PATVIRTINTA
VšĮ Klaipėdos miesto polikinika
Vyr. Gydytojo
2020 m. kovo 10 d. įsakymu Nr. 17

VŠĮ KLAIPĖDOS MIESTO POLIKLINIKOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. VšĮ Klaipėdos miesto poliklinika, buveinės adresas Taikos pr. 76, Klaipėda, informacinės sistemos duomenų saugos nuostatai (toliau – Duomenų saugos nuostatai) nustato saugų elektroninės informacijos tvarkymą užtikrinančius principus ir reikalavimus (toliau – Saugos politika) VšĮ Klaipėdos miesto poliklinikos (toliau – Poliklinikos) valdomoje informacinėje sistemoje (toliau - IS), jos posistemėse ir duomenų rinkmenose atliekant Poliklinikai pavestas funkcijas.

2. Duomenų saugos nuostatus įsakymu tvirtina Poliklinikos vyr. gydytojas. Šio dokumento dalys gali būti išplatinamos su Poliklinikos informacija susijusioms šalims joms prieinama ir suprantama forma.

3. Šiuose Duomenų saugos nuostatuose vartojamos sąvokos:

Administratorius – Poliklinikos darbuotojas, atliekantis funkcijas, susijusias su IS naudotojų teisių valdymu, IS komponentais, šių IS komponentų sąranka, IS pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos incidentus.

Elektroninė informacija – neįslaptinta informacija (arba duomenys), saugoma, perduodama ar kitaip apdorojama elektroniniu būdu IS, leidžiančiose tokią informaciją saugoti, perduoti, ar kitaip apdoroti, arba valstybės ir žinybiniuose registruose ir sudaranti sąlygas sėkmingai atlikti Poliklinikos funkcijas.

Informacinė sistema (IS) – elektroninio pašto, finansų ir apskaitos valdymo sistemos, Poliklinikos interneto svetainės, dokumentų valdymo sistemos, vidaus elektroninės informacijos visuma.

IS valdytojas – Poliklinika.

Informacijos saugumas – apima informacijos konfidencialumo, vientisumo ir prieinamumo išsaugojimą. Papildomai gali būti įtraukti ir kiti kriterijai, tokie kaip autentiškumas, atskaitingumas, neišsižadėjimas ir patikimumas.

Informacijos saugumo incidentas – vienas ar daugiau nepageidaujamų ir netikėtų informacijos saugumo įvykių, turinčių didelę tikimybę pakenkti veiklai ir keliančių grėsmę informacijos saugumui (ISO/IEC TR 18044:2004).

Informacijos saugumo įvykis – nustatytas sistemos, tarnybos ar tinklo įvykis, rodantis galimą informacijos saugumo politikos spragą ar informacijos saugumo priemonių triktį arba anksčiau nenumatytos situacijos, kuri gali būti susijusi su informacijos saugumu, atsiradimą (ISO/IEC TR 18044:2004).

Informacinis turtas – bet kokios formos informacija, taip pat su ja susijęs materialus (kompiuterių bei ryšio įrenginiai, patalpos ir pan.) bei nematerialus (reputacija, įvaizdis) turtas.

Grėsmė – potenciali nepageidaujamų įvykių, galinčių padaryti žalą VšĮ Klaipėdos miesto poliklinikos informacijai, galimybė.

Kenksminga programinė įranga – programinė įranga, turinti kenkėjiškų tikslų ar daranti neigiamą įtaką, pvz.: virusai, „kirminai“, „trojos arkliai“, šnipinėjimo programinė įranga ir pan.

Konfidenciali informacija – informacija, prieinama ir atskleidžiama tik įgaliotiems asmenims.

1

Konfidencialumas – savybė, kad informacija prieinama ir atskleidžiama tik tam įgaliotiems asmenims.

IS naudotojas – VšĮ Klaipėdos miesto poliklinikos darbuotojas, dirbantis pagal darbo sutartį, susijusių šalių, rangovų atstovas, kuriam suteikta priėjimo prie VšĮ Klaipėdos miesto poliklinikos informacijos ir/ar informacinių sistemų teisė naudotis informacinės sistemos ištekliais numatytoms funkcijoms atlikti.

Paslaugos - skaičiavimų ir ryšio paslaugos, bendrosios paslaugos (pvz.: šildymas, apšvietimas, energija, oro kondicionavimas).

Pažeidžiamumas – turto ar kitų vertingų dalykų grupės silpnoji vieta, kuria gali pasinaudoti grėsmė.

Personalas (žmogiškieji ištekliai) – darbuotojai, dirbantys pagal darbo sutartis.

Prieinamumas – savybė, užtikrinanti įgalioto subjekto prieigos ir naudojimosi, esant reikalui, galimybę.

Programinė įranga – taikomoji programinė įranga, sisteminė programinė įranga, plėtros priemonės ir paslaugų programos.

Rizika – potenciali galimybė, kad konkreti grėsmė pasinaudos informacinio ištekliaus ar informacinių išteklių grupės pažeidžiamumu ir sunaikins ar sugadins informacinį ištekių.

Šifravimas – duomenų pakeitimo procesas iš pradinės būsenos į būseną, kai duomenys negali būti perskaityti (naudojami) neturint priemonių / informacijos (šifravimo rakto), kuriomis galima duomenis sugrąžinti į pradinę būseną.

Trečiasis asmuo – asmuo ar organizacija, kuri pripažįstama nepriklausoma nuo dalyvaujančių asmenų, nagrinėjant svarstomą klausimą.

Turtas – visa, kas turi kokią nors vertę VšĮ Klaipėdos miesto poliklinikoje.

Vadovybė – VšĮ Klaipėdos miesto poliklinikos vyr. gydytojas.

Vientisumas – savybė, nusakanti išteklių tikslumo ir pilnumo apsaugą.

4. Šioje Informacijos saugumo politikoje vartojami sutrumpinimai:

Poliklinika – VšĮ Klaipėdos miesto poliklinika, buveinės adresas Taikos pr. 76, Klaipėda.

Darbuotojai – Poliklinikos darbuotojai, dirbantys pagal darbo sutartis.

IT – informacinės technologijos.

5. IS duomenų saugos tikslai:

5.1 Informacijos patikimumo, vientisumo, konfidencialumo, prieinamumo ir saugumo užtikrinimas;

5.2 Kompiuterizuotų darbo vietų tinkamo saugumo lygio įdiegimas bei saugumo stebėsena;

5.3 Nuolatinis vietinio kompiuterinio tinklo funkcionalumo užtikrinimas bei saugumo stebėsena;

5.4 Tinkamo kompiuterinės, tinklo, ir programinės įrangos funkcionalumo ir saugumo užtikrinimas.

6. Informacijos saugumo užtikrinimo prioritetinės kryptys:

6.1 IS perduodamų duomenų konfidencialumo užtikrinimas:

6.2 IS perduodamų duomenų vientisumo užtikrinimas;

6.3 IS duomenų prieinamumo užtikrinimas;

6.4 IS veiklos tęstinumo užtikrinimas.

7. IS duomenų saugai užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo, atsakomybės, elektroninės informacijos saugos lygio kėlimo, saugos priemonių projektavimo ir diegimo principus.

8. VšĮ Klaipėdos miesto poliklinika, veikianti kaip Informacinės sistemos valdytojas ir tvarkytojas, vykdo šias funkcijas:

8.1. užtikrina valdomų IS elektroninės informacijos saugumą, vientisumą, konfidencialumą, prieinamumą, tinkamą kompiuterių bei komunikacinės įrangos funkcionavimą Poliklinikoje.

8.2. vadovaudamasis saugos nuostatais, skiria IS saugos įgaliotinį, administratorių, esant poreikiui, sudaro elektroninės informacijos saugos darbo grupes;

8.3. tvirtina saugos politiką įgyvendinančius dokumentus.

9. IS tvarkytojo funkcijos ir atsakomybė:

9.1. užtikrina IS veikimui ir duomenų mainams būtinos techninės ir programinės įrangos įdiegimą, nepertraukiamą funkcionalumą, tinkamą priežiūrą bei atnaujinimą;

9.2. organizacinėmis, teisinėmis, techninėmis ir metodinėmis priemonėmis užtikrina saugų IS duomenų tvarkymą;

9.3. organizuoja IS veikimui, priežiūrai ir plėtrai reikalingų funkcinių, techninių, programinių priemonių įsigijimą, įdiegimą, modernizavimą;

9.4. užtikrina, kad IS būtų administruojama saugiai ir laikantis šių Saugos nuostatų, Lietuvos Respublikos įstatymų bei kitų teisės aktų;

9.5. skiria darbuotojus, atsakingus už IS sklandų veikimą, priežiūrą, atnaujinimą;

9.6. skiria ir administruoja IS naudotojus, organizuoja jų mokymą;

9.7. vykdo kitas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu, kitais įstatymais ir teisės aktais bei Poliklinikos vyr. gydytojo įsakymais nustatytas funkcijas.

10. Administratorius organizuoja ir kontroliuoja šių saugos nuostatų įgyvendinimą ir atlieka šias funkcijas:

10.1. teikia IS valdytojui pasiūlymus dėl:

10.1.1. saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

10.1.2. IS saugos reikalavimų atitikties vertinimo atlikimo;

10.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių IS, tyrimą (išskyrus atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės);

10.3. teisės aktų nustatyta tvarka atlieka IT saugos atitikties vertinimą. Jei vertinimui atlikti būtina įsigyti vertinimo paslaugas, teikia IS valdytojui pasiūlymus dėl minėtų paslaugų įsigijimo.

10.4. atsako už IS funkcionavimą, naudotojų registravimą ir registravimosi vardų skyrimą, prieigos teisių nustatymą

10.5. įvertina naudotojų pasirengimą dirbti su IS;

10.6. IS valdytojo vadovui rengia pasiūlymus dėl IS kūrimo, palaikymo, priežiūros, techninės, programinės įrangos modernizavimo ir duomenų saugos užtikrinimo;

10.7. administruoja IS ar jos komponentus, nustato pažeidžiamas vietas, parenka ir diegia saugos priemones bei užtikrina jų atitiktį saugos nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimams;

10.8. registruoja elektroninės informacijos saugos incidentus, teikia pasiūlymus dėl minėtų incidentų pašalinimo;

10.9. tvarkydamas IS elektroninę informaciją neatskleidžia ir neperduoda tvarkomos informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija tiek Poliklinikoje, tiek už jos ribų.;

10.10. atsako už IS funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugų administravimą, funkcionavimo užtikrinimą.

10.11. atsako už priskirtų IS komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, duomenų perdavimo tinklų) administravimą, pažeidžiamų vietų nustatymą ir saugos priemonių parinkimą bei jų atitiktį saugos nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimams;

10.12. atlieka kitas šiuose saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose priskirtas funkcijas ir kitus IS valdytojo nurodymus, susijusius su IS sauga.

11. Informacinė sistema tvarkoma vadovaujantis šiais teisės aktais:

11.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

11.2. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas 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 Valstybės informacinių sistemų elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

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

11.4 Lietuvos standartai LST ISO/IEC 29002:2009, LST/IEC 27001/2006, taip pat kiti Lietuvos ir tarptautinės grupės „Informacijos technologija. Saugumo metodai“ standartai;

11.5 Informacinių išteklių valdymo įstatymas;

11.6. Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4d įsakymas Nr. IV-832 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

11.7. Šie Saugos nuostatai ir kiti teisės aktai, kuriais reglamentuojamas elektroninės informacijos tvarkymo teisėtumas, IS valdytojo veikla ir elektroninės informacijos saugos valdymas.

11.8. Bendruoju duomenų apsaugos reglamentu.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

12. IS paskirtis – kaupti, apdoroti ir saugoti Poliklinikos veiklai vykdyti reikalingus duomenis.

13. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių, patvirtintų Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, 4.4 papunkčiu, informacinėje sistemoje tvarkoma elektroninė informacija priskiriama kitai elektroninei informacijai.

14. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių, patvirtintų Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 nutarimu Nr. 716, 5.4 papunkčiu, informacinė sistema priskiriama ketvirtosios kategorijos informacinėms sistemoms.

15. IS sauga turi būti įgyvendinama siekiant išsaugoti IS elektroninės informacijos savybes. Pirmiausia turi būti diegiamos priemonės, skirtos išsaugoti toms elektroninės informacijos savybėms, kurių praradimas turėtų didžiausią įtaką IS darbui.

16. Pasirenkant saugos priemones prioritetas teikiamas toms priemonėms, kurių diegimas reikalauja mažiausiai sąnaudų ir duoda didžiausią efektą.

17. Prioritetinis IS elektroninės informacijos (arba duomenų) pateikimo būdas yra informacinių technologijų ir elektroninių ryšių priemonėmis. Siektinas elektroninės informacijos pasiekiamumo lygis darbo dienomis darbo laiku – 90 procentų.

18. Teisės aktų nustatyta tvarka atliekant informacinių technologijų saugos atitikties vertinimą, būtina:

18.1. Įvertinti saugos nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimų ir realios saugos situacijos atitiktį;

18.2 patikrinti ne mažiau 10 procentų atsitiktinai parinktų IS naudotojų kompiuterinių darbo vietų įdiegtas programas ir jų sąranką;

18.3. patikrinti ir įvertinti IS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktį;

18.4. įvertinti pasirengimą užtikrinti IS veiklos tęstinumą įvykus saugos incidentui.

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

19.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

19.2. informacijos saugos priemonės diegimo kainos adekvatumas saugomos informacijos vertei;

19.3. turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

20. Elektroninės informacijos saugai užtikrinti yra taikomos šios bendrosios programinės įrangos naudojimo nuostatos:

20.1. tarnybinėse stotyse, darbuotojų kompiuterinėse darbo vietose turi būti naudojama tik legali ir saugi programinė įranga.

20.2. Antivirusinės sistemos virusų parašų bazės atnaujinimo ir kompiuterių operacinių sistemų kritinių pataisų diegimo terminai netaikomi toms darbo vietoms, kurios laikinai yra nenaudojamos. Pradėjus naudoti, visos pataisos įdiegiamos per 3 darbo dienas.

21. IS duomenų saugai užtikrinti tarnybinėse stotyse taikomos šios programinės įrangos naudojimo nuostatos:

21.1. operacinių sistemų ir taikomųjų programų sąranka parenkama taip, kad būtų užtikrintas didžiausias saugumo lygis, sustabdomi nereikalingi darbui procesai;

21.2. ribojama ar blokuojama prieiga prie operacinės sistemos prievadų;

21.3. programinę įrangą atnaujina ir kontroliuoja administratorius. Paslaugų tiekėjai programinę įrangą gali atnaujinti tik dalyvaujant administratoriui.

22. Duomenų saugai užtikrinti IS naudotojų, darbuotojų darbo vietose taikomos šios programinės įrangos naudojimo nuostatos:

22.1. įdiegiama programinė įranga, skirta apsisaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.). Antivirusinės sistemos virusų parašų duomenų bazė atnaujinama automatiškai. Ilgiausias leistinas neatnaujinimo laikas – 5 darbo dienos. Kompiuterio operacinė sistemos kritinės pataisos diegiamos automatiškai. Programinę įrangą atnaujina ir kontroliuoja administratorius;

22.2. IS naudotojų paskyros turi būti apribotų teisių, kurios neleidžia įdiegti papildomos programinės įrangos bei keisti sistemos, kompiuterio ar programinės įrangos sisteminių nustatymų. Programinę įrangą diegia administratorius.

23. Pagrindiniai atsarginių kopijų darymo ir atkūrimo reikalavimai:

23.1. Duomenų saugai užtikrinti daromos pagrindinių duomenų atsarginės duomenų kopijos.;

23.2. atsarginės kopijos daromos reguliariai, kiekvieną darbo dieną;

23.3. duomenys kiekvieną darbo dieną (00:00 val. - 08:00 val.) kopijuojami į nutolusią dedikuoto serverio duomenų saugyklą ir saugomos mažiausiai 24 valandas.

23.4. sukurtai atsarginei kopijai nurodoma kopijavimo data;

23.5. darant (padarius) atsargines kopijas, būtina užtikrinti kopijų kokybę;

23.6. atsarginės kopijos turi būti daromos automatiškai. Jas atkurti turi teisę tik administratorius.

IV. REIKALAVIMAI PERSONALUI

24. IS administratorius privalo išmanyti elektroninės informacijos saugos principus, administruoti ir prižiūrėti duomenų bazes ir priskirtas IS posistemes, taip pat mokėti užtikrinti jų saugumą, būti susipažinęs su šiais saugos nuostatais ir kitais saugumo politiką įgyvendinančiais dokumentais.

25. IS duomenų tvarkytojai privalo:

25.1. būti susipažinę su šiais saugos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais;

25.2. mokėti dirbti su Windows operacine sistema, biuro taikomosiomis programomis arba turėti Europos kompiuterio naudotojo pažymėjimą;

25.3. nuolat tobulinti darbo kompiuteriu žinias.

26. IS naudotojai, pastebėję elektroninės informacijos saugos pažeidimų, nusikalstamos veiklos požymių, neveikiančias ar netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones, privalo apie tai pranešti IS administratoriui.

V. BAIGIAMOSIOS NUOSTATOS

27. IS valdytojas, IS administratorius ir IS naudotojai, pažeidę šių Saugos nuostatų ir kitų saugos politiką įgyvendinančių dokumentų nuostatas, atsako teisės aktų nustatyta tvarka.

28. Saugos dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau, kaip kartą per metus.