PATVIRTINTA
VšĮ Klaipėdos rajono savivaldybės
Gargždų ligoninės vyr. gydytojos
2019 m. kovo 27 d. įsakymu Nr. 25

VŠĮ KLAIPĖDOS RAJONO SAVIVALDYBĖS GARGŽDŲ LIGONINĖS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės (toliau – Įstaiga) informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės tvarkomos elektroninės informacijos saugos tikslus, elektroninės informacijos saugos užtikrinimo prioritetines kryptis, saugų elektroninės informacijos valdymą, organizacinius, techninius ir personalui keliamus reikalavimus, naudotojų supažindinimo su saugos dokumentais principus, apibrėžia elektroninės informacijos saugos politiką.

2. Šiuose Saugos nuostatuose vartojamos sąvokos:

2.1. **IT sistemos tvarkytojas** - VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės paskirtas darbuotojas ar įmonė, prižiūrinti Įstaigos IT ūkį, elektroninės informacijos saugos politikos įgyvendinimą bei užtikrinanti VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės kibernetinę saugą;

2.2. **Sistemos naudotojas** – darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės ištekliais numatytoms funkcijoms atlikti.

3. VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės tvarkomos elektroninės informacijos saugos užtikrinimo tikslas – sudaryti sąlygas saugiai automatizuotu būdu tvarkyti ir saugoti elektroninę informaciją Įstaigoje, užtikrinti elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

4. VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės informacijos saugumui užtikrinti naudojamos organizacinės, techninės, programinės ir fizinės informacijos apsaugos priemonės.

5. Įstaigos elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. Įstaigos elektroninės informacijos konfidencialumo užtikrinimas;

5.2. Įstaigos elektroninės informacijos vientisumo užtikrinimas;

5.3. Įstaigos elektroninės informacijos prieinamumo užtikrinimas;

5.4. Prieigos prie Įstaigos elektroninių duomenų kontrolė;

5.5. Įstaigos rizikos valdymas;

5.6. Įstaigos veiklos tęstinumo užtikrinimas;

5.7. Įstaigos tvarkomų asmens duomenų apsauga;

5.8. Įstaigos naudotojų saugos mokymas.

6. Saugos nuostatai taikomi:

6.1. Įstaigos, kaip informacinių sistemų ir asmens duomenų valdytojui;

6.2. Įstaigos IT sistemos tvarkytojams;

6.3. Įstaigos informacinės sistemos naudotojams;

7. **VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninė, kaip informacinių sistemų ir asmens duomenų valdytojas:**

7.1. atsako už Įstaigos saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą;

7.2. atsako už Įstaigos informacinėje sistemoje tvarkomos informacijos ir asmens duomenų tvarkymo teisėtumą ir saugumą;

7.3. užtikrina nepertraukiamą Įstaigos informacinės sistemos veikimą ir duomenų, esančių informacinės sistemos duomenų bazėse, saugumą ir saugų duomenų perdavimą kompiuterių tinklais (automatiniu būdu);

7.4. rengia ir tvirtina saugos ir kitus dokumentus, užtikrinančius Įstaigos informacinės sistemos ir duomenų tvarkymo teisėtumą, Įstaigos elektroninės informacijos saugą;

7.5. koordinuoja Įstaigos IT sistemos tvarkytojo darbą;

7.6. analizuoja IT sistemos tvarkytojo pateiktus pasiūlymus, priima sprendimus dėl Įstaigos informacinės sistemos techninių ir programinių priemonių, būtinų elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

7.7. organizuoja Įstaigos informacinės sistemos rizikos vertinimą;

8. **VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės IT sistemos tvarkytojas:**

8.1. užtikrina tinkamų organizacinių ir techninių priemonių, skirtų elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo, įgyvendinimą;

8.2. užtikrina tinkamą techninės įrangos išdėstymą ir priežiūrą, informacinių sistemų priežiūrą, tinklo valdymą, naudojimosi internetu saugumą ir kitas informacinių technologijų priemones;

8.3. užtikrinta Įstaigos informacinės sistemos techninę priežiūrą ir nepertraukiamą veikimą;

8.4. užtikrina, kad sistemos naudotojai, turintys teisę naudotis Įstaigos informacinės sistemos elektronine informacija, laikytųsi reikalavimų, nustatytų Įstaigos saugos dokumentuose;

8.5. užtikrina prieigos prie elektroninės informacijos ir asmens duomenų apsaugą, valdymą ir kontrolę;

8.6. prieigą prie elektroninės informacijos ir asmens duomenų suteikia tik tiems darbuotojams, kuriems elektroninė informacija ir asmens duomenys yra reikalingi jų funkcijoms vykdyti. Darbo santykiams pasibaigus, prieigas buvusiems darbuotojams panaikina;

8.7. užtikrina, kad su elektronine informacija ir asmens duomenimis būtų galima atlikti tik tuos veiksmus, kuriems atlikti naudotojui yra suteiktos teisės;

8.8. užtikrina elektroninės informacijos ir asmens duomenų apsaugą nuo neteisėto prisijungimo prie vidinio kompiuterinio tinklo elektroninių ryšių priemonėmis;

8.9. užtikrina kompiuterinės įrangos apsaugą nuo kenksmingos programinės įrangos (antivirusinių programų įdiegimas, atnaujinimas ir pan.).

8.10. užtikrina saugių protokolų ir (arba) slaptažodžių naudojimą, kai elektroninė informacija ir asmens duomenys perduodami išoriniais duomenų perdavimo tinklais;

8.11. užtikrina, kad informacinių sistemų testavimas nebūtų vykdomas su realiais asmens duomenimis, išskyrus būtinus atvejus, kurių metu būtų naudojamos organizacinės ir techninės asmens duomenų saugumo priemonės, užtikrinančios realių asmens duomenų saugumą;

8.12. užtikrina periodinį esminės elektroninės informacijos atsarginių kopijų sukūrimą ir esminės elektroninės informacijos atkūrimą, jos praradimo atveju;

8.13. teikia siūlymus informacinės sistemos valdytojui dėl elektroninės informacijos saugos tobulinimo, informacinės sistemos saugos dokumentų priėmimo, keitimo arba panaikinimo;

8.14. teikia siūlymus informacinės sistemos valdytojui dėl techninių ir programinių priemonių, būtinų elektroninės informacijos ir asmens duomenų saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo, organizuoja jų įdiegimą ir modernizavimą;

8.15. teikia informaciją apie informacinės sistemos saugos politikos įgyvendinimą;

8.16. koordinuoja įvykusių incidentų dėl Įstaigos elektroninės informacijos saugos tyrimą, informuoja Įstaigos vadovą apie įvykusius incidentus ir teikia pasiūlymus dėl tokių incidentų valdymo;

8.17. organizuoja Įstaigos naudotojų supažindinimą su Įstaigos saugos dokumentais;

8.18. organizuoja ir atlieka Įstaigos informacinės sistemos rizikos įvertinimą;

8.19. prižiūri Įstaigos informacinę sistemą sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų) sąranką, užtikrinant, kad ji atitiktų Įstaigos saugos dokumentų reikalavimus;

8.20. vykdo Įstaigos vadovo nurodymus ir pavedimus, susijusius su Įstaigos informacinės sistemos ir elektroninės informacijos saugos užtikrinimu;

9. **VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės sistemos naudotojas:**

9.1. atsako už Įstaigos informacinėje sistemoje tvarkomos elektroninės informacijos ir asmens duomenų saugumą. Bet kokia informacija ir duomenys, patenkantys sistemos naudotojui darbinių pareigų atlikimo metu, bus laikomi ir traktuojami kaip konfidencialūs ir saugomi duomenys pagal šiuos Saugos nuostatas; jie negali būti atskleidžiami bet kokioms trečiosioms šalims, nebent Įstaigos direktorius paskelbtų, kad tokia informacija tapo vieša arba yra kitaip perkvalifikuota į informaciją, kuriai netaikoma čia nustatyta apsauga;

9.2. neturi teisės atskleisti ar perduoti tvarkomos Įstaigos elektroninės informacijos ir asmens duomenų. Visi asmens duomenys ir kita informacija, pagal kurią galima nustatyti asmens tapatybę, renkama ir tvarkoma tik tada, kai tai reikalinga, ir tik tokia apimtimi, kokia reikalinga tam, kad sistemos naudotojas galėtų atlikti darbines funkcijas jam suteiktų įgaliojimų ribose ir prisilaikant įstatyminių reikalavimų duomenų apsaugai (ypač 2016 m. balandžio 27 d. Reglamento (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)).

9.3. duomenų subjektų – fizinių asmenų prašymus, susijusius su asmens duomenimis ir/ arba asmens duomenų tvarkymu, kuriuos sistemos naudotojas gavo vykdydamas savo darbines pareigas, turi nedelsiant perduoti duomenų apsaugos pareigūnui ar kitam, direktoriaus įsakymu paskirtam, atsakingam asmeniui, kuris nagrinės pateiktą prašymą ar skundą.

9.4. kiekvienas Įstaigos darbuotojas privalo laikytis šių duomenų saugos nuostatų, taip pat ir taikytinų vietinių, regioninių ar tarptautinių įstatymų bei taisyklių, kuriomis nustatyti informacijos/duomenų tvarkymo ir apsaugos reikalavimai. Duomenų saugos nuostatų nesilaikymas bus laikomas šiurkščiu darbo pareigų pažeidimu ir, Įstaigos pasirinkimu, gali užtraukti drausmines sankcijas arba darbuotojo atleidimą. Pažeidimą padariusiam darbuotojui, priklausomai nuo pažeidimo, gali būti taikoma administracinė arba baudžiamoji atsakomybė;

9.5. atlikti kitas Saugos nuostatų, Įstaigos asmens duomenų tvarkymo taisyklių ir kitų teisės aktų nustatytas funkcijas.

10. Teisės aktai, kuriais vadovaujamasi, tvarkant VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės elektroninę informaciją ir užtikrinant jos saugą:

10.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

10.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

10.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

10.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

10.5. Organizaciniai ir techniniai kibernetinio saugumo reikalavimai;

10.6. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtinti Valstybės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“;

10.7. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

10.8. Lietuvos standartai LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos reikalavimai“ ir kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys informacijos saugumą;

10.9. Bendrasis duomenų apsaugos reglamentas. 2016 m. balandžio 27 d. Reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB);

10.10. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugą.

II SKYRIUS

ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

11. VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės IT sistemos tvarkytojas, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, kuri skelbiama Vidaus reikalų ministerijos interneto svetainėje (http://www.vrm.lt/Rizikos_analize.pdf), Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, esant reikalui organizuoja Įstaigos rizikos įvertinimą;

12. Pasikeitus Įstaigos informacinės sistemos struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų šalinimas ir kt.) ar nustačius naujų rizikos veiksnių, Įstaigos IT sistemos tvarkytojas gali organizuoti neeilinį Įstaigos informacinės sistemos rizikos įvertinimą;

13. Įstaigos direktoriaus rašytiniu pavedimu Įstaigos rizikos įvertinimą gali atlikti pats Įstaigos IT sistemos tvarkytojas.

14. Įstaigos rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama Įstaigos direktoriui. Rizikos įvertinimo ataskaita rengiama vertinant rizikos veiksnius, galinčius turėti įtakos Įstaigos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai:

14.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

14.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis elektronine informacija, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

14.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

15. Pagrindinės nuostatos dėl rizikos veiksnių vertinimo:

15.1. Įstaigos rizikos vertinimą inicijuoja Įstaigos direktorius ar Įstaigos IT sistemos tvarkytojas;

15.2. Įstaigos rizika nustatoma rizikos vertinimo metu;

15.3. Įstaigos rizikos vertinimo dažnumą nustato Įstaigos direktorius arba IT sistemos tvarkytojas;

15.4. Įstaigos IT sistemos tvarkytojas yra atsakingas už Įstaigos rizikos vertinimo atlikimo organizavimą;

16. Įstaigos rizikos vertinimas atliekamas vadovaujantis:

16.1. Lietuvos standartu LST ISO/IEC 27001, LST ISO/IEC 27002 ir kitais Lietuvos ir tarptautiniais standartais, reglamentuojančiais rizikos vertinimą;

16.2. Įstaigos patvirtintu Kibernetinių incidentų valdymo planu.

17. Rizikos valdymo procesą sudaro:

17.1. rizikos vertinimo konteksto nustatymas, rizikos vertinimas (informacinių išteklių inventorizacija ir jų įtakos Įstaigos tvarkytojo veiklai vertinimas, rizikos analizė, rizikos įvertinimas), rizikos tvarkymas ir rizikos stebėsena ir peržiūra;

17.2. VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninė, atsižvelgdama į Įstaigos rizikos vertinimo rezultatus, prireikus tvirtina Įstaigos IT sistemos tvarkytojo parengtą rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis, priemonių vykdymo terminai ir vykdytojai rizikos valdymo priemonėms įgyvendinti;

18. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

18.1. rizika turi būti sumažinta iki priimtino lygio;

18.2. elektroninės informacijos saugos priemonės diegimo kaina turi būti proporcinga saugomos elektroninės informacijos vertei;

18.3. kur galima turi būti įdiegtos prevencines informacijos saugos priemones.

19. Įstaigos asmens duomenų apsauga turi būti užtikrinta, vadovaujantis:

19.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

19.2. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo;

19.3. Įstaigos asmens duomenų tvarkymo taisyklėmis.

20. Siekiant užtikrinti šių saugos nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per metus inventorizuojama informacinės sistemos techninė ir programinė įranga.

21. Techninės, administracinės ir kitos duomenų saugumo valdymo priemonės turi būti pasirenkamos taip, kad su kuo mažesnėmis išlaidomis būtų užtikrintas informacinės sistemos veiklos tęstinumas ir saugus naudotojų darbas.

III SKYRIUS

ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

22. Programinės įrangos, skirtos apsaugoti VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninę nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

22.1. VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninėje tarnybinių stočių ir kompiuterinėse darbo vietose esanti programinė įranga (operacinės sistemos, duomenų bazių ir aplikacijų valdymo programinė įranga, interneto naršyklės, interneto naršyklių priedai ir kt.) turi būti konfigūruojama laikantis programinės įrangos gamintojų saugaus konfigūravimo rekomendacijų. Už tarnybinių stočių programinės įrangos konfigūravimą ir kontrolę atsakingas Įstaigos paskirtas IT sistemos tvarkytojas;

22.1. Įstaigos tarnybinių stočių ir kompiuterinėse darbo vietose esanti programinė įranga turi būti atnaujinama ne vėliau kaip per 5 darbo dienas po programinės įrangos gamintojų pranešimo apie programinės įrangos atnaujinimą. Už tarnybinių stočių programinės įrangos atnaujinimą atsakingas Įstaigos paskirtas IT sistemos tvarkytojas;

22.2. Įstaigos kompiuterinėse darbo vietose prieigos teisės turi būti apribojamos iki minimalių, būtinų tik tiesioginėms darbo užduotims atlikti, teisių;

22.3. Įstaigos kompiuterinis tinklas, esant galimybei, turi būti apsaugotas lokaliomis ugniasienėmis;

22.4. VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninėje tarnybinėse stotyse ir kompiuterinėse darbo vietose turi būti naudojama antivirusinė programinė įranga, apsauganti nuo kenksmingų programų, įskaitant elektroninio pašto apsaugą. Antivirusinė programinė įranga turi būti atnaujinama automatiniu būdu kiekvieną dieną.

23. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo nuostatos:

23.1. turi būti naudojama tik legali, Įstaigos funkcijoms vykdyti būtina programinė įranga;

23.2. programinė įranga turi būti nuolatos atnaujinama, laikantis gamintojo reikalavimų;

23.3. programinę įrangą diegti, šalinti ir konfigūruoti gali tik IT sistemos tvarkytojas;

23.4. turi būti įdiegta prieigos prie Įstaigos elektroninės informacijos per registravimąsi, teisių suteikimą ir slaptažodžius sistema;

23.5. prieigos prie elektroninės informacijos ir asmens duomenų slaptažodžiai:

23.5.1. turi būti suteikiami, keičiami ir saugomi užtikrinant jų konfidencialumą;

23.5.2. turi būti unikalūs, sudaryti iš ne mažiau kaip 8 simbolių, nenaudojant asmeninio pobūdžio informacijos;

23.5.3. turi būti keičiami ne rečiau kaip kartą per 3 mėnesius;

23.5.4. pirmojo prisijungimo metu naudotojas turi būtinai pakeisti slaptažodį;

23.6. turi būti įdiegta prieigos prie elektroninės informacijos ir asmens duomenų kontrolę užtikrinanti programinė įranga, kuri:

23.6.1. fiksuoja ir kontroliuoja registravimosi bei teisių gavimo pastangas;

23.6.2. leidžia nustatyti leistinų nepavykusių prisijungimų prie programinės įrangos skaičių;

23.6.3. fiksuoja šiuos prisijungimų prie asmens duomenų įrašus: prisijungimo identifikatorius, data, laikas, trukmė, jungimosi rezultatas (sėkmingas, nesėkmingas). Šie įrašai turi būti saugomi ne trumpiau kaip 1 metus;

23.6.4. asmens duomenų paieškos užklausoje turi būti nurodomas asmens duomenų naudojimo tikslas;

23.6.5. užtikrina asmens duomenų, esančių išorinėse duomenų laikmenose ir elektroniniame pašte, saugos kontrolę ir ištrynimą po jų panaudojimo perkeliant į duomenų bazes ir pan.;

23.6.6. registruoti asmens duomenų kopijavimo, jei jis daromas, ir atkūrimo jų avarinio praradimo atveju veiksmus (kada ir kas atliko šiuos veiksmus);

24. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotojų serverių ir kitos) pagrindinės naudojimo nuostatos:

24.1. Įstaigos naudotojų elektroninės informacijos perdavimo tinklo ir užkardų priežiūrą atlieka Įstaigos paskirtas IT sistemos tvarkytojas;

24.2. tinklo ir užkardų konfigūracija turi būti peržiūrima ne rečiau kaip kartą per metus;

24.3. duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

25. Leistinos Įstaigos kompiuterių naudojimo ribos:

25.1. stacionarūs ir nešiojamieji Įstaigos kompiuteriai privalo būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai atlikti. Iš kompiuterių, kurie perduodami remontui ar techninei priežiūrai atlikti, turi būti pašalinta visa Įstaigos apriboto naudojimo elektroninė informacija;

25.2. visuose Įstaigos kompiuteriuose privaloma naudoti papildomas saugos priemones, kuriomis patvirtinama kompiuterio Įstaigos naudotojo tapatybė bei šifruojami duomenys.

26. Įstaigos atsarginių elektroninių duomenų kopijų ir duomenų atkūrimo nuostatos:

26.1. atsarginės Įstaigos duomenų kopijos turi būti daromos automatiniu būdu ne rečiau kaip vieną kartą per savaitę;

26.2. atsarginių kopijų laikmenos turi būti saugomos kitoje patalpoje, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota;

26.3. turi būti periodiškai atliekamas (išbandomas) duomenų atkūrimas iš atsarginių duomenų kopijų;

26.4. už atsarginių Įstaigos elektroninių duomenų kopijų įrašymą ir atkūrimą atsakingas IT sistemos tvarkytojas.

IV SKYRIUS

REIKALAVIMAI PERSONALUI

27. Įstaigos IT sistemos tvarkytojas turi:

27.1. išmanyti elektroninės informacijos saugos užtikrinimo principus;

27.2. sugebėti vertinti rizikos veiksnių tikimybes ir žalos galimybes, organizuoti ir kontroliuoti trūkumų šalinimą;

27.3. tobulinti kvalifikaciją elektroninės informacijos saugos srityje;

27.4. vadovautis Įstaigos saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą ir asmens duomenų apsaugą;

27.5. išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugą, administruoti ir prižiūrėti informacines sistemas.

28. Įstaigos sistemos tvarkytoju negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jo paskyrimo praėję mažiau kaip vieneri metai.

29. Įstaigos informacinės sistemos naudotojai turi:

29.1. turėti pagrindinius darbo kompiuteriu įgūdžius ir mokėti tvarkyti elektroninę informaciją;

29.2. būti susipažinę su Saugos nuostatais bei teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą;

29.3. būti susipažinę su Įstaigos asmens duomenų tvarkymo taisyklėmis ir teisės aktais, reglamentuojančiais asmens duomenų apsaugą;

30. Įstaigos IT sistemų naudotojai, pastebėję elektroninės informacijos saugumo politikos pažeidimų, nusikalstamos veikos požymių ar netinkamai veikiančių Įstaigos elektroninės informacijos saugos užtikrinimo priemonių, nedelsdami privalo apie tai pranešti Įstaigos IT sistemos tvarkytojui.

31. Įstaigos IT sistemos tvarkytojas įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeidžiančią Įstaigos elektroninę informaciją (jos konfidencialumą, vientisumą ar prieinamumą), turi pranešti Įstaigos direktoriui. Jei taikoma, generalinis direktorius apie duomenų ar informacijos saugumo pažeidimus turi pranešti valdžios institucijoms ir susijusiems asmenims, kaip numatyta taikytinuose įstatymuose ir taisyklėse.

32. Įstaigos IT sistemos tvarkytojas ne rečiau kaip kartą per metus inicijuoja IT sistemos naudotojų mokymą elektroninės informacijos saugos klausimais, periodiškai įvairiais būdais primena apie saugumo problemas (pvz., pranešimai elektroniniu paštu, naujų darbuotojų instruktavimas).

V SKYRIUS

NAUDOTOJŲ SUPAŽINDINIMAS SU SAUGOS DOKUMENTAIS

33. Už Įstaigos naudotojų supažindinimą pasirašytinai su šiais saugos nuostatais, saugumo politiką įgyvendinančiais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą yra atsakingas Įstaigos direktorius.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

34. Asmenys, pažeidę šių Saugos nuostatų reikalavimus, atsako teisės aktų nustatyta tvarka.

35. Saugos nuostatai ir kiti su Įstaigos elektroninės informacijos sauga susiję dokumentai turi būti peržiūrimi ne rečiau kaip kartą per metus ir prireikus atnaujinami.
