitais pagrindais nutraukiama su juo sudaryta darbo sutartis, arba, kai Ligoninės darbuotoja (-as) išleidžiama (-as) nėštumo ir gimdymo, vaiko priežiūros, vaiko priežiūros iki trejų metų atostogų, o taip pat kitais atvejais Ligoninės direktoriaus sprendimu, darbuotojas ne vėliau kaip paskutinę darbo Ligoninėje dieną arba bet kuriuo kitu metu, nurodžius Ligoninės direktoriui, privalo grąžinti Ligoninei priklausančią informacinių technologijų techninę ir programinę bei kitą jam patikėtą įrangą, laikmenas, Ligoninės direktoriui arba, jo nurodymu, už IT paslaugas atsakingam asmeniui ar kitam Ligoninės darbuotojui, kartu su visais slaptažodžiais.

40. Prieš grąžindamas Ligoninei priklausančią informacinių technologijų techninę ir programinę bei kitą jam patikėtą įrangą, laikmenas – pašalinti visus aplankus, dokumentus su duomenų subjektų asmens duomenimis ir kitą vaizdo ar garso informaciją, kurioje yra ar gali būti duomenų subjektų asmens duomenų, taip pat ir iš naudoto el. pašto dėžutės, išskyrus atvejus, kai Ligoninės direktoriaus sprendimu Ligoninės darbuotojui yra nurodoma tokią informaciją palikti arba perkelti į Ligoninės duomenų saugojimo vietą;

41. Visuose stacionariuose bei nešiojamuose kompiuteriuose bei kitoje techninėje įrangoje turi būti nustatyta, kad nedirbant su jais 10 (dešimt) minučių, automatiškai įsijungtų ekrano užsklanda, kurią būtų galima pašalinti tik įvedus slaptažodį arba PIN kodą. Šiuos nustatymus atitinkamai kiekvienas darbuotojas nustato savarankiškai jam suteiktame kompiuteryje. Kilus klausimams, darbuotojas turi teisę bei pareigą kreiptis į už Ligoninės IT paslaugas atsakingą darbuotoją.

42. Darbo stočių (kompiuterių) paleidimo ir ekranų užsklandų slaptažodžiai turi būti keičiami ne rečiau kaip kas 3 (tris) mėnesius.

43. Atsitraukus nuo kompiuterio (pietų pertraukos metu, po darbo prieš išeinant namo ir pan.), privaloma saugiai išjungti visas programų, duomenų bazių valdymo ekranines aplikacijas. Išeinant iš kabineto / patalpos, jeigu jame nelieka daugiau darbuotojų, kabinetas/patalpa turi būti

užrakinamas arba užrakinamas kompiuterio ekranas, kuris gali būti atrakinamas tik darbuotojui suvedus slaptažodį.

44. Ligoninė, nepažeisdama darbuotojų interesų tiek, kiek tai yra būtina šioje Tvarkoje numatytiems tikslams pasiekti, laikantis Tvarkoje nurodytų principų, turi teisę savo nuožiūra tikrinti darbuotojų naudojamą informacinių ir komunikacinių technologijų priemones ir įrangą, jose naudojamą ir/ar saugomą informaciją, susijusią su Ligoninės veikla. Ligoninė taip pat turi teisę (bet ne pareigą) savo nuožiūra, apie tai neinformuodama darbuotojo, pašalinti dokumentus, bylas, el. pašto žinutes ar kitą elektroninę korespondenciją, jeigu tokie dokumentai, bylos ar kiti duomenys ar informacija, Ligoninės nuožiūra, neatitinka šios Tvarkos ar taikytinų įstatymų ar kitų teisės aktų reikalavimų. Atsižvelgiant į kitas šios Tvarkos nuostatas, darbuotojai, susipažindami su šia Tvarka, patvirtina, kad yra apie tai informuoti.

45. Visos Programinės įrangos licencijos, laikmenos ir dokumentai saugomi pas už IT paslaugas atsakingą darbuotoją arba Ligoninės direktorių.

46. Už IT paslaugas atsakingas darbuotojas reguliariai atlieka programinės įrangos patikrinimą ir imasi reikalingų veiksmų, kad būtų užtikrintas teisėtas, saugus, Ligoninės ir/ar trečiųjų asmenų interesus atitinkantis šios įrangos naudojimas.

47. Ligoninės kompiuteriuose esančios antivirusinės programos automatiškai tikrina visas naujai įrašomas ar bandomas pasiekti bylas, taip pat ir visus įeinančius ir išeinančius el. laiškus.

48. Bendros apsaugos nuo virusų taisyklės:

48.1. Prieš naudojant nežinomas išorines duomenų laikmenas arba kurios buvo naudojamos kitame kompiuteryje, būtina atlikti jų antivirusinę profilaktiką;

48.2. Kilus įtarimui patikrinti kompiuterį nuo virusų;

48.3. Siekiant išvengti kompiuterinių virusų, nepaleisti nežinomų programų. Gavus nežinomų siuntėjų atsiųstų elektroninių laiškų priedus, kuriuose gali būti kompiuterinių virusų, darbuotojas privalo neatidaryti gautų elektroninių laiškų priedų ir informuoti tiesioginį arba Ligoninės vadovą;

48.4. Darbuotojas, pastebėjęs virusų atakos požymius, privalo išjungti kompiuterį ir kreiptis į tiesioginį arba Ligoninės vadovą.

49. Darbuotojas neturi teisės savavališkai keisti jam priskirtos kompiuterinės įrangos (monitoriai, skeneriai, spausdintuvai bei kopijavimo aparatų spausdinimo valdikliai, klaviatūros, pelės, kolonėlės, ausinės, vaizdo kameros bei fotokameros, multimedijos projektoriai ir pan.) ir įdiegtos programinės įrangos.

50. Darbuotojams, naudojantiems elektroninį paštą, interneto prieigą ir kitą informacinių technologijų ir telekomunikacijų įrangą, draudžiama:

50.1. Siųsti elektroninio pašto žinutes, naudojantis kito asmens arba neegzistuojančiu elektroninio pašto adresu;

50.2. Siųsti elektroninio pašto žinutes, nuslepiant savo tapatybę;

50.3. Negavus Ligoninės vadovo sutikimo, siųsti elektrinius laiškus, kuriuose yra informacija pripažįstama konfidencialia informacija ar Ligoninės komercine paslaptimi, išskyrus, jei informacija siunčiama asmeniui, kuris turi teisę gauti šią informaciją;

50.4. Negavus Ligoninės vadovo sutikimo perduoti, platinti, atskleisti tretiesiems asmenims darbui su technine ir programine įranga jiems suteiktus prieigos vardus, slaptažodžius ar kitus duomenis;

50.5. Kurti ar platinti laiškus, skatinančius gavėją siųsti laiškus kitiems. Laiškai su perspėjimais dėl kompiuterinių virusų, telefonų pasiklausymų ar kitų tariamų reiškinų, kuriuose prašoma nusiųsti gautą laišką visiems savo kolegoms, draugams ar pažįstamiems, turi būti nedelsiant ištrinami. Jei pranešimas sukelia įtarimų, prieš jį pašalinant, pranešti tiesioginiam arba Ligoninės vadovui;

50.6. Naudoti interneto prieigą ir elektroninį paštą asmeniniams tikslams, Lietuvos Respublikos įstatymais draudžiamai veiklai, šmeižiančio, įžeidžiančio, grasinančiojo pobūdžio ar

visuomenės dorovės ir moralės principams prieštaraujanti informacijai, kompiuterių virusams, masinei nepageidaujamai informacijai „spam“ siųsti ar kitiems tikslams, galintiems pažeisti Ligoninės ar kitų asmenų teisėtus interesus;

50.7. Atlikti veiksmus, pažeidžiančius fizinio ar juridinio asmens teises, kurias saugo autorių, gretutinių ir intelektualinės nuosavybės teisių apsaugos įstatymai. Tarp tokių veiksmų yra programinės įrangos diegimas, naudojimas, saugojimas arba platinimas neturint licencijos, neleistinas autorių teisėmis apsaugotų kūrinių kopijavimas;

50.8. Parsisiųsti arba platinti tiesiogiai su darbu nesusijusią grafinę, garso ir vaizdo medžiagą, žaidimus ir programinę įrangą, siųsti duomenis, kurie užkrėsti virusais, turi įvairius kitus programinius kodus, bylas, galinčias sutrikdyti kompiuterinių ar telekomunikacinių įrenginių bei programinės įrangos funkcionavimą ir saugumą;

50.9. Atskleisti prisijungimo prie Ligoninės sistemų informaciją (prisijungimo vardą, slaptažodį) arba leisti naudotis savo prisijungimo vardu kitiems asmenims; Dirbant su slaptažodžiais reikia laikytis taisyklių:

50.9.1 Saugoti slaptažodį. Neužrašinėti jo ant popieriaus skiaučiu, kalendorių ir pan. Nepalikti lapelio su slaptažodžiu priklijuoto prie vaizduoklio arba prie apatinės darbo stalo pusės;

50.9.2 Nenaudoti trumpų ir elementarių slaptažodžių sudarytų iš reikšminių žodžių.

50.9.3 Pažeisti bet kurio kompiuterio, tinklo ar paskyros autentifikacijos arba saugumo sistemas;

50.9.4 Ardyti ar išmontuoti ar kitaip keisti kompiuterinę įrangą;

50.9.5 Perkopijuoti programinę įrangą;

50.9.6 Savarankiškai šalinti kompiuterinės įrangos gedimus;

50.9.7 Parsisiųsti ar žaisti internetinius ar kitus kompiuterinius žaidimus;

50.9.8 Savavališkai blokuoti antivirusines programas ar kitas programas;

50.9.9 Sutrikdyti kompiuterinės sistemos darbą arba panaikinti galimybę naudotis teikiama paslauga ar informacija;

50.9.10 Dalyvauti interneto lažybose ir azartiniuose lošimuose;

50.9.11 Naudoti Ligoninės išteklius komercinei veiklai vystyti ar naudai gauti;

50.9.12 Savavališkai keisti kompiuterių ar kitų prietaisų tinklo parametrus (IP adresą ir pan.), savarankiškai keisti, taisyti informacinių technologijų ir telekomunikacijų techninę ir programinę įrangą;

50.9.13 Pažeisti kitų tinklų, kurių paslaugomis naudojama, naudojimo arba ekvivalentiškas taisykles;

50.9.14 Savavališkai keisti interneto naršyklės ir elektroninio pašto programinės įrangos parametrus, susijusius su apsauga arba prisijungimo būdu, nepaisyti bet kurio iš įdiegtų saugumo mechanizmų;

50.9.15 Atlikti bet kokius kitus su darbo funkcijų vykdymu nesusijusius ir teisės aktams prieštaraujančius veiksmus;

50.9.16 Neįgaliotiems asmenimis Ligoninėje ar už Ligoninės naudoti ir perduoti slaptažodžius ir kitus duomenis, kuriais pasinaudojus programinėmis ir techninėmis priemonėmis galima sužinoti Ligoninės duomenis ar kitaip sudaryti sąlygas susipažinti su Ligoninės duomenimis.

51. Keitimosi informacija politika.

51.1. Perduodant informaciją elektroniniu paštu, būtina:

Atidžiai užrašyti adresato elektroninio pašto adresą, kad informacija nebūtų perduota kitam asmeniui;

51.1.1 Už organizacijos ribų siunčiamiems laiškam naudoti el. pašto programoje numatytą el. laiško parašą (signature) ir jo nekeisti;

51.1.2 Priimant sprendimus pagal elektroniniu paštu gautą informaciją, būtina

įsitikinti šios informacijos tikrumu (kitas asmuo gali apsimesti tikruoju siuntėju). Kilus įtarimui bei svarbiais atvejais rekomenduojama susisiekti su siuntėju ir įsitikinti ar gautas laiškas buvo jo išsiųstas.

51.2. Neatverti pridėtų (angl. „attached“) failų, kurie yra gauti iš nepažįstamų asmenų, arba nėra galimybės įsitikinti šių failų turiniu.

51.3. Už pašalinių asmenų naudojimąsi internetu kompiuteryje ir informacijos perdavimą elektroniniu paštu yra atsakingas kompiuterio naudotojas.

51.4. Darbuotojai, naudojantys Ligoninės kompiuterinę techninę ir programinę įrangą privalo:

51.4.1 Kompiuterinę techninę ir programinę įrangą, elektroninio pašto ir interneto paslaugas naudoti tik darbo funkcijoms atlikti;

51.4.2 Kompiuterines programas naudoti vadovaujantis konkrečių kompiuterinių programų licencijų reikalavimais bei šia tvarka.

52. Nuotolinio darbo politika.

52.1. Nuotoliniam Ligoninės darbuotojų prisijungimui prie Ligoninės kompiuterių tinklo yra taikomi tokie pat saugumo standartai kaip ir lokaliai prisijungimui.

52.2. Asmenys, atliekantys nuotolinį prisijungimą turi užtikrinti, kad jų šeimos nariai ar pašaliniai asmenys neprieitų prie organizacijos duomenų ir kompiuterinės įrangos, nepažeistų organizacijos informacijos saugumo valdymo sistemos nuostatų.

52.3. Nuotoliniu būdu dirbantis darbuotojas turi laikytis šių reikalavimų:

52.3.1 Niekam neatskleisti prisijungimo ir kitų slaptažodžių;

52.3.2 Užtikrinti, kad kompiuterinė įranga nuotolinio prisijungimo prie organizacijos Tinklo metu nėra prisijungusi prie kitų išorinių tinklų;

52.3.3 Nenaudoti organizacijos informacinių resursų su darbu nesusijusiai veiklai;

52.3.4 Nekeisti nuotolinio prisijungimo įrangos parametrų;

52.3.5 Užtikrinti, kad nuotoliniu būdu prijungtame kompiuteryje naudojama operacinė sistema ir antivirusinė programinė įranga būtų reguliariai atnaujinama.

53. Nešiojamųjų kompiuterių naudojimo tvarka.

53.1. Nešiojamojo kompiuterio negalima palikti be priežiūros viešose vietose ir transporto priemonėse;

53.2. Keliaujant draudžiama nešiojamąjį kompiuterį atiduoti į lėktuvo, autobuso, traukinio ar kitos transporto priemonės bagažo skyrių, nebent vežėjo taisyklės reikalauja kitaip;

53.3. Dirbant viešose vietose, nešiojamasis kompiuteris turi būti tokioje padėtyje, kad pašaliniai asmenys negalėtų matyti ekrane rodomos informacijos;

53.4. Nesinaudojant nešiojamuoju kompiuteriu jį būtina išjungti, išregistruoti iš naudotojo paskyros arba užrakinti operacinę sistemą taip, kad jungiantis iš naujo reikėtų įvesti naudotojo vardą ir slaptažodį;

53.5. Draudžiama leisti naudotis nešiojamaisiais kompiuteriais pašaliniams asmenims. Draudžiama perduoti tretiesiems asmenims nešiojamame kompiuteryje esančios informacijos kopijas. Draudžiama naudoti nešiojamąjį kompiuterį neteisėtai veiklai vykdyti;

53.6. Draudžiama keisti nešiojamojo kompiuterio, jame esančios programinės įrangos techninius parametrus;

53.7. Nešiojamame kompiuteryje draudžiama diegti su darbu nesusijusią programinę įrangą;

53.8. Praradus nešiojamąjį kompiuterį, apie tai reikia nedelsiant pranešti tiesioginiam vadovui;

53.9. Visi aukščiau išvardinti reikalavimai yra taikomi (kiek tai techniškai yra įmanoma) ir kitiems organizacijoje naudojamiems nešiojamiems prietaisams, galintiems talpinti ir apdoroti informaciją (pvz. delniniai kompiuteriai, telefonai ir pan.).

54. Ligoninės vadovas neužtikrina, kad bus išsaugotas privatumas to, ką Ligoninės darbuotojai sukuria, siunčia ar gauna Ligoninės informacinėje sistemoje.

55. Organizuojant stebėseną laikomasi proporcingumo, tikslingumo, skaidrumo, saugumo, tikslumo ir duomenų išsaugojimo bei būtinumo principų, ir stebėsenos priemonės taikomos tik tais atvejais, kai iškeltų tikslų kitomis, mažiau darbuotojų privatumą ribojančiomis priemonėmis, pasiekti neįmanoma arba, Ligoninės vertinimu, yra nepraktiška.

56. Stebėsenos ir kontrolės darbo vietoje tikslai:

56.1. Apsaugoti konfidencialius Ligoninės duomenis nuo atskleidimo tretiesiems asmenims;

56.2. Apsaugoti Ligoninės klientų ir darbuotojų asmens duomenis nuo neteisėto perdavimo tretiesiems asmenims;

56.3. Apsaugoti Ligoninės informacines sistemas nuo įsilaužimų ir duomenų vagysčių, virusų, pavojingų interneto puslapių, kenkėjiškų programų;

56.4. Apsaugoti Ligoninės turtą ir užtikrinti asmenų saugumą Ligoninės patalpose ar teritorijoje;

56.5. Apsaugoti Ligoninės turtinius interesus ir užtikrinti darbo pareigų laikymąsi.

57. Ligoninė pasilieka teisę be atskiro darbuotojo įspėjimo riboti prieigą prie atskirų interneto svetainių ar programinės įrangos. Nepakankant minėtų priemonių, Ligoninė gali tikrinti, kaip darbuotojas laikosi elektroninio pašto ir interneto resursų naudojimo reikalavimų nurodytais tikslais, tiriant incidentus, atiduoti darbuotojų naudojamą įrangą tirti tretiesiems asmenims, kurie teisės aktų nustatyta tvarka turi teisę tokius duomenis gauti.

58. Darbuotojų naudojamų elektroninės komunikacijos priemonių, programinės ir/ar techninės įrangos, dokumentų/ failų/ informacijos peržiūra ar patikrinimas gali būti vykdoma siekiant apginti Ligoninės ir jos darbuotojų interesus. Peržiūra ar patikrinimas gali būti vykdoma šiais atvejais:

58.1. Kai darbuotojo daugiau nei 1 (viena) darbo dieną dėl nežinomos priežasties nėra darbe arba pasibaigia darbuotojo darbo sutartis su Ligonine, o būtina užtikrinti Ligoninės veiklos tęstinumą;

58.2. Kai darbuotojas yra laikinai nedarbingas, atostogauja ar dėl kitų priežasčių jo nėra darbe, o būtina užtikrinti Ligoninės veiklos tęstinumą. El. pašto, dokumentų, esančių duomenų saugykloje, informacijos ir kt. dokumentų ar failų peržiūrai atlikti IT specialistas Ligoninės direktoriaus nurodymu sukuria laikiną vartotoją bei prisijungimo duomenis (vartotojo vardą, slaptažodį) ir apie juos informuoja darbuotoją, kuriam pavesta atlikti peržiūrą. Laikinas vartotojas ir prisijungimo duomenys turi būti nedelsiant panaikinami, kai išnyksta aplinkybės dėl kurių būtina atlikti peržiūrą. Už jų panaikinimą atsakingas IT specialistas;

58.3. Kai reikia patikrinti informaciją apie galimai neteisėtus darbuotojo veiksmus, kurių patvirtinimą arba paneigimą galima įrodyti peržiūrint darbuotojo siųstų arba gautų elektroninių laiškų ir jų priedų turinį, interneto jungimosi laiką, trukmę ir kt. (internetu srauto duomenys), el. pašto siųstų ir gautų laiškų adresus, datą, laiką ir kt. (el. pašto srauto duomenys), naudotų kitų Ligoninės ar ne Ligoninės instaliuotų programų datą, laiką, trukmę ir kt., naudotų Ligoninės ar ne Ligoninės laikmenų operacijų kiekį, pobūdį, trukmę, turinį;

58.4. Kai Ligoninė yra atsakinga už darbuotojo atliktų veiksmų padarinius ir reikia ginti Ligoninės interesus siekiant gauti patvirtinimą ar paneigimą dėl galimai neteisėtų darbuotojo veiksmų;

58.5. Kai darbuotojas elektroninės komunikacijos priemones, programinę ir/ar techninę įrangą galimai naudoja ne darbo funkcijų Ligoninės vykdymo tikslais ir/ar pažeidžiant šią Tvarką.

59. Ligoninė, siekiant šiame skyriuje nurodytų tikslų, gali būti naudojamos specialios programos, kuriomis automatiniu būdu išsaugoma informacija apie darbuotojų naršymo istoriją, kuri yra saugoma ne ilgiau kaip 6 (šešis) mėnesius. Saugomi duomenys apie darbuotojų naršymo istoriją nėra stebimi nuolatos, jų peržiūrėjimas vykdomas tik tuomet, kai kyla pagrįstas įtarimas dėl teisės aktų ar darbo pareigų pažeidimo, ir tik tiek, kiek tai susiję su padarytu ir/ar įtariamu pažeidimu. Duomenų peržiūrėjimo procedūroje sudaroma galimybė dalyvauti ir darbuotojui, kurio duomenys yra peržiūrimi, nebent Ligoninė nusprendžia, kad darbuotojo dalyvavimas galėtų pakenkti tyrimo kokybei.

60. Šia Tvarka darbuotojai yra informuojami, kad Ligoninė gali patikrinti jiems priskirtuose kompiuteriuose įdiegtų komunikacijos programų (pavyzdžiui, skype) turinį ar kitokį elektroninį susirašinėjimą tiek, kiek tai yra būtina šioje Tvarkoje nurodytiems tikslams pasiekti.

61. Ligoninė pasilieka teisę be atskiro pranešimo riboti prieigą prie atskirų interneto svetainių ar programinės įrangos. Ligoninei nusprendus, jog tokių priemonių nepakanka, siekiamiems tikslams pasiekti, Ligoninė gali tikrinti, kaip darbuotojas laikosi el. pašto ir/ar interneto resursų naudojimo reikalavimų, taip pat perduoti darbuotojų naudojamą įrangą ištirti tretiesiems asmenims.
