PATVIRTINTA
Direktoriaus 2020 m. birželio 5 d.
Įsakymu Nr.V-95

VŠĮ ANYKŠČIŲ RAJONO SAVIVALDYBĖS LIGONINĖS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. VšĮ Anykščių rajono savivaldybės ligoninės (toliau - Ligoninės) informacinės sistemos duomenų saugos nuostatai (toliau – saugos nuostatai) reglamentuoja Ligoninės informacinės sistemos (toliau – IS) elektroninės informacijos saugą ir nustato IS saugos politiką.

2. Saugos nuostatų tikslas – užtikrinti IS tvarkomų duomenų konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei kompiuterių tinklo įrangos funkcionavimą.

3. Saugos nuostatai parengti vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“.

4. Šiuose saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, ir kituose Lietuvos Respublikos teisės aktuose vartojamas sąvokas.

5. Elektroninės informacijos saugos užtikrinimo prioritetinės kryptys ir tikslai:

5.1. elektroninės informacijos konfidencialumas;

5.2. elektroninės informacijos prieinamumas;

5.3. elektroninės informacijos vientisumas;

5.4. IS veiklos tęstinumas;

5.5. asmens duomenų apsauga.

6. IS valdytoja ir tvarkytoja yra Ligoninė, adresas: Ramybės g.15, Anykščiai.

7. Ligoninės , kaip IS valdytoja ir tvarkytoja:

7.1. atsako už IS tvarkomos elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugą;

7.2. rengia dokumentus, susijusius su IS saugos užtikrinimu;

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

7.4. tobulina IS ir IS elektroninės informacijos saugą;

7.5. organizuoja IS rizikos vertinimą;

7.6. vykdo IS sudarančių informacinių išteklių inventorizaciją;

7.7. atlieka kitas saugos nuostatuose ir kituose teisės aktuose numatytas funkcijas.

8. Ligoninės direktorius skiria IS saugos įgaliotinį ir IS administratorių.

9. IS saugos įgaliotinis atlieka šias funkcijas:

9.1. koordinuoja ir prižiūri IS saugos politikos įgyvendinimą;

9.2. teikia IS valdytojo vadovui pasiūlymus dėl:

9.2.1. IS administratoriaus paskyrimo ir reikalavimų IS administratoriui nustatymo;

9.2.2. institucijos informacinių technologijų saugos atitikties vertinimo atlikimo Informacinių technologijų saugos atitikties vertinimo metodikos, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156, nustatyta tvarka;

9.2.3. IS saugos dokumentų priėmimo, keitimo;

9.3. koordinuoja elektroninės informacijos saugos incidentų, įvykusių IS, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, elektroninės informacijos saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

9.4. teikia IS administratoriui ir IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

9.5. turi teisę pagal savo įgaliojimus teikti privalomus vykdyti nurodymus ir pavedimus kitiems IS valdytojo ir IS tvarkytojų darbuotojams, jeigu tai būtina saugos politikai įgyvendinti;

9.6. organizuoja rizikos įvertinimą;

9.7. periodiškai organizuoja IS naudotojų mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas;

9.8. atlieka kitas šiuose saugos nuostatuose, Bendrųjų elektroninės informacijos saugos reikalavimų apraše ir kituose teisės aktuose nustatytas IS saugos įgaliotiniui priskirtas funkcijas.

10. IS administratorius atlieka šias funkcijas:

10.1. naudotojams suteikia teisę naudotis elektronine informacija ir kompiuteriu paskirtoms funkcijoms atlikti;

10.2. administruoja tarnybines stotis, kompiuterių tinklo įrangą, pašto ir paieškos sistemas, nustato pažeidžiamų vietų ir saugos reikalavimų atitiktį;

10.3. registruoja saugos įvykius, informuoja apie juos IS saugos įgaliotinį, teikia pasiūlymus dėl įvykį sukėlusių priežasčių pašalinimo;

10.4. atlieka kitas saugos nuostatuose ir kituose teisės aktuose numatytas funkcijas.

11. Tvarkant elektroninę informaciją ir užtikrinant jos saugumą vadovaujamasi:

11.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

11.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

11.3. Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymu;

11.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716;

11.5. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832;

11.6. Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71 (1.12);

11.7. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156;

11.8. kitais teisės aktais, kurie reglamentuoja elektroninės informacijos saugumo politiką ir duomenų tvarkymo teisėtumą, valstybės informacinių sistemų tvarkytojų veiklą ir elektroninės informacijos saugos valdymą.

12. Savivaldybės administracijos IS saugumas užtikrinamas vadovaujantis Lietuvos standartais:

12.1. LST ISO/IEC 27001:2006 ,,Informacijos technologija. Saugos metodai. Informacijos saugos valdymo sistemos. Reikalavimai (tapatus ISO/IEC 27001:2005)“;

12.2. LST ISO/IEC 27002:2009 ,,Informacijos technologija. Saugos metodai. Informacijos saugos valdymo praktikos kodeksas (tapatus ISO/IEC 27002:2005)“;

12.3. kitais Lietuvos ir tarptautiniais standartais, reglamentuojančiais elektroninės informacijos saugą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 4.3.2 ir 4.3.3 punktais, savivaldybės administracijos IS elektroninė informacija priskiriama žinybinės elektroninės informacijos kategorijai.

14. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.4 punktu, Ligoninės IS pagal elektroninės informacijos svarbos kategoriją priskiriama ketvirtai kategorijai.

15. IS saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, kuri skelbiama Lietuvos Respublikos vidaus reikalų ministerijos interneto svetainėje, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, ne rečiau kaip kartą per metus organizuoja IS rizikos vertinimą. Prireikus IS saugos įgaliotinis gali organizuoti neeilinį IS rizikos vertinimą. IS valdytojo vadovo rašytiniu pavedimu IS rizikos vertinimą gali atlikti pats IS saugos įgaliotinis.

16. IS rizikos vertinimo rezultatai išdėstomi Ligoninės IS rizikos vertinimo ataskaitoje, kurią tvirtina Ligoninės direktorius (toliau – ataskaita). Ataskaita rengiama vertinant rizikos veiksnius, galinčius turėti įtaką elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai yra šie:

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

16.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis kompiuterine įranga elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

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

17. Atsižvelgiant į ataskaitą, gali būti tvirtinamas Ligoninės IS rizikos įvertinimo ir rizikos valdymo priemonių planas, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

18. Elektroninės informacijos saugos priemonės yra parenkamos atsižvelgiant į poreikį ir Ligoninės turimus resursus.

19. Elektroninės informacijos saugumą užtikrina IS techninė ir programinė įranga, IS saugos įgaliotinis ir IS administratorius.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

20. Naudotojų prieigos prie IS suteikimo tvarka nustatyta Ligoninės informacinės sistemos naudotojų administravimo taisyklėse.

21. Prieiga naudotojams suteikiama tik prie tų išteklių, kurie yra būtini tiesioginėms pareigoms atlikti.

22. Stacionarūs ir nešiojamieji IS naudotojų kompiuteriai turi būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai. Iš kompiuterių, kurie perduoti remontui ar techninei priežiūrai, turi būti pašalinta visa riboto naudojimo elektroninė informacija.

23. Naudotojams draudžiama patiems diegti bet kokią programinę įrangą. Programinę įrangą, reikalingą naudotojo funkcijoms atlikti, diegia ir prižiūri IS administratorius, išskyrus programinę įrangą nešiojamuosiuose kompiuteriuose, perduotuose naudotis savivaldybės tarybos nariams jų kadencijos laikotarpiui.

24. Naudotojams gali būti suteikiama nuotolinio prisijungimo prie IS galimybė.

25. Saugos reikalavimai, taikomi jungiantis prie IS nuotoliniu būdu, turi būti ne mažesni nei jungiantis prie IS vidiniame savivaldybės administracijos tinkle.

26. Tarnybinėse stotyse ir darbo vietų kompiuteriuose turi būti naudojama programinė įranga, skirta apsaugoti IS nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.) (toliau – antivirusinė programinė įranga). Antivirusinė programinė įranga turi būti atnaujinama kartą per parą.

27. IS funkcionuoti būtina tarnybinėse stotyse ir IS naudotojų kompiuteriuose 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 kontrolę atsako IS administratorius.

28. Ligoninės kompiuterių tinklas turi būti užkarda atskirtas nuo viešųjų telekomunikacijų tinklų.

29. Metodai, kuriais gali būti užtikrinamas saugus IS duomenų teikimas ir (ar) gavimas:

29.1. IS duomenys perduodami automatiniu būdu (naudojant TCP/IP protokolą) realiu laiku arba asinchroniniu režimu pagal IS duomenų teikimo ir gavimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka;

29.2. už duomenų teikimo ir gavimo sutartyse nurodomų saugos reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas IS administratorius.

30. IS duomenų kopijavimo tvarka:

30.1. Kiekvieną savaitę kuriama duomenų bazės kopija į UAB “Edrana“ FTP serverį.

31. Už IS duomenų atsarginių kopijų darymą yra atsakingas IS administratorius, už kopijų saugojimą ir atstatymą atsakingi UAB „ Edrana“.

IV. REIKALAVIMAI PERSONALUI

32. Naudotojai privalo rūpintis tvarkomos elektroninės informacijos sauga.

33. Naudotojai turi būti susipažinę su šiais saugos nuostatais ir kitais saugos politikos įgyvendinamaisiais dokumentais.

34. IS saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis teisės aktais, standartais ir kitais su elektroninės informacijos sauga susijusiais dokumentais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

35. IS saugos įgaliotiniu 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 jos paskyrimo praėję mažiau kaip vieneri metai.

36. IS administratorius privalo išmanyti elektroninės informacijos saugos principus, darbą su kompiuterių tinklais, mokėti užtikrinti jų saugumą, taip pat administruoti ir prižiūrėti duomenų bazes, turi būti susipažinęs su saugos nuostatais ir saugos politikos įgyvendinamaisiais dokumentais.

37. Naudotojai turi turėti darbo kompiuteriu įgūdžių.

38. Naudotojams turi būti nuolat rengiami elektroninės informacijos saugos mokymai, įvairiais būdais primenama apie elektroninės saugos problematiką (pvz.: priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės). Saugos mokymai organizuojami ne rečiau kaip kartą per 2 metus. Mokymus organizuoja ir jų efektyvumą vertina IS saugos įgaliotinis.

V. INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

39. Už naudotojų supažindinimą pasirašytinai su šiais saugos nuostatais, saugos politikos įgyvendinamaisiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, taip pat su atsakomybe už saugos dokumentų nuostatų pažeidimus, atsakingas IS saugos įgaliotinis. Už saugos dokumentuose nustatytų reikalavimų nesilaikymą yra atsakingi savivaldybės administracijos padalinių vadovai.

40. Pakartotinis supažindinimas su Ligoninės IS saugos dokumentais yra vykdomas elektroniniu paštu pasikeitus saugos dokumentams.

41. Saugos nuostatai ir saugos politikos įgyvendinamieji dokumentai yra skelbiami Ligoninės interneto svetainėje.

VI. BAIGIAMOSIOS NUOSTATOS

42. Saugos nuostatai yra privalomi IS saugos įgaliotiniui, IS administratoriui ir IS naudotojams.

43. Naudotojai, pažeidę šių saugos nuostatų ar saugos politiką įgyvendinančių dokumentų reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____