PATVIRTINTA
Direktoriaus 2021-11-30
Įsakymu Nr. V-75

VŠĮ „PANEVĖŽIO MIESTO POLIKLINIKOS“ INFORMACINĖS SISTEMOS FOXUS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. UAB „SOFTDENT“ informacinės sistemos Foxus (toliau – „**IS foxus**“) duomenų saugos nuostatai (toliau – „**Saugos nuostatai“**) nustato principus ir taisykles, užtikrinančias saugų IS Foxus elektroninės informacijos tvarkymą.

2. Saugos nuostatų tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti IS Foxus esančią elektroninę informaciją, užtikrinti jos konfidencialumą, tinkamą kompiuterizuotų darbo vietų bei tinklo įrangos funkcionalumą. IS Foxus duomenų saugai užtikrinti kompleksiškai naudojamos organizacinės, fizinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo į saugos incidentus, atsakomybės, elektroninės informacijos saugos supratimo bei saugos priemonių projektavimo ir diegimo principus.

3. Pagrindinės Saugos nuostatose vartojamos sąvokos:

a) **Bendrovė –** UAB „SOFTDENT“, pagal Lietuvos Respublikos įstatymus įsteigta bendrovė, kurios juridinio asmens kodas 110799112, registruota buveinė Drobės g. 62, LT-45181 Kaunas, Lietuvos Respublika, duomenys apie kurią kaupiami ir saugomi Juridinių asmenų registre. Bendrovė yra IS Foxus valdytojas.

b) **Elektroninės informacijos saugos incidentas** – įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

c) **Saugos įgaliotinis** – Bendrovės direktoriaus paskirtas darbuotojas, atsakantis už IS Foxus elektroninės informacijos saugos priemonių bei saugą reglamentuojančių reikalavimų įgyvendinimą.

d) **Administratoriai** – Bendrovės direktoriaus paskirti darbuotojai, dirbantys Bendrovėje pagal darbo sutartis ar kitais pagrindais, bei atliekantys IS Foxus kasdieninę priežiūrą.

e) **Naudotojai** – VšĮ „Panevėžio miesto poliklinika“, pagal Lietuvos Respublikos įstatymus įsteigta įstaiga, kurios kodas 148194854, registruota adresu Nemuno g. 75, LT-37355 Panevėžys, Lietuvos Respublika, duomenys apie kurią kaupiami ir saugomi Juridinių asmenų registre. Sveikatos priežiūros įstaiga, sudariusi sutartį su Bendrove dėl asmens duomenų tvarkymo IS Foxus, darbuotojai (sveikatos priežiūros

specialistai, įgalioti administracijos darbuotojai), turintis teisę naudotis IS Foxus ištekliais jų numatytoms funkcijoms atlikti.

f) **Vartotojai** – fiziniai asmenys, kurie registruojasi E-pacientas.lt portale ir kurių asmens duomenis tvarko Bendrovė.

g) **Sveikatos priežiūros įstaigos** – asmens sveikatos priežiūros paslaugas teikiantys juridiniai asmenys, sudarę su Bendrove sutartis dėl duomenų tvarkymo IS Foxus.

h) **Duomenų teikėjai/gavėjai** – Naudotojai bei valstybinės institucijos, kuriomis Sveikatos priežiūros įstaigos teikia bei gauna duomenis IS Foxus Naudotojams, Vartotojams, Administratoriams, Saugos įgaliotiniui bei kitiems asmenims, kurie teisėtais pagrindais naudojasi IS Foxus.

4. Saugos nuostatai privalomi visiems IS Foxus Naudotojams, Vartotojams, Administratoriams, Saugos įgaliotiniui bei kitiems asmenims, kurie teisėtais pagrindais naudojasi IS Foxus.

5. Pagrindinės IS Foxus elektroninės informacijos saugumo užtikrinimo kryptys:

a) organizacinių saugaus darbo su duomenimis priemonių įgyvendinimas ir kontrolė;

b) fizinė elektroninės informacijos apdorojimo priemonių apsauga;

c) techninės ir programinės elektroninės informacijos apsaugos priemonės.

6. Bendrovės vadovo funkcijos ir atsakomybė:

a) vadovauja ir organizuoja IS Foxus veiklą, skirdamas Saugos įgaliotinį, Administratorius bei kitus atsakingus darbuotojus;

b) kontroliuoja, kad IS Foxus būtų tvarkomas vadovaujantis teisės aktų reikalavimais bei šiais Saugos nuostatais.

7. Saugos įgaliotinio funkcijos:

a) teikia Bendrovės vadovui pasiūlymus dėl Administratorių paskyrimo;

b) teikia Administratoriams bei Naudotojams nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos politikos įgyvendinimu;

c) teikia pasiūlymus dėl saugos nuostatų pakeitimo ar kitų saugos dokumentų priėmimo;

d) koordinuoja Elektroninės informacijos saugos incidentų, įvykusių IS Foxus, tyrimą bei esant reikalui informuoja kompetentingas institucijas dėl galimai neteisėtų veikų, susijusių su informacijos saugumo incidentais;

e) organizuoja IS Foxus sistemos rizikos įvertinimą;

f) kitas funkcijas, kurios reikalingos užtikrinti IS Foxus elektroninės informacijos saugą.

8. Administratoriaus funkcijos ir atsakomybė:

a) atsako už IS Foxus tinkamą funkcionavimą;

b) įvertina Naudotojų pasirengimą dirbti su informacine sistema ir suteikia Naudotojams teisę naudotis informacinės sistemos galimybėmis paskirtoms funkcijoms atlikti;
c) prižiūri Vartotojų tinkamą prisiregistravimą prie IS Foxus posistemės E.pacientas.lt;
d) teikia pasiūlymus IS Foxus palaikymo, priežiūros ir duomenų saugumo klausimais;
e) atlieka IS Foxus sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimo aptikimo sistemų, duomenų perdavimo tinklų) administravimą, pažeidžiamų vietų ir saugos reikalavimų atitikties nustatymą;
f) registruoja ir informuoja Saugos įgaliotinį apie Elektroninės informacijos saugos incidentus ir teikia pasiūlymus;
g) vykdo kitas Administratoriui paskirtas funkcijas.

II DUOMENŲ SAUGOS VALDYMAS

9. IS Foxus duomenys nėra vieši ir prieinami tik:
a) Naudotojams – Sveikatos priežiūros įstaigos darbuotojams tik šios įstaigos IS Foxus tvarkomi duomenys. Naudotojui yra priskiriamos tik tok funkcijos, kurios priklauso naudotojui pagal darbo sritį;
b) Vartotojams – IS Foxus posistemėje esantys jų asmens duomenys.

10. IS Foxus duomenys teikiami Duomenų gavėjams pagal Sveikatos priežiūros įstaigų sudarytas duomenų teikimo sutartis.

11. Saugos įgaliotinis ne rečiau kaip vieną kartą per metus organizuoja IS Foxus rizikos įvertinimą, atsižvelgdamas į LR vidaus reikalų ministerijos išleistą metodologinę priemonę „Rizikos analizės vadovas“. Prireikus Saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą.

12. IS Foxus rizikos įvertinimas išdėstomas Rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos IS Foxus elektroninės informacijos saugai. Svarbiausi rizikos veiksniai yra šie:
a) subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, fiziniai informacijos technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kt.);
b) subjektyvūs tyčiniai (nesankcionuotas naudojimasis duomenims gauti, duomenų pakeitimas ir sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kt.);
c) atsitiktinės subjektyvios aplinkybės (darbuotojų praradimas, audros, gaisrai, vandens poveikis, elektros instaliacijos gedimas ir kt.);

d) nenugalima jėga (*force majeure*).

13. Atsižvelgdama į rizikos įvertinimo ataskaitą, prireikus Bendrovės vadovas ar jo įgaliotas asmuo tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir (ar) kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

14. Siekdamas užtikrinti Saugos nuostatose nustatytų reikalavimų įgyvendinimo organizavimą ir kontrolę, Saugos įgaliotinis ne rečiau kaip kartą per metus organizuoja informacinių technologijų saugos atitikties vertinimą, kurio metu:

a) įvertina Saugos nuostatų ir kitų saugos politiką įgyvendinančių dokumentų bei realios duomenų saugos situacijos atitiktis;
b) inventorizuoja IS Foxus techninę ir programinę įrangą (pasirinktinai);
c) tikrina visose IS Foxus serveriuose (tarnybinėse stotyse), administratoriaus bei nemažiau kaip 10% Naudotojų (Sveikatos priežiūros įstaigų darbuotojų) kompiuterinėse darbo vietose įdiegtą programinę įrangą ir jos sąranką;
d) peržiūri Administratoriams ir Naudotojams suteiktų teisių atitiktis jų vykdomoms funkcijoms;
e) įvertina pasirengimą užtikrinti IS Foxus veiklos tęstinumą įvykus saugos incidentui;
f) analizuoja rizikos veiksnius, galimas jų pašalinimo arba neigiamo poveikio sumažinimo priemones ir jei reikalinga koreguoja rizikos įvertinimo ataskaitą.

15. Atlikus informacinių technologijų saugos atitikties vertinimą, esant poreikiui rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus Bendrovės vadovas ar jo įgaliotas asmuo.

16. Techninės, programinės ir organizacinės elektroninės informacijos saugos priemonės pasirenkamos taip, kad, patiriant kuo mažiau išlaidų būtų užtikrintas IS Foxus veiklos tęstinumas ir saugus Naudotojų darbas.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

17. IS Foxus Naudotojams tiesioginė prieiga prie duomenų suteikiama įgyvendinus jų autentifikavimo priemones:

a) Naudotojai (Sveikatos priežiūros įstaigų darbuotojai) prie jiems skirtos IS Foxus prieigos jungiasi su unikaliu vartotojo vardu ir slaptažodžiu;
b) Naudotojo unikalus slaptažodis susideda ne mažiau, kaip iš 8 simbolių (raidžių ir skaičių), kurie turi būti atnaujinami ne rečiau, kaip kas 60 (šešiasdešimt) kalendorinių dienų.

18. Naudotojų prisijungimo teisių suteikimo procedūros:

a) Suteikiant prisijungimo duomenis naujai prie IS Foxus prisijungiančiai Sveikatos priežiūros įstaigai, Sveikatos priežiūros įstaigos administracija atsiunčia visų

įstaigoje dirbančių Sveikatos priežiūros specialistų ir darbuotojų sąrašą kuriems reikalingas prisijungimas prie sistemos: vardą, pavardę, gimimo datą, spaudo numerį ir seriją, darbo ir pacientų priėmimo laikų informaciją (reikalinga sudaryti darbo grafikams), kontaktinį telefoną. Administratorius sukuria Sveikatos priežiūros įstaigos nurodytiems darbuotojams prisijungimus ir darbo aplinkas IS Foxus. Bendrovės įgalioti asmenys nuvyksta į Sveikatos priežiūros įstaigą ir apmokymų darbo su IS Foxus sistemos metu asmeniškai kiekvienam Naudotojui įteikia individualius prisijungimo vardus ir slaptažodžius, atspausdintus ant popieriaus lapo.

19. Naudotojų prisijungimo teisių panaikinimo procedūra: Sveikatos priežiūros įstaigos administracija susisiekia su Administratoriumi el.paštu ir informuoja apie Naudotojo prisijungimo teisių panaikinimą. Ne vėliau kaip kitą darbo dieną Administratorius deaktyvuoja naudotojo prisijungimo duomenis. naudotojo prisijungimo duomenys neatkuriamai ištrinami per 5 (penkias) darbo dienas nuo deaktyvavimo dienos.

20. Vartotojo prisijungimo duomenis susikuria pats Vartotojas registruojantis E-pacientas.lt interneto tinklalapyje. Vartotojo prisijungimo duomenys: registracijos metu nurodytas el.pašto adresas bei sukurtas slaptažodis iš ne mažiau, kaip iš 8 simbolių (žodžių ir skaičių). Vartotojas, ištrindamas savo paskyrą, panaikina savo prisijungimo duomenis.

21. Duomenų apsikeitimas tarp Sveikatos priežiūros įstaigos administracijos ir Bendrovės valdomų serverių vyksta šifruotu kanalu (SSL su naudojamais algoritmais: SHA1 žinutėms ir RSA raktų apsikeitimui, naudojamas 128 bitų ilgio raktas). SSL sertifikatasyra išduotas StartCom Ltd. sertifikavimo atgentūros. Naudotojo prisijungimas prie E.pacientas.lt ar Sveikatos priežiūros įstaigoms skirta IS Foxus prieiga apsaugoti unikaliu slaptažodžiu, kuris susideda ne mažiau, kaip iš 8 simbolių (raidžių ir skaičių).

22. Nepavykę Naudotojų ar Administratorių prisijungimai yra automatiškai registruojami elektroniniame žurnale, maksimalus leistinas neteisingų prisijungimų bandymų skaičius 3 (trys). Vėlesnis bandančiojo IP adresas įtraukiamas į ugniasienės sąrašus iki kol Administratorius šio IP adreso nepašalina iš šio sąrašo. Maksimalus neteisingas prisijungimo laikas yra 3 sekundės. Administratorių prisijungimas prie duomenų bazių yra užtikrinamas ir privačiais raktais (128 bitų ilgio).

23. Naudotojų bei Administratorių prisijungimo duomenys: prisijungimo identifikatorius, data, laikas, jungimosi rezultatas (sėkmingas, nesėkmingas), bylos, prie kurių buvo jungtasi, atlikti veiksmai su asmens duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kiti duomenų tvarkymo veiksmai) fiksuojami elektroniniame žurnale. Naudotojų (Sveikatos priežiūros įstaigų darbuotojų) elektroniniai žurnalai peržiūrimi ne rečiau, kaip kas 3 (tris) darbo dienas. Ne rečiau, kaip kas mėnesį Sveikatos priežiūros įstaigoms elektroniniu būdu siunčiamos ataskaitos apie jų darbuotojų prisijungimo duomenis. Esant būtinybei Administratorių prisijungimo duomenis peržiūri Saugos įgaliotinis.

24. IS Foxus sistemoje prisijungimo duomenys saugomi 1 (vienerius) metus.

25. IS Foxus duomenys Naudotojams, Duomenų gavėjams perduodami automatiniu būdu naudojant TCP/IP protokolą realiame laike („On-line“režimu). Visi duomenys Naudotojams siunčiami šifruotu SSL kanalu, šifruojant ne trumpesniu, kaip 128 bitų ilgio raktu. Duomenų gavėjams (į valstybines informacines sistemas) duomenys teikiami šifruotu VPN kanalu, kitiems privatiems Duomenų gavėjams duomenys teikiami šifruotu SSL kanalu, šifruojant ne trumpesniu, kaip 128 bitų ilgio raktu.

26. IS Foxus duomenų saugai užtikrinti yra taikomos tam tikros programinės įrangos naudojimo nuostatos:

a) IS Foxus serveriuose, Administratorių, Naudotojų kompiuterinėse darbo vietose įdiegiama legali (su naujausiais pataisymais) programinė įranga;
b) IS Foxus serverių, Administratorių, Naudotojų kompiuterinių darbo vietų operacinių sistemų ir taikomųjų programų sąranka parenkama tokiu būdu, kad būtų užtikrintas didžiausias saugumo lygis;
c) IS Foxus serverių, administratoriaus, naudotojų kompiuterinėse darbo vietose turi būti diegiama programinė įranga, skirta apsisaugoti nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidautino elektroninio pašto ir pan.). Programinė įranga atnaujinama periodiškai, užtikrinant nepertraukiamą apsaugą;
d) IS Foxus programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims;
e) kompiuterinis tinklas, prie kurio prijungti serveriai, nuo viešojo interneto turi būti atskirti tinklo užkarda (angl. Firewall);
f) Naudotojų, naudojančių nešiojamus kompiuterius savo funkcijoms vykdyti ne savo darbo vietoje, kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas vartotojo tapatybės patvirtinimas. Nešiojamuose kompiuteriuose įdiegta slaptažodžiu apsaugota ekrano užsklanda, kuri aktyvuojama automatiškai, jei nėra vykdomi jokie veiksmai su kompiuteriu 15 (penkiolika) minučių.

27. IS Foxus programinės, techninė įrangos saugos priemonių įgyvendinimą organizuoja Administratoriai.

28. Už atsarginių IS Foxus duomenų kopijų darymą ir saugojimą atsako trečiasis asmuo, su kuriuo Bendrovė yra sudariusi sutartį dėl duomenų kopijavimo bei duomenų saugojimo. Duomenų kopijos turi būti daromos automatiškai kasdien. Detalios duomenų kopijų saugojimo priemonės, būdai ir vieta, kopijų atkūrimo tvarka, naikinimo tvarka išdėstomi Asmens duomenų tvarkymo taisyklėse bei kitose Bendrovės vadovo patvirtintuose dokumentuose.

IV. REIKALAVIMAI ASMENIMS, NAUDOJANTIEMS FOXUS

29. Saugos įgaliotinis privalo išmanyti informacijos saugos užtikrinimo principus, savo darbe turi būti susipažinęs su esminiais reikalavimais, turėti atitinkamą kvalifikaciją, sugebėti prižiūrėti, kaip įgyvendinama saugos politika.

30. Administratorius privalo turėti dokumentais patvirtintą informacinių technologijų specialisto kvalifikaciją, privalo išmanyti informacijos saugos principus, darbą su kompiuterių tinklais, mokėti užtikrinti jų saugumą, taip pat administruoti ir prižiūrėti duomenų bazes, turi būti susipažinęs su Saugos nuostatais, taip pat kitais Bendrovės patvirtintais su elektroninės informacijos ar duomenų sauga susijusiais dokumentais.

31. Naudotojai privalo turėti pagrindinius darbo su kompiuteriu įgūdžius.

32. Naudotojai, pastebėję saugos politikos pažeidimus, nusikalstamos veiklos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti Bendrovei.

33. Saugos įgaliotinis esant poreikiui organizuoja IS Foxus Naudotojų mokymus kvalifikacijos tobulinimo ir duomenų saugos klausimais, taip pat periodiškai Naudotojams primena saugumo problemas (elektroniniu paštu, per internetinę svetainę, atmintinėmis naujiems Naudotojams ir pan.).

V. ASMENŲ, NAUDOJANČIŲ IS FOXUS ATSAKOMYBĖ

34. Asmenys, naudojantys IS Foxus, privalo savo kompetencijos ribose rūpintis sistemos bei joje tvarkomos elektroninės informacijos bei duomenų saugumu.

35. Tvarkyti sistemos duomenis gali tik tie Naudotojai, kurie yra susipažinę su šiuose nuostatose jiems aktualiais reikalavimais.

36. Administratorių supažindinimą su šiais nuostatais ir bei kitais Bendrovės saugos politiką reglamentuojančiais dokumentais bei atsakomybę už šių reikalavimų nesilaikymą pasirašytinai organizuoja Saugos įgaliotinis. naudotojai supažindinami elektroniniu būdu prieš jiems suteikiant teises tvarkyti sistemos duomenis.

37. Asmenys, naudojantys IS Foxus ir pažeidę šiuose nuostatose ar kituose Bendrovės turimuose saugos politiką reglamentuojančiais dokumentuose nustatytus reikalavimus (su kuriais asmenys buvo supažindinti), atsako įstatymų nustatyta tvarka.

VI. NUOSTATŲ ATNAUJINIMO TVARKA

38. Saugos įgaliotinis, siekdamas užtikrinti sistemos ir joje tvarkomų duomenų saugumą, teikia siūlymus Bendrovės vadovui dėl nuostatų keitimo ar kitų saugumo politiką reglamentuojančių teisės aktų priėmimo, keitimo ar panaikinimo.

39. Saugos nuostatai ir kiti saugumo politiką reglamentuojantys dokumentai iš esmės peržiūrimi ir prireikus keičiami ne rečiau kaip kartą per metus atliekant šių nuostatų II skirsnyje nurodytą vertinimą.