PATVIRTINTA
VšĮ Raseinių psichikos sveikatos centro
direktoriaus 2021 m. gruodžio 27 d.
įsakymu Nr. V-39

VIEŠOSIOS ĮSTAIGOS RASEINIŲ PSICHIKOS SVEIKATOS CENTRO INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. VšĮ Raseinių psichikos sveikatos centro (toliau – Įstaiga) valdomos ir tvarkomos informacinės sistemos (toliau – Informacinė sistema arba IS) saugaus elektroninės informacijos tvarkymo taisyklių (toliau - Taisyklės) tikslas – nustatyti elektroninės informacijos tvarkymo, techninius ir kitus elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus.

2. Taisyklės parengtos vadovaujantis šiais teisės aktais:

2.1. Lietuvos Respublikos kibernetinio saugumo įstatymu;

2.2. Bendrųjų elektroninės informacijos saugos reikalavimų 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“;

2.3. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

2.4. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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) (toliau – Reglamentas (ES)2016/679);

2.5. Lietuvos Respublikos Sveikatos apsaugos ministro 2021 m. rugpjūčio 30 d. V-1959 įsakymu „Dėl sveikatos priežiūros įstaigos informacinės sistemos pavyzdinių saugaus elektroninės informacijos tvarkymo taisyklių, sveikatos priežiūros įstaigos informacinės sistemos pavyzdinių naudotojų administravimo taisyklių ir sveikatos priežiūros įstaigos informacinės sistemos pavyzdinio veiklos tęstinumo valdymo plano patvirtinimo“.

2.6. kitais teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

3. Taisyklėse vartojamos sąvokos:

3.1. **Elektroninė informacija** – visa Įstaigos informacija, kuri tvarkoma informacinių technologijų priemonėmis.

3.2. **Informacinė sistema** – apima visus Įstaigos serverius ir naudotojo įrenginius, kaip kompiuteriai, telefonai, planšetės, išorinės laikmenos, tinklo infrastruktūra, sisteminė (operacinės sistemos, archyvavimo programinė įranga, kt.) ir taikomoji programinė įranga (biuro programų paketai, specializuota programinė įranga, kt.), duomenys, kiti kompiuteriniai komponentai ar sistemos, kurie priklauso Įstaigai ar yra naudojami Įstaigos reikmėms. Tokioms informacinėms sistemoms priklauso visos vidinės ir išorinės paslaugos, kaip Interneto prieiga, elektroninis paštas, komunikacijos priemonės.

3.3.**Informacijos sauga** – Informacijos konfidencialumo, vientisumo ir pasiekiamumo išsaugojimas.

3.4.**Informacijos saugos įgaliotinis** - Įstaigos vadovo paskirtas darbuotojas, administruojantis Informacijos saugos klausimus Įstaigoje.

3.5. **Informacinės sistemos administratorius** – Įstaigos vadovo paskirtas darbuotojas ar paslaugų teikėjas, su kuriuo pasirašyta sutartis, administruojantis Informacines sistemas.

3.6. **Naudotojas –** Įstaigos darbuotojas, rangovas ar kitas trečias asmuo, kuriam teisėtai suteikta prieiga prie Įstaigos Informacinių sistemų.

3.7. kitos taisyklėse vartojamos sąvokos atitinka šių taisyklių 2 punkte nurodytuose teisės aktuose nustatytas sąvokas.

4. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

4.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti Įstaigos Elektroninę informaciją;

4.2. užtikrinti, kad Elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

4.3. vykdyti Elektroninės informacijos saugos (kibernetinių) incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į Elektroninės informacijos saugos (kibernetinius) incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

5. IS elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų IS elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė;

5.2. IS elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.3. IS tvarkymo kontrolė;

5.4. IS paslaugų ir naudojimosi IS Elektronine informacija kontrolės užtikrinimas;

5.5. IS tvarkomų asmens duomenų apsauga;

5.6. IS veiklos tęstinumo užtikrinimas;

5.7. IS naudotojų mokymas.

6. Įstaiga atsako už Elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir politikos įgyvendinimo organizavimą, priežiūrą ir Elektroninės informacijos tvarkymo teisėtumą.

II. FIZINĖS, TECHNINĖS IR ORGANIZACINĖS SAUGOS PRIEMONĖS

7. Saugiam IS Elektroninės informacijos tvarkymui užtikrinti naudojamos fizinės, techninės ir organizacinės duomenų saugos priemonės.

8. Kompiuterinės įrangos apsaugos priemonės:

8.1. prieigos teisės prie IS tarnybinių stočių, kontrolė užtikrinama, prieigos teises suteikiant tik Informacinės sistemos administratoriui;

8.2. Svarbiausios kompiuterinės įrangos sujungimas klasteriniu rėžimu, dubliuojant svarbiausią kompiuterinę įrangą, vykdoma šios kompiuterinės įrangos techninės būklės nuolatinė stebėsena;

8.3. tarnybinės stotys maitinamos per nepertraukiamą maitinimo šaltinį su įtampos reguliavimo funkcija ir baterija, užtikrinančia sistemos veikimą bent 10 min. ir programine valdymo įranga, išjungiančia tarnybines stotis, neatkūrus maitinimo per šį laiką;

8.4. garantuojama visos IS kompiuterių techninės įrangos gamintojo garantinė priežiūra, o po garantiniu laikotarpiu Informacinės sistemos administratoriaus arba išorinių priežiūros paslaugų teikėjų priežiūra;

8.5. fizinė prieiga prie IS tarnybinių stočių kontroliuojama ir ribojama (atskiros rakinamos patalpos arba rakinama spinta);

8.6. patalpose, kuriose yra laikomos IS tarnybinės stotys, yra gaisro ir įsilaužimo saugumo davikliai, kondicionavimo sistema;

8.7. daromos atsarginės Informacinės sistemos elektroninės informacijos kopijos, kurios saugomos kitoje patalpoje ar geografinėje vietoje negu aktyvi (veikianti) duomenų bazė;

8.8. Informacinės sistemos vidinių elektroninių duomenų perdavimo tinklas atskirtas nuo viešųjų telekomunikacinių tinklų, naudojant užkardą;

8.9. Informacinės sistemos kompiuterių aparatinės įrangos keitimas gali būti atliekamas tiktai gavus Informacinės sistemos administratoriaus leidimą;

8.10. visi tarnybinių stočių techninės įrangos gedimai ir keitimai registruojami žurnale;

8.11. Informacinės sistemos administratorius gauna perspėjimą, kai Informacinės sistemos tarnybinėse stotyse iki nustatytos pavojingos ribos sumažėja laisvos operatyviosios atminties ar vietos diske (diskuose) ar duomenų saugykloje, ilgą laiką stipriai apkraunamas centrinis procesorius ir/ar tinklo sąsaja.

9. Sisteminės ir taikomosios programinės įrangos apsaugos priemonės:

9.1. naudojama tiktai legali ir įteisinta Informacinės sistemos sisteminė ir taikomoji programinė įranga;

9.2. programinės įrangos diegimą atlieka tik Įstaigos įgalioti asmenys;

9.3. IS sisteminės ir taikomosios programinės įrangos apsaugai nuo virusų ir kitų kenkėjiškų programų naudojama specializuota, nuolat automatiškai atnaujinama programinė įranga;

9.4. kiekvienas Informacinės sistemos naudotojas sistemoje unikaliai identifikuojamas - savo tapatybę patvirtinta naudotojo vardu ir slaptažodžiu, jų atlikti veiksmai su Informacinės sistemos fiksuojami elektroniniuose žurnaluose;

9.5. Informacinės sistemos administravimo ir priežiūros funkcijos atliekamos naudojant atskirą tam skirtą administratoriaus identifikatorių, kuriuo naudojantis negalima atlikti Informacinės sistemos naudotojo funkcijų;

9.6. Informacinės sistemos naudotojo teisė naudotis sistema panaikinama pasibaigus darbo santykiams;

9.7. Siekiant, kad su Informacinėje sistemoje saugoma elektronine informacija ir asmens duomenimis negalėtų susipažinti pašaliniai asmenys, imamasi šių priemonių:

9.7.1. baigus darbą ar pasitraukiant iš Informacinės sistemos darbo vietos turi būti: atsijungiama nuo Informacinės sistemos, įjungiama ekrano užsklanda su slaptažodžiu;

9.7.2. Informacinės sistemos naudotojui 15 min. nesinaudojant Informacine sistema, sesija yra automatiškai nutraukiama ir, norint pratęsti darbą su Informacine sistema, reikia iš naujo patvirtinti Informacinės sistemos naudotojo tapatybę;

9.7.3. Papildomos taikomos saugos priemonės nustatytos Informacinės sistemos naudotojų administravimo taisyklėse.

9.8. Informacinės sistemos sisteminės ir taikomosios programinės įrangos keitimas bei atnaujinimas gali būti atliekamas tik gavus Informacinės sistemos administratoriaus leidimą;

9.9. visi Informacinės sistemos kompiuterių sisteminės ir taikomosios programinės įrangos keitimai bei atnaujinimai registruojami žurnale.

10. Saugumo užtikrinimo elektroninės informacijos perdavimo tinklais priemonės:

10.1. Informacinės sistemos duomenys, siunčiami per viešuosius tinklus yra šifruojami;

10.2. viešai prieinama Informacinės sistemos elektroninė informacija saugoma atskirame kompiuterių potinklyje - DMZ (angl. demilitarized zone).

11. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

11.1. užtikrinamas išorės poveikio šaltinių - transporto priemonių keliamos vibracijos, eismo įvykių, radijo stočių, kitų išorės šaltinių minimalus poveikis patalpoms ir jose esančiai Informacinės sistemos techninei ir programinei įrangai;

11.2. patalpose įrengta fizinė apsauga: rakinamos durys, veikia signalizacija;

11.3. patalpos atitinka priešgaisrinės saugos reikalavimus, jose yra gaisro gesinimo priemonės. Periodiškai atliekama gaisro gesinimo priemonių patikra;

11.4. patalpose įrengti įsilaužimo davikliai;

11.5. patalpos atskirtos nuo bendrojo naudojimo patalpų, asmenys patekti į šias patalpas gali tik lydimi Informacinės sistemos administratoriaus;

11.6. asmenys, norintys patekti į tarnybinių stočių patalpas, užregistruojami;

11.7. techninė įranga įnešama ir išnešama iš patalpų tik leidus Informacinės sistemos administratoriui;

11.8. techninė įranga apsaugoma nuo elektros srovės svyravimų, nuo neteisėtos prieigos prie techninės įrangos, jos sugadinimo ar neteisėto poveikio jai;

11.9. ryšių kabeliai apsaugoti nuo neteisėto prisijungimo prie jų ir jų pažeidimo;

11.10. įgyvendintos gamintojo nustatytos techninės įrangos darbo sąlygos;

11.11. Informacinės sistemos tarnybinių stočių patalpose įrengtas nuolatinis oro temperatūros palaikymas.

12. Darbo apskaitos ir kitos elektroninės informacijos saugos priemonės:

12.1. programiniu būdu registruojami IS naudotojų veiksmai su IS Elektronine informacija;

12.2. Informacinės sistemos naudotojams suteikiama prieigos prie Informacinės sistemos teisė atlikti veiksmus tik su jiems priskirtais duomenimis;

12.3. Informacinės sistemos tarnybinių stočių įvykių žurnaluose registruojami ir ne mažiau kaip 1 (vienerius) metus saugomi duomenys, nurodant įvykio laiką ir naudotojo identifikatorių, apie:

12.3.1. tarnybinių stočių įjungimą bei išjungimą;

12.3.2. sėkmingus ir nesėkmingus bandymus registruotis prie Informacinės sistemos;

12.3.3. bandymus prieiti prie Informacinės sistemos informacinių išteklių;

12.3.4. kitus svarbius Informacinėje sistemoje saugomos ir apdorojamos elektroninės informacijos saugai įvykius.

III. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

13. Informacinės sistemos saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka:

13.1. Elektroninė informacija į IS gali būti įvedama, joje keičiama, atnaujinama ir naikinama tik Taisyklių, kitų teisės aktų, reglamentuojančių saugų Elektroninės informacijos tvarkymą, nustatyta tvarka;

13.2. Elektroninė informacija gali būti tvarkoma pagal IS naudotojams ir IS administratoriams suteiktas prieigos teises ir tik turint teisėtą tikslą ir pagrindą;

14. Informacinės sistemos naudotojų veiksmų registravimo tvarka:

14.1. IS naudotojų tapatybė ir veiksmai su Informacinės sistemos duomenimis fiksuojami programinėmis priemonėmis;

14.2. IS naudotojų tapatybė ir veiksmai su IS duomenimis įrašomi automatiniu būdu Informacinės sistemos duomenų bazės veiksmų žurnale, apsaugotame nuo neteisėto jame esančių duomenų panaudojimo, pakeitimo, iškraipymo ar sunaikinimo;

14.3. IS duomenų bazės veiksmų žurnalo duomenys prieinami Informacinės sistemos administratoriui bei atitinkamas teises turintiems Informacinės sistemos naudotojams.

15. Atsarginių Informacinės sistemos elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka:

15.1. už Informacinės sistemos elektroninės informacijos atsarginių kopijų darymą ir atkūrimą yra atsakingas Informacinės sistemos administratorius.

15.2. prarasti, iškraipyti ar sunaikinti IS duomenys atkuriami iš IS elektroninės informacijos atsarginių kopijų;

15.3. atsarginės Informacinės sistemos elektroninės informacijos kopijos daromos periodiškai. Kartą per savaitę daroma rezervinė bazių ir failų duomenų kopija.

15.4. atsarginėse kopijos, archyvuose ir išorinės duomenų laikmenos saugomi asmens duomenys yra šifruojami;

15.5. siekiant įsitikinti, jog rezervinė kopija yra nesugadinta, po kiekvienos rezervinio

kopijavimo procedūros atliekamas patikrinimas.

15.6. atkūrimas iš atsarginių kopijų periodiškai išbandomas – ne rečiau kaip kartą per metus.

16. Saugaus Informacinės sistemos elektroninės informacijos perkėlimo ir teikimo susijusioms informacinėms sistemoms, elektroninės informacijos gavimo iš jų užtikrinimo tvarka:

16.1. už elektroninės informacijos, teikiamos iš kitų informacinių sistemų, atnaujinimą Informacinėje sistemoje yra atsakingas Informacinės sistemos administratorius.

16.2. duomenų mainai tarp Informacinės sistemos ir kitų informacinių sistemų vykdomi su šių informacinių sistemų valdytojais sudarytose elektroninės informacijos teikimo sutartyse numatytais būdais, terminais ir numatytos apimties;

17. Informacinės sistemos elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

17.1. Informacinės sistemos administratorius, užtikrindamas Informacinės sistemos elektroninės informacijos vientisumą, privalo naudoti visas įmanomas fizines, programines ir organizacines priemones, skirtas Informacinėje sistemoje tvarkomiems duomenims apsaugoti nuo neteisėtų veiksmų;

17.2. siekiant patikrinti, ar su Informacinės sistemos duomenimis nėra vykdoma neleidžiama veikla, Informacinės sistemos administratorius kiekvieną darbo dieną privalo peržiūrėti programinės įrangos elektroniniuose žurnaluose sukauptus atitinkamus įrašus;

17.3. Informacinės sistemos naudotojas, pastebėjęs Taisyklėse nustatytų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones arba įtaręs, kad su IS duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai Informacinės sistemos administratoriui. Informacinės sistemos administratorius, atsiradus įtarimams dėl neteisėtų veiksmų su Informacinės sistemos duomenimis, pasinaudojęs Informacinės sistemos duomenų bazės veiksmų žurnalo įrašais, nustato neteisėto poveikio šaltinį, laiką ir veiksmus, atliktus su Informacinės sistemos programine įranga ir (ar) duomenimis;

17.4. Informacinės sistemos administratorius, įtaręs, kad Informacinės sistemos naudotojo pastebėti pažeidimai yra pagrįsti, privalo apie tai pranešti Informacijos saugos įgaliotiniui.

17.5. Informacijos saugos įgaliotinis, gavęs pranešimą apie vykdomus neteisėtus veiksmus su Informacine sistema arba su Informacinėje sistemoje tvarkomais duomenimis, inicijuoja elektroninės informacijos saugos incidento valdymo procedūras, kaip nustatyta Informacinės sistemos veiklos tęstinumo valdymo plane.

18. Informacinės sistemos pokyčių valdymo tvarka apima šiuos procesus:

18.1. pokyčių identifikavimą;

18.2. pokyčių skirstymą į kategorijas, atsižvelgiant į pokyčių svarbą, aktualumą, poreikį ir pan.;

18.3. pokyčių įtakos vertinimą;

18.4. pokyčių prioritetų nustatymą;

18.5. pokyčių atlikimą.

19. IS pokyčių valdymo tvarkos detalizavimas:

19.1. pokyčius inicijuoti gali Informacijos saugos įgaliotiniai ir Informacinės sistemos administratorius;

19.2. pokyčiai gali būti inicijuojami identifikavus Informacinės sistemos veikimo netikslumus, iškilus naujoms saugumo Informacinės sistemos grėsmėms, siekiant gerinti Informacinės sistemos našumą ir pan.;

19.3. užregistruoti pokyčiai skirstomi į kategorijas pagal svarbą, aktualumą, poreikį siekiant nustatyti įgyvendinimo eiliškumą;

19.4. tarpusavyje nesusiję pokyčiai vienu metu neįgyvendinami;

19.5. prioritetiniais laikomi pokyčiai susiję su duomenų apsauga, Informacinės sistemos saugumu;

19.6. įvertinamos pokyčių keliamos rizikos, įskaitant poveikį duomenų saugumui, poveikį

Informacinės sistemos saugumui, funkcionalumui ir pan.;

19.7. pokyčiai planuojami ir testuojami naudojant atskirą testavimui skirtą aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu bei 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);

19.8. nustatomas galimas Informacinės sistemos neveikimo terminas pokyčių diegimo metu;

19.9. patvirtinus sėkmingo testavimo rezultatus, diegimui gamybinėje aplinkoje turi būti paruoštas diegimo paketas, numatytos diegimo procedūros;

19.10. turi būti numatytos atstatomosios / grįžtamosios procedūros nesėkmingų pokyčių diegimų atvejais;

19.11. įgyvendinant pokyčius, kurių metu galimi Informacinės sistemos veikimo sutrikimai, Informacinės sistemos administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki planuojamų pokyčių vykdymo pradžios informuoti Informacinės sistemos naudotojus apie tokių darbų pradžią, numatomą trukmę ir galimus sutrikimus;

19.12. jei įdiegti pokyčiai turi įtakos Informacinės sistemos naudotojų darbui (keičiasi Informacinės sistemos funkcionalumai, naudojimo tvarka), su informacija apie pasikeitimus supažindinamos visos suinteresuotos šalys.

20. Nešiojamųjų kompiuterių ir mobiliųjų įrenginių naudojimo tvarka:

20.1. išvežti iš patalpų nešiojamieji kompiuteriai negali būti palikti be priežiūros viešose vietose;

20.2. nešiojamieji kompiuteriai turi būti apsaugoti slaptažodžiais, juose esanti informacija turi būti šifruojama. Jei įmanoma, turi būti aktyvuotas nešiojamojo kompiuterio BIOS slaptažodis. Kompiuterio išdavimo metu, naudotojas turi nedelsiant pasikeisti standartinį ar prieš tai nustatytą slaptažodį;

20.3. prieš perduodant nešiojamąjį kompiuterį Informacinės sistemos naudotojui, jis turi būti patikrinamas antivirusine programine įranga;

20.4. nešiojamojo kompiuterio grąžinimas ir antivirusinės programos tikrinimo rezultatai turi būti registruojami žurnale;

20.5. nešiojami kompiuteriai turi būti apsaugoti ekrano atrakinimo slaptažodžiu, arba biometrinėmis apsaugomis priemonėmis (pvz. piršto skenavimas);

20.6. jei nešiojamojo įrenginio operacinės sistemos funkcionalumas suteikia tokią galimybę, turi būti įjungta įrenginio nuotolinio atminties ištrynimo bei gamyklinių parametrų atstatymo funkcija.

21. Belaidžio tinklo saugumas ir kontrolė:

21.1. belaidės prieigos taškai diegiami tik atskirame potinklyje, kontroliuojamoje zonoje;

21.2. atliekami tikrinimai Informacinės sistemos infrastruktūroje ar nėra eksploatuojami neleistini ar techninių kibernetinio saugumo reikalavimų neatitinkantys belaidžiai įrenginiai;

21.3. Prisijungiant prie belaidžio tinklo, taikomas ryšių ir informacinių sistemų naudotojų tapatumo patvirtinimo EAP (angl. Extensible Authentication Protocol) / TLS (angl. Transport Layer Security) protokolas;

21.4. Belaidėje sąsajoje uždrausta naudoti SNMP (angl. Simple Network Management Protocol) protokolą, uždrausti visi nebūtini valdymo protokolai, išjungti nenaudojami TCP (angl. Transmission Control Protocol) / UDP (angl. User Datagram Protocol) prievadai;

21.5. uždraustas lygiarangis (angl. peer to peer) funkcionalumas, neleidžiantis belaidžiais įrenginiais palaikyti ryšį tarpusavyje

21.6. belaidis ryšys turi šifruojamas mažiausiai 128 bitų ilgio raktu, pakeisti belaidės prieigos stotelėje standartiniai gamintojo raktai;

21.7. Kompiuteriuose, mobiliuosiuose įrenginiuose išjungta belaidė prieiga, jeigu jos nereikia darbo funkcijoms atlikti, išjungtas lygiarangis (angl. peer to peer) funkcionalumas, belaidė periferinė

prieiga.

IV. REIKALAVIMAI INFORMACINĖS SISTEMOS FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

22. Paslaugų teikėjų prieigos prie Informacinės sistemos lygiai ir sąlygos:

22.1. Informacinės sistemos administratorius suteikia prieigos prie Informacinės sistemos elektroninės informacijos teisę (peržiūrėti Informacinės sistemos duomenis, atlikti užklausas Informacinėje sistemoje, vykdyti veiksmus su Informacinės sistemos duomenimis ir kt.) ir fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nurodytam laikotarpiui jam nustatytoms funkcijoms atlikti;

22.2. Informacinės sistemos administratorius, suteikdamas prieigos prie Informacinės sistemos elektroninės informacijos teisę, paslaugų teikėjo įgaliotą fizinį asmenį supažindina su prieigos prie Informacinės sistemos elektroninės informacijos sąlygomis;

22.3. pasibaigus sutartyje nurodytam laikotarpiui, Informacinės sistemos administratorius panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie Informacinės sistemos elektroninės informacijos teisę ir apie tai jį informuoja sutartyje numatytu būdu.

22.4. Įsigyjant viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugas, elektroninės informacijos prieglobos paslaugas, skaitmenines paslaugas, jų teikėjams taikomi reikalavimai, nustatyti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimai). Pirkimo dokumentuose turi būti nustatyta, kad paslaugų teikėjo teikiamos paslaugos turi atitikti Organizacinių ir techninių kibernetinio saugumo reikalavimus.

23. Sutartyje su paslaugų teikėju, aprašant prieigą prie Informacinės sistemos elektroninės informacijos, jos apdorojimą, perdavimą ar valdymą, turi būti numatyti elektroninės informacijos saugos reikalavimai, apimantys (neapsiribojant):

23.1. informacijos saugumo nuostatas;

23.2. vertybių apsaugai užtikrinti reikalingas saugumo priemones;

23.3. užtikrinimą, kad paslaugų teikėjo susiję darbuotojai supranta saugumo reikalavimus ir savo atsakomybę;

23.4. keitimų valdymo procedūrą;

23.5. prieigos prie elektroninės informacijos nuostatas;

23.6. informavimo apie saugumo incidentus ir spragas tvarką;

23.7. priimtino ir nepriimtino paslaugų teikimo lygio apibrėžimą;

23.8. šalių atsakomybę;

23.9. intelektinės nuosavybės teises ir autorių teisių perdavimo aspektus.

23.10. Asmens duomenų apsaugos reikalavimus.

24. Reikalavimai keliami patalpoms, įrangai, informacinių sistemų priežiūrai, elektroninės informacijos perdavimui tinklams ir kitoms paslaugoms:

24.1. visų Informacinės sistemos veiklą palaikančių sistemų (elektros energijos, vandens tiekimo, nuotekų šalinimo, šildymo, vėdinimo ir oro kondicionavimo) funkcionalumas, pajėgumas, patikimumas ir kitos savybės turi atitikti sistemų, kurias jos aptarnauja, reikalavimus.

24.2. Informacinės sistemos veiklą palaikančių sistemų kokybė (t. y. atitiktis keliamiems reikalavimams) turi būti reguliariai tikrinama ir išbandoma, siekiant užtikrinti šių paslaugų funkcionavimą ir sumažinti galimas šių paslaugų funkcionavimo sutrikimo pasekmes.

24.3. Informacinės sistemos veiklą palaikančių sistemų kokybės patikrinimas ir išbandymas atliekamas ne rečiau kaip kartą per metus, jį inicijuoja Informacinės sistemos administratorius.

V. BAIGIAMOSIOS NUOSTATOS

25. Informacijos saugos įgaliotinis, Informacinės sistemos administratorius ir naudotojai, pažeidę Informacinės sistemos elektroninės informacijos saugą reglamentuojančių dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.