PATVIRTINTA
VšĮ Telšių rajono pirminės sveikatos
priežiūros centro direktoriaus
2019 m. rugpjūčio 2 d.
įsakymu Nr. V-81

ORGANIZACINIŲ IR TECHNINIŲ ASMENS DUOMENŲ SAUGUMO PRIEMONIŲ ĮGYVENDINIMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Organizacinių ir techninių asmens duomenų saugumo priemonių įgyvendinimo tvarkos aprašas (toliau – Aprašas) nustato organizacines ir technines asmens duomenų saugumo priemones ir jų taikymo tvarką VšĮ Telšių rajono pirminės sveikatos priežiūros centrui (toliau – Telšių PSPC) tvarkant asmens duomenis automatiniu būdu ir neautomatiniu būdu susistemintose rinkmenose.

2. Aprašas taikomos Telšių PSPC, kaip duomenų valdytojai tvarkančiai asmens duomenis, ir jos pasitelktiems paslaugų teikėjams, teikiantiems su asmens duomenų tvarkymu ir (ar) duomenų saugumo užtikrinimu susijusias bei kitas paslaugas (toliau – Paslaugų teikėjai). Aprašo privalo laikytis visi Telšių PSPC darbuotojai, tvarkantys asmens duomenis ar su jais susipažįstantys.

3. Aprašas parengtos vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1–88) (toliau – Reglamentas (ES) 2016/679) ir Valstybinės duomenų apsaugos inspekcijos 2018 m. spalio 31 d. Tinkamų organizacinių ir techninių duomenų saugumo priemonių įgyvendinimo gairėmis asmens duomenų valdytojams ir tvarkytojams.

4. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (ES) 2016/679.

II SKYRIUS
ASMENS DUOMENŲ SAUGOS ORGANIZAVIMAS

5. Telšių PSPC siekia užtikrinti darbuotojų pareigų ir atsakomybės sričių atskyrimą, kad būtų sumažinta neteisėto ar netyčinio asmens duomenų pakeitimo, atskleidimo ar netinkamo panaudojimo rizika.

6. Telšių PSPC direktorius yra atsakingas už tai, kad Telšių PSPC darbuotojai ir paslaugų tiekėjai vadovautųsi šiuo Aprašu.

7. Telšių PSPC informacinių technologijų priežiūrą vykdantis asmuo, kuriuo gali būti Telšių PSPC darbuotojas arba išorės paslaugų teikėjas (toliau – IT saugos įgaliotinis), yra atsakingas už informacijos saugos valdymo palaikymą, darbo organizavimą, periodinį informacijos saugos rizikos vertinimą ir informacijos saugos koordinavimą bei kontrolę Telšių PSPC.

8. Telšių PSPC darbuotojai yra asmeniškai atsakingi už šių Aprašo nuostatų laikymąsi, tinkamą asmens duomenų tvarkymą ir saugumo priemonių užtikrinimą vadovaujantis šiame Apraše ir teisės aktuose įtvirtintais asmens duomenų tvarkymo reikalavimais.

9. Telšių PSPC užtikrina, kad prieiga prie visos Telšių PSPC informacijos, įskaitant asmens duomenis, nebūtų suteikiama vienam asmeniui, nekontroliuojant jo veiksmų.

10. Telšių PSPC užtikrina, kad būtų registruojami naudotojų veiksmai, atliekami su asmens duomenimis.

11. Telšių PSPC užtikrina, kad Paslaugų teikėjai būtų supažindinti su Telšių PSPC taikomais asmens duomenų saugumo reikalavimais ir raštu įsipareigotų jų laikytis. Asmens duomenų

saugumo reikalavimai gali būti įtvirtinti sutartyje su Paslaugų teikėju arba pridedami kaip jos priedas. Paslaugų teikėjai turi laikytis šių principų:

11.1. gavus prieigą prie Telšių PSPC tvarkomų asmens duomenų, tvarkyti tik tuos asmens duomenis, kurie yra būtini paslaugų teikimui;

11.2. užtikrinti asmens duomenų konfidencialumą, t. y. kad asmens duomenys nebūtų atskleidžiami Paslaugų teikėjo organizacijos viduje bei už jos ribų;

11.3. užtikrinti asmens duomenų vientisumą, t. y. Paslaugų teikėjai negali keisti Telšių PSPC tvarkomų asmens duomenų turinio ar formos;

11.4. Paslaugų teikėjo darbuotojai negali ištrinti ar perkelti Telšių PSPC tvarkomų asmens duomenų;

11.5. prisijungimas prie Telšių PSPC vidinių sistemų ar tinklo yra galimas tik iš anksto sutartu laiku, gavus prašymą iš atsakingų Telšių PSPC darbuotojų arba pastebėjus įvykius, kurie gali neigiamai įtakoti Telšių PSPC darbą.

12. Telšių PSPC turi IT išteklių, naudojamų asmens duomenims tvarkyti, registrą (techninės, programinės ir tinklo įrangos). Už registro pildymą atsakingas IT saugos įgaliotinis. Registro forma pateikiama šio Aprašo priede.

13. IT ištekliai reguliariai, kartą per 3 mėnesius, peržiūrimi ir prireikus atnaujinami. Už peržiūrą atsakingas IT saugos įgaliotinis.

III SKYRIUS
ELEKTRONINĖS DARBO PRIEMONĖS IR JŲ NAUDOJIMAS

14. Darbo vietų kompiuteriai, programinė įranga, kompiuterių tinklai, spausdintuvai, interneto ryšys, elektroninio pašto sistema, kita kompiuterių įranga bei kitos Telšių PSPC darbuotojams suteiktos elektroninės darbo priemonės turi būti naudojamos tik darbuotojų tiesioginėms darbo funkcijoms atlikti.

15. Darbuotojams draudžiama darbo vietos kompiuteryje diegti ar šalinti programas arba kitaip modifikuoti darbo vietos kompiuteryje veikiančią sistemą.

16. Darbo vietų kompiuteriuose draudžiama diegti nelicencijuotą programinę įrangą, programinę įrangą, kuri sudaro galimybes pasinaudoti šio kompiuterio ištekliais per tinklą.

17. Telšių PSPC naudojama tik legali programinė įranga, kuri konfigūruojama ir atnaujinama laikantis jos gamintojo rekomendacijų.

18. Serveriuose, duomenų bazėse tvarkomi asmens duomenys yra šifruojami.

19. Kiekvienas stacionarus kompiuteris turi turėti nuolatinę vietą. Draudžiama pernešti kompiuterį į kitą darbo vietą be IT saugos įgaliotinio ar Telšių PSPC direktoriaus leidimo ir žinios. Ši nuostata netaikoma nešiojamiesiems kompiuteriams.

20. Nešiojamieji kompiuteriai, mobilieji telefonai ir kiti mobilieji įrenginiai (toliau – mobilieji įrenginiai) Telšių PSPC suteikti darbuotojams, gali būti naudojami tik atliekant darbo funkcijas. Mobilieji įrenginiai naudojami ir prižiūrimi vadovaujantis gamintojo rekomendacijomis.

21. Vartotojų autentifikavimas ir laiškų pasiėmimas iš pašto serverio prieinamas tik šifruotais protokolais (SSL, TLS, HTTPS). Visas įeinantis elektroninio pašto srautas tikrinamas patikima antivirusine programa, kurios pavyzdžių bazė reguliariai (ne rečiau kaip kartą per savaitę) automatiškai atnaujinama. Gaunami elektroniniai laiškai tikrinami nepageidaujamų elektroninių laiškų (*angl. spam*) filtru.

22. Darbuotojo elektroninio pašto paskyra išjungiama atleidus darbuotoją. Išjungus elektroninio pašto paskyrą, duomenys yra saugomi 30 kalendorinių dienų nuo šios paskyros išjungimo dienos. Telšių PSPC direktorius ar jo įgaliotas asmuo per 30 kalendorinių dienų gali prašyti prieigos prie pašto dėžutės, jei to reikia siekiant užtikrinti Telšių PSPC veiklos tęstinumą. Po 30 kalendorinių dienų nuo paskyros išjungimo ji naikinama, o pašto dėžutės duomenys ištrinami arba, jei buvo pateiktas prašymas, perduodami Telšių PSPC direktoriui ar jo įgaliotam asmeniui toliau saugoti.

23. Darbuotojams draudžiama Telšių PSPC suteiktą elektroninį paštą naudoti asmeniniam susirašinėjimui.

24. Darbo tikslais naudojamuose mobiliuosiuose įrenginiuose turi būti naudojamos ne mažesnio saugumo lygio priemonės, nei SIM kortelė su PIN kodu arba ekrano užsklanda su slaptažodžiu. SIM kortelės ir ekrano užsklandos kodai turi būti skirtingi.

25. Mobiliuose įrenginiuose turi būti įdiegta mobiliųjų įrenginių valdymo programinė įranga, leidžianti nuotoliniu būdu blokuoti įrenginį, ištrinti duomenis, apriboti nesankcionuotos programinės įrangos diegimą.

26. Darbuotojams draudžiama leisti naudotis turimomis elektroninėmis darbo priemonėms tretiesiems asmenims (šeimos nariams ir kt).

27. Jeigu Telšių PSPC leidžiamas nuotolinis darbas, tokiu atveju privalo būti naudojamos bent šios saugumo priemonės:

27.1. prie vidinio tinklo jungiamasi per virtualų privatų tinklą (VPN);

27.2. naudojama ekrano užsklanda su slaptažodžiu;

27.3. disko šifravimo programos;

27.4. naudojama lokali operacinės sistemos ugniasienė;

27.5. naudojamos antivirusinės programos ar kitokia apsauga nuo kenkėjiškų programų;

27.6. prisijungimo slaptažodis negali būti išsaugomas interneto naršyklėje.

IV SKYRIUS
PRIEIGOS TEISIŲ VALDYMAS

28. Asmens duomenis gali tvarkyti tik Telšių PSPC direktorius ir tie Telšių PSPC darbuotojai, kuriems jie yra būtini darbo funkcijų vykdymui.

29. Prieigos teisių prašymai turi būti registruojami elektroninėmis priemonėmis ar kitu būdu.

30. Naudotojų paskyros yra asmeninės. Naudotojų identifikatoriai (prisijungimo vardai) yra unikalūs ir asmeniniai. Bendrų paskyrų naudojimas yra draudžiamas, išskyrus informacinių sistemų integracijos bei informacinių technologijų infrastruktūros priežiūros tikslais.

31. Darbuotojams yra suteikiamos tik tokios prieigos teisės, kurios yra reikalingos jų darbo funkcijų atlikimui.

32. Privilegijuotų (administratoriaus) prieigos teisių suteikimas ir naudojimas turi būti ribojamas ir kontroliuojamas. Privilegijuotos teisės yra suteikiamos esant tiesioginio darbuotojo vadovo, darbuotojo, atsakingo už asmens duomenų tvarkymą, bei darbuotojo, atsakingo už informacijos saugą, sutikimui. Sutikimai turi būti dokumentuojami arba leidimai turi būti suteikiami tokiu būdu, jog būtų galima įsitikinti, kad leidimas buvo duotas.

33. Prieš suteikiant privilegijuotas teises, turi būti įvertinama darbuotojo esamų pareigų atskyrimo galimybė bei kylančios rizikos.

34. Prieigos teisės turi būti peržiūrimos bent kartą per metus. Šią peržiūrą atlieka darbuotojų tiesioginiai vadovai ir darbuotojai, atsakingi už asmens duomenų tvarkymą.

35. Privilegijuotų naudotojų teisės turi būti peržiūrimos bent du kartus per metus. Šią peržiūrą atlieka darbuotojai, atsakingi už asmens duomenų tvarkymą.

36. Pasikeitus darbuotojo pareigoms, turi būti peržiūrimos ir, jei reikia, keičiamos prieigos prie asmens duomenų teisės.

37. Atleidžiant darbuotoją iš darbo, nutraukiant sutartinius santykius su Paslaugų teikėju, prieigos teisės turi būti panaikintos ne vėliau nei iki paskutinės darbo arba paslaugų teikimo dienos Telšių PSPC pabaigos.

38. Konfidencialumo įsipareigojimai lieka galioti darbuotojui ar Paslaugų teikėjui nutraukus santykius su Telšių PSPC.

V SKYRIUS
SLAPTAŽODŽIŲ NAUDOJIMAS

39. Slaptažodžiai turi būti sudaromi laikantis šių reikalavimų:

39.1. minimalus slaptažodžio ilgis – 8 klaviatūros simboliai, panaudojant 4 klaviatūros simbolių grupes: mažosios raidės, didžiosios raidės, skaitmenys, specialūs simboliai;

39.2. maksimali slaptažodžio galiojimo trukmė – 60 dienų;

39.3. negalima naudoti paskutinių 7 slaptažodžių.

39. Po 3 nesėkmingų bandymų suvesti slaptažodį įrenginys yra blokuojamas pagal gamintojo saugumo reikalavimus.

40. Pirminiai slaptažodžiai naudotojui turi būti perduodami konfidencialumą užtikrinančiu būdu, pavyzdžiui užrašant ir įteikiant darbuotojui į rankas uždaru pavidalu (užklijuotame voke ar pan.). Pirmo prisijungimo metu naudotojas privalo pasikeisti slaptažodį.

41. Draudžiama palikti informaciją apie slaptažodžius lengvai pasiekiamoje fizinėje ar elektroninėje formoje, pavyzdžiui, užrašyti ant lapelio šalia kompiuterio, patalpinti bendrame serveryje ir panašiai. Draudžiamas automatinis slaptažodžių išsaugojimas.

42. Visi informacinių sistemų gamintojų sukurti pirminiai slaptažodžiai turi būti pakeičiami pirmojo prisijungimo metu.

43. Informacinio turto privilegijuotų (administratoriaus) paskyrų slaptažodžiai turi būti keičiami rankiniu būdu, ne rečiau kaip vieną kartą per metus. Po tokių slaptažodžių pakeitimo apie tai informuojamas Telšių PSPC direktorius ar kitas jo įgaliotas asmuo.

44. Darbuotojas yra atsakingas už jo slaptažodžių konfidencialumą. Draudžiama atskleisti naudojamus slaptažodžius kitiems darbuotojams ar kitiems neįgaliotiems asmenims.

45. Slaptažodžiai turi būti nedelsiant pakeičiami, jei įtariama, kad slaptažodžių saugumas yra pažeistas (slaptažodis tapo prieinamas neįgaliotiems asmenims ar kt.).

46. Techninėmis priemonėmis turi būti užtikrinta, kad tinklu perduodami slaptažodžiai būtų šifruoti.

47. Turi būti registruojami sėkmingi ir nesėkmingi naudotojų bandymai prisijungti prie paskyrų, turi būti ribojamas kelių iš eilės nesėkmingų prisijungimų skaičius, blokuojant naudotojo paskyrą.

48. Techninėmis priemonėmis turi būti užtikrinama, jog nenaudojant kompiuterio daugiau nei 15 minučių, automatiškai aktyvuojama ekrano užsklanda. Norint toliau naudotis kompiuteriu, turi būti privaloma įvesti naudotojo slaptažodį.

VI SKYRIUS
NUOSAVŲ DARBUOTOJŲ ĮRENGINIŲ NAUDOJIMAS DARBUI

49. Jei darbuotojas Telšių PSPC direktoriaus sutikimu naudoja darbui nuosavas elektronines darbo priemones, Telšių PSPC turi prijungti tokį įrenginį prie Telšių PSPC tinklo bei užtikrinti, kad nuosavuose įrenginiuose bus įdiegtos tokios pačios apsaugos priemonės, kokios yra įdiegiamos Telšių PSPC įrenginiuose.

50. Naudojant darbui nuosavus įrenginius, darbuotojas privalo darbo tikslais sukurti ir šio Aprašo reikalavimus atitinkančiu slaptažodžiu apsaugoti atskirą paskyrą ir / arba naudoti kitas priemones, kurios padėtų atskirti duomenis, tvarkomus vykdant darbo funkcijas, nuo duomenų, tvarkomų asmeniniais tikslais.

51. Jei darbuotojas Telšių PSPC sutikimu naudoja darbui nuosavus įrenginius, Telšių PSPC turi teisę motyvuotai paprašyti darbuotojo nedelsiant sudaryti galimybę Telšių PSPC darbuotojams ar Paslaugų teikėjams susipažinti su darbuotojo nuosavuose įrenginiuose esančiais duomenimis.

52. Telšių PSPC turi teisę darbuotojui priklausančiuose nuosavuose įrenginiuose esančius asmens duomenis, susijusius su darbuotojo darbo funkcijų vykdymu, savo nuožiūra naudoti ir / arba tokius duomenis ištrinti.

53. Kai darbuotojas nutraukia sutartį su Telšių PSPC, jis privalo Telšių PSPC atstovo akivaizdoje ištrinti visus su darbu Telšių PSPC susijusius asmens duomenis iš nuosavų įrenginių. Darbuotojas taip pat turi sudaryti galimybę Telšių PSPC atstovui peržiūrėti darbo tikslams naudotus įrenginius ir įsitikinti, jog su darbu Telšių PSPC susiję asmens duomenys yra tinkamai ištrinti.

VII SKYRIUS
FIZINĖ SAUGA

54. Telšių PSPC užtikrina patekimo į patalpas kontrolę ir apsaugą, kuri apima apsaugos (judesio) signalizaciją ir kitas priemones.

55. Pašaliniai asmenys į Telšių PSPC patalpas, kuriose įrengtos tarnybinės stotys, gali patekti tik lydimi Telšių PSPC darbuotojų.

56. Ne darbo metu Telšių PSPC patalpose įjungiama signalizacija.

57. Tarnybinėms stotims, kompiuterizuotoms darbo vietoms ir tinklo komutatoriams užtikrinamas atsarginis elektros tiekimas naudojant centrinį nepertraukiamo maitinimo šaltinį.

58. Visose Telšių PSPC patalpose įrengta priešgaisrinė signalizacija, įspėjimo apie gaisrą sistema, ir ugnies gesintuvai (CO2).

59. Tinkamas aplinkos drėgnumas ir patalpų temperatūra tarnybinių stočių patalpoje užtikrinama naudojant kondicionavimo sistemą.

60. Dokumentai, kuriuose yra asmens duomenų, saugomi rakinamose spintose arba seifuose.

61. Fizinės saugos priemonių patikrinimas atliekamas ne rečiau kaip kartą per metus arba kitais teisės aktų nustatytais terminais.

VIII SKYRIUS
ĮRANGOS SAUGUMAS

62. Telšių PSPC priklausanti įranga yra laikoma Telšių PSPC patalpose, išskyrus:

62.1. nešiojamuosius kompiuterius ir mobiliuosius įrenginius, kuriais, vadovaujantis Telšių PSPC vidaus teisės aktais, galima dirbti ir ne Telšių PSPC patalpose;

62.2. Telšių PSPC informacinių sistemų serverius, esančius duomenų centre ir skirtus pagrindinei veiklai vykdyti;

62.3. Telšių PSPC informacinių sistemų serverius, skirtus veiklos tęstinumui užtikrinti nenumatytų situacijų metu.

63. Telšių PSPC naudojama komunalinių paslaugų įranga (elektros skydinė, vandens tiekimo įranga, šildymo ir kondicionavimo įranga) turi būti tinkamai prižiūrima ir periodiškai testuojama siekiant užtikrinti nepertraukiamą jos veikimą.

64. Telšių PSPC naudojami maitinimo ir telekomunikacijų kabeliai turi būti prižiūrimi ir apsaugoti (prisijungimas prie jų turi būti autorizuotas, kabelių mazgai turi būti paslėpti) nuo slapto prisijungimo, trukdžių ir pažeidimų.

65. Telšių PSPC naudojama įranga turi būti techniškai prižiūrima, atliekant reguliarius jos patikrinimus pagal įrangos gamintojo pateiktas specifikacijas, o įrangos priežiūrą gali atlikti tik tinkamą kompetenciją turintys specialistai.

66. Stacionariai Telšių PSPC įrangai, kuri yra ne Telšių PSPC patalpose, turi būti užtikrinama ne žemesnio lygio sauga kaip ir įrangai, kuri yra Telšių PSPC patalpose.

67. Telšių PSPC įrangos, kuri yra laikoma Paslaugų teikėjų patalpose, saugumas turi būti užtikrinamas įtraukiant informacijos saugos reikalavimus į sutartį su Paslaugų teikėju. Paslaugų teikėjo atsakomybė ir įsipareigojimai įtvirtinami sutartyje vadovaujantis Reglamento (ES) 2016/679 nuostatomis.

68. Nebenaudotina stacionari įranga turi būti saugiai sunaikinama, užtikrinant, kad joje esantys asmens duomenys yra sunaikinti ir negali būti atkurti.

69. Keičiant darbuotojo elektronines darbo priemones, informacija iš darbuotojo turėtų elektroninių darbo priemonių turi būti perkeliama į naują priemonę, o turėta įranga paruošiama pakartotiniam naudojimui.

70. Nebenaudotinos elektroninės darbo priemonės gali būti parduodamos, atiduodamos labdarai, atiduodamos sunaikinimui prieš tai įsitikinus, jog įrenginiuose buvę asmens duomenys yra sunaikinti ir negali būti atkurti.

71. Nešiojamos įrangos (elektroninių darbo priemonių) negalima palikti be priežiūros ne Telšių PSPC patalpose, išskyrus atvejus, kai nešiojama įranga paliekama saugioje ir ne visiems prieinamoje bei matomoje vietoje, pavyzdžiui, mašinos bagažinėje, užrakintame susitikimų kambaryje. Skrydžio metu įrangą privaloma laikyti rankiniame bagaže.

72. Darbuotojai turi laikytis Švaraus stalo ir Švaraus ekrano politikos.

73. Švaraus stalo politika reiškia, kad:

73.1. asmens duomenys, esantys popierinėse ar elektroninėse duomenų laikmenose, kai jie nėra naudojami darbuotojo užduotims atlikti, laikomi rakinamose spintose arba stalčiuose.

73.2. ant stalo nepaliekami atvirai matomi spausdinti dokumentai, taip pat negali būti paliekami prisijungimo prie informacinių sistemų paskyrų duomenys (prisijungimo vardai ir slaptažodžiai);

73.3. dokumentai, kuriuose yra asmens duomenų, nepaliekami prie daugiafunkcinių įrenginių (spausdintuvų, kopijavimo aparatų ir kt.);

73.4. dokumentai ir USB laikmenos su asmens duomenimis, pasibaigus susitikimui, nepaliekami susitikimų kambariuose;

73.5. iš susitikimų kambariuose esančių stacionarių kompiuterių turi būti ištrinami asmens duomenys, naudoti susitikimo metu, bei įvykdoma komanda „Logout“ išjungiant kompiuterį ar komunikacijos priemones.

74. Švaraus ekrano politika reiškia, kad:

74.1. kompiuteriai, kai jais nesinaudojama, turi būti užrakinami rankiniu būdu arba automatiškai su ekrano užsklanda. Pirmenybė teikiama automatiniam ekrano užsklandos naudojimui. Rankinis būdas gali būti naudojamas tik tada, kai nėra galimybių automatiškai naudoti ekrano užsklandą;

74.2. darbo dienos pabaigoje, pabaigus darbą, kompiuteris turi būti išjungiamas.

IX SKYRIUS
APSAUGA NUO KENKĖJIŠKOS PROGRAMINĖS ĮRANGOS

75. Telšių PSPC naudojama ugniasienė, antivirusinė, programinės įrangos kontrolės ir kita programinė įranga, skirta realiu metu stebėti, aptikti, blokuoti ir šalinti nesankcionuotą ar kenksmingą programinę įrangą. Ši įranga turi nuolat, bet ne rečiau kaip kartą per savaitę, automatiškai pasitikrinti dėl atnaujinimų gamintojo svetainėje ir informuoti administratorių apie reikšmingus įvykius. Darbuotojams draudžiama savarankiškai keisti programinės įrangos atnaujinimų nustatymus.

76. Jei suteikiama galimybė prie Telšių PSPC tvarkomų asmens duomenų jungtis nuotoliniu būdu, turi būti jungiamasi naudojant virtualų privatų tinklą (VPN).

77. Darbuotojams draudžiama leisti kitiems asmenims naudotis jiems darbo vietoje priskirta kompiuterine įranga ar savo prieigos vardu (prisijungimo vardu ir slaptažodžiu), išsinešti stacionarią kompiuterinę įrangą iš Telšių PSPC patalpų.

78. Kompiuterinėse darbo vietose antivirusinė programinė įranga turi automatiškai pradėti skenuoti į kompiuterį įdėtą išorinę duomenų laikmeną. Darbo vietų kompiuteriuose gali būti naudojamos tik darbo reikmėms skirtos išorinės duomenų laikmenos. Darbuotojams draudžiama asmeniniais tikslais asmens duomenis išsinešti už Telšių PSPC ribų išorinėse laikmenose (CD / DVD, USB, kt.).

X SKYRIUS
ATSARGINĖS KOPIJOS

79. Telšių PSPC atsarginės asmens duomenų kopijos daromos automatiškai kiekvieną dieną. Atsarginių kopijų tikslas – užtikrinti asmens duomenų prieinamumą ir vientisumą.

80. Asmens duomenys atsarginėse kopijose turi būti užšifruoti arba būtina imtis kitų priemonių duomenų saugumui užtikrinti.

81. Atsarginės kopijos turi būti saugomos kitame pastate, nei yra įrenginiai, kurių elektroninė informacija buvo nukopijuota.

XI SKYRIUS
SU SAUGUMU SUSIJUSIŲ ĮVYKIŲ REGISTRAVIMAS IR STEBĖSENA

82. Informacijos saugos įvykiai informacinėse sistemose turi būti registruojami. Siekiant užtikrinti, kad visi informacinių sistemų nesklandumai būtų nustatyti, yra naudojami įvykių, veiksmų ir klaidų registravimo žurnalai, įtraukiant įvykių datą, laiką ir įvykio informaciją. Prisijungimai prie informacinių sistemų (kas ir kada jungėsi, kokius pakeitimus ar kitus veiksmus atliko) protokoluojami pagal konkrečios sistemos funkcines galimybes ir saugomi ne mažiau kaip 6 mėnesius.

83. Įvykių žurnaluose yra asmens duomenų, todėl jiems yra taikomos atitinkamos organizacinės ir techninės saugumo priemonės.

84. Tarnybinių stočių saugumo įvykių žurnalai turi būti reguliariai peržiūrimi bent kartą per mėnesį.

85. Privilegijuotiems naudotojams (administratoriams) draudžiama trinti ar deaktyvuoti savo veiklos įrašus.

86. Visų Telšių PSPC naudojamų informacijos apdorojimo sistemų laikrodžiai privalo būti sinchronizuoti pagal tikslų laiko šaltinį. Tarnybinėse stotyse ir kompiuteriuose laikas sinchronizuojamas nustatytais laiko intervalais siunčiant užklausas į tinklo laiko protokolo (angl. Network Time Protocol) serverius.

XII SKYRIUS
INFORMACINIŲ SISTEMŲ VALDYMO PRIEMONĖS

87. Serverių operacinės sistemos ir įdiegtos programinės įrangos atnaujinimas vykdomas ne darbo metu numatytomis techninio aptarnavimo valandomis, prieš tai informavus Telšių PSPC darbuotojus. Prieš serverių atnaujinimą būtina išsaugoti rezervinę serveriuose saugomos informacijos kopiją.

88. Darbo vietų kompiuterių operacinių sistemų atnaujinimas atliekamas centralizuotai ir, jei techniškai įmanoma, automatiškai, prieš tai apie keitimo poveikį darbui informavus darbuotojus.

89. Darbo vietų kompiuteriai privalo būti reguliariai perkraunami, kad įsigaliotų įdiegti atnaujinimai.

90. Atnaujinimai diegiami tik atlikus išsamų bei sėkmingą testavimą dėl pakeitimo poveikio operacinei sistemai, naudotojo sąsajai ir kitoms įdiegtoms informacinėms sistemoms.

XIII SKYRIUS
TECHNINIŲ PAŽEIDŽIAMUMŲ VALDYMAS

91. Reguliariai turi būti atliekamas Telšių PSPC IT infrastruktūros techninio pažeidžiamumo vertinimas.

92. Techninio pažeidžiamumo vertinimo metu nustatyti trūkumai, priklausomai nuo kritiškumo, turi būti šalinami nedelsiant arba sudaromas trūkumų šalimo priemonių planas, numatomi trūkumų šalinimo terminai, paskiriami atsakingi asmenys ir biudžetas.

93. Darbuotojams draudžiama darbo vietų kompiuteriuose savo nuožiūra diegti programinę įrangą.

94. Esant poreikiui darbo vietos kompiuteryje įdiegti nestandartinę programinę įrangą, darbuotojas turi kreiptis į IT saugos įgaliotinį, kuris, įvertinęs su konkrečia programine įranga susijusią riziką, suteiks leidimą ją įdiegti (įdiegs) arba pasiūlys naudoti alternatyvų sprendimą.

95. Nestandartinė programinė įranga gali būti diegiama tik atlikus išsamų bei sėkmingą jos poveikio operacinei sistemai, naudotojo sąsajai, kitoms informacinėms sistemoms testavimą.

XIV SKYRIUS
TINKLO SAUGUMAS

96. Kiekvienas naujas prie tinklo prijungiamas informacijos apdorojimo įrenginys turi atitikti šiuos minimalius saugumo reikalavimus:

96.1. turi būti naudojama gamintojo palaikoma sisteminė programinė įranga;

96.2 turi būti įdiegta apsauga nuo kenkėjiško programinio kodo;

96.3. pirmo prisijungimo prie kompiuterinės darbo vietos metu sistema automatiškai turi paprašyti naudotojo pasikeisti administratoriaus suteiktą slaptažodį.

XV SKYRIUS
ASMENS DUOMENŲ PERDAVIMAS

97. Perduodant asmens duomenis elektroniniu būdu, turi būti naudojami saugūs informacijos perdavimo kanalai ir laikmenos:

97.1. perduodant asmens duomenis elektroniniu paštu, naudojama darbinė elektroninio pašto dėžutė. Perduodant specialių kategorijų asmens duomenis, jie turi būti šifruojami arba turi būti taikomos kitos konfidencialumą užtikrinančios priemonės.

97.2. naudojant Telšių PSPC išduotas informacijos laikmenas: CD / DVD, USB atmintines. Informacijos laikmenose esantys asmens duomenys turi būti užšifruoti arba taikomi slaptažodžiai.

98. Asmens duomenys gali būti perduodami ir popierinėje formoje, užtikrinant, jog ji yra perduodama tiesiogiai klientui, naudojantis patvirtintomis informacijos perdavimo paslaugomis: asmeniškai; registruotu laišku; per kurjerius.

99. Kitų elektroninės informacijos apsikeitimo platformų naudojimas galimas tik įsitikinus jų patikimumu.

100. Sutartyse su trečiosiomis šalimis turi būti numatomi tinkami apsikeitimo asmens duomenimis būdai ir su tuo susiję saugumo reikalavimai.

101. Asmeninės elektroninio pašto dėžutės, socialinių tinklų platformų naudojimas susirašinėjimui darbo tikslais yra draudžiamas.

102. Su trečiosiomis šalimis privaloma pasirašyti konfidencialumo susitarimus arba atitinkamas nuostatas įtraukti į sutartis. Su Telšių PSPC darbuotojais, tvarkančiais asmens duomenis ar galinčiais su jais susipažinti, pasirašomi konfidencialumo pasižadėjimai.

103. Už konfidencialumo užtikrinimo procesų koordinavimą bei priežiūrą yra atsakingas Telšių PSPC direktorius ar kitas jo įgaliotas asmuo.

XVI SKYRIUS
INFORMACINIŲ SISTEMŲ KŪRIMO IR PRIEŽIŪROS PROCESŲ SAUGUMAS

104. Naujų informacinių sistemų ar funkcionalumų kūrimas turi vykti saugioje, nuo eksploatavimo atskirtoje aplinkoje.

105. Visi pakeitimai ir pakeitimų prašymai turi būti registruojami, fiksuojant jų statusų pakeitimus, statusų pakeitimo autorius bei laiką.

106. Prieš vykdant informacinių sistemų pakeitimus turi būti užtikrinama, kad pakeitimai yra apsvarstyti, ištestuoti bei patvirtinti, kad jie būtų įdiegti tinkamai ir nesukeltų neigiamo poveikio darbui ar informacinėms sistemoms.

107. Visi pakeitimai turi būti diegiami iš anksto numatytu ir suderintu laiku, siekiant kuo mažiau trukdyti Telšių PSPC veiklai.

108. Apie pakeitimų, kurie gali turėti įtakos informacinių sistemų ar jų naudotojų darbui, diegimą turi būti informuojami naudotojai.

109. Prieš diegiant pakeitimą turi būti įsitikinama, jog susidarius nenumatytoms aplinkybėms, bus galima atstatyti iki pakeitimo buvusius funkcionalumus ir užtikrinti Telšių PSPC veiklos tęstinumą.

110. Už tinkamą pakeitimo diegimą atsakingas IT saugos įgaliotinis.

111. Prieš priimant sukurtą informacinę sistemą turi būti atliekamas sistemos priėmimo testavimas.

112. Priėmimo testavimo metu yra testuojamas informacijos saugos atitikimas reikalavimams bei informacinės sistemos atitikimas specifikacijai.

113. Už diegiamos sistemos saugumo testavimo procesus atsakingas IT saugos įgaliotinis.

114. Atliekant testavimą, neturi būti naudojami asmens duomenys. Jeigu tokie duomenys yra būtini testavimo atlikimui, turi būti užtikrinama, jog jie yra pakeičiami, užmaskuojami, o atlikus testavimą ištrinami iš testavimo aplinkos.

XVII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

115. Organizacinių ir techninių saugumo priemonių efektyvumas reguliariai (ne rečiau kaip kartą per dvejus metus) peržiūrimas. Nustatyti trūkumai, priklausomai nuo kritiškumo, yra šalinami nedelsiant arba sudaromas trūkumų šalimo priemonių planas, paskiriami atsakingi asmenys ir biudžetas.

116. Aprašas peržiūrimas ir prireikus atnaujinamas ne rečiau kaip kartą per metus.

117. Telšių PSPC darbuotojai su Aprašu supažindinami pasirašytinai.

118. Darbuotojams, tvarkantiems asmens duomenis, periodiškai (ne rečiau kaip kartą per metus) organizuojami asmens duomenų apsaugos ir saugumo mokymai.

_____

Organizacinių ir techninių asmens duomenų saugumo priemonių įgyvendinimo tvarkos aprašo priedas

(IT išteklių, naudojamų asmens duomenims tvarkyti, registro forma)

IT IŠTEKLIŲ, NAUDOJAMŲ ASMENS DUOMENIMS TVARKYTI, REGISTRAS

Eil. Nr.	Įrangos tipas	Pavadinimas	Vieta	Naudotojas / atsakingas asmuo
Techninė įranga				
1.				
2.				
3.				
4.				
Programinė įranga				
5.				
6.				
7.				
8.				
Tinklo įranga				
9.				
10.				
11.				
12.				

_____