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

INFORMACINIŲ TECHNOLOGIJŲ SAUGUMO REIKALAVIMŲ DIEGIMO ĮSTAIGOJE TVARKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. VšĮ Klaipėdos rajono savivaldybės Gargždų ligoninės (toliau – Įstaiga), informacinių technologijų reikalavimų diegimo Įstaigoje tvarka (toliau – Tvarka), nustato Įstaigos tvarkomų informacinių technologijų saugos tikslų, elektroninės informacijos saugos užtikrinimo priemonių, saugų elektroninės informacijos valdymą, organizacinius, techninius ir personalui keliamus reikalavimus, naudotojų supažindinimo su saugos dokumentais principus.

II SKYRIUS
ATSAKINGO UŽ IT ŪKĮ KONTROLĖS VEIKSMAI IR DOKUMENTACIJA

2. Atsakingas už Įstaigos IT ūkį asmuo:

2.1. atlieka ir dokumentuoja (aiškiai aprašant) serverių, kompiuterių, kompiuterinių tinklų, programinės įrangos, saugumo įrangos ir kitos su IT ūkiu susijusios techninės ir programinės įrangos ir priemonių inventorizavimą ir auditą. Darbai atliekami periodiškai, kartą per 2 metus;

2.2. atlieka asmens duomenų tvarkymo rizikos vertinimą, kurio metu:

2.2.1. paruošia rizikos vertinimo politiką ir procedūras. Rizikos vertinimo tikslas nustatyti galimą poveikį asmens duomenų konfidencialumui, saugumui ir pasiekiamumui. Visi vertinimai fiksuojami atskiruose dokumentuose. Rizikos vertinimas turi būti atliekamas bent 1-ną kartą per metus;

2.3. paruošia sistemų veiklos atnaujinimo ir tęstinumo nenumatytais avariniais atvejais strategiją ir planą (netikėtumų valdymas), bei tikrinant avarinio asmens duomenų atkūrimo tvarką, atlieka praktinius bandymus ir testavimus. Bent 1-ną (vieną) kartą per metus atlieka bandomąjį duomenų atkūrimą. Atlikus duomenų atkūrimą, atlieka informacinės sistemos funkcionalumo ir duomenų vientisumo ir parengtumo testavimą;

2.4. paruošia strategiją kibernetinių incidentų ir duomenų saugumo pažeidimų atveju bei darbuotojų funkcijų ir veiksmų planą;

2.5. įvertina visas Įstaigos turimas informacines sistemas ar kitus išteklius, kur tvarkomi asmens duomenys pagal tai, kokią įtaką veiklai turės jų neveikimas ar nepasiekiamumas;

2.6. esant poreikiui ar įvykus incidentui sukuria papildomas duomenų apsaugos taisykles ir procedūras;

2.7. Paruošia dokumentaciją ir vykdo registracijas apie:

2.7.1. vartotojų veiksmus;

2.7.2. registruoja ir saugo įvykius ir prisijungimus prie asmens duomenų, pateikiant jų ataskaitas (prisijungimo identifikatorius, data, laikas, trakinė, jungimosi rezultatas (sėkmingas,

nesėkmingas), bylos prie kurių buvo jungtasi, atlikti veiksmai su duomenimis (įvedimas, peržiūra, keitimas, naikinimas)) ir kiti asmens duomenų tvarkymo veiksmai;

2.7.3. paruošia vartotojų prieigos prie duomenų identifikavimo politiką, bei vykdo priežiūrą:

2.7.3.1. privilegijuotų ir paprastų vartotojų išorinių prisijungimų prie duomenų sistemų vertinimas (tikslu administruoti informacinę sistemą bei techninius išteklius;

2.8. periodiškai peržiūri informacines sistemas, duomenų bazes bei veda tinklo įrenginių audito žurnalus (tikslu pastebėti saugos incidentus, nesankcionuotos prieigos bandymus, nepavykusius prisijungimus ir pan.);

2.9. ne rečiau nei kartą per 1 mėnesį peržiūri naudotojų prisijungimų prie duomenų bazės (-ių) įrašų elektroninį žurnalą ir duomenų valdytojui pateikia peržiūra ataskaitas.

III SKYRIUS
PRIEIGOS PRIE SERVERIŲ BEI ASMENS DUOMENŲ KONTROLĖ

3. Atsakingas už Įstaigos IT ūkį asmuo organizuoja bei kontroliuoja prieigą prie serverių bei asmens duomenų apsaugą juose.

4. Atsakingas už Įstaigos IT ūkį asmuo paruošia tvarką klientų prieigai prie savo asmens duomenų. Reikalavimų griežtumas priklauso nuo rizikos analizės rezultatų, t. y., kokios rizikos grupės asmens duomenys yra prieinami prisijungus atitinkamai identifikuojantis. Prieiga prie asmens duomenų suteikiama tik tiems darbuotojams, kuriems ji yra reikalinga jų darbinių funkcijų įgyvendinimui. Su asmens duomenimis konkretūs darbuotojai gali atlikti tik tuos veiksmus, kuriems atlikti jiems yra suteiktos teisės pagal jų užimamas pareigybes ir atliekamas darbines funkcijas.

5. Duomenų kopijavimas į išorines laikmenas turi būti griežtai ribojamas ir kontroliuojamas. Atsakingas už Įstaigos IT ūkį asmuo, esant galimybėms, paruošia duomenų kopijavimo automatinį monitoringą su įvykių automatine registracija elektroniniame žurnale.

6. Informacinės sistemos funkcionalumas suprojektuojamas taip, kad būtų galima detaliai nurodyti, prie kokių duomenų ar jų grupių leidžiama prieiga ir kokias funkcijas su jais galima atlikti.

7. Vartotojų prisijungimo veiksmai prie informacinių sistemų, kuriose tvarkomi asmens duomenys, taip pat prieiga prie asmens duomenų bazių ar failų turi būti griežtai kontroliuojami. Atsakingas asmuo prieigai prie asmens duomenų, paruošia kontrolės tvarką ir taisykles, kurios nustato kas, kaip ir kada kontroliuoja šį procesą. Pagrindinis tokios analizės šaltinis yra informacinės sistemos, duomenų bazės, tarnybinės stoties, ugniasienės ir kitų techninių ir programinių įrenginių kuriami elektroniniai įvykių žurnalai. Siekiant, kad kontrolės procesas būtų patogus, patartina naudoti papildomas programas, kurios integruoja ir apdoroja elektroninių įvykių žurnalų informaciją bei pateikia suvestines pagal pageidaujamus parametras.

8. Informacinėse sistemose turi būti fiksuojami prisijungimų ir prie kitų asmens duomenų įrašai: prisijungimo identifikatorius, bylos, prie kurių buvo jungtasi, datos, laikai, trukmės ir kiti atlikti veiksmai su asmens duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kiti asmens duomenų tvarkymo veiksmai). Prie asmenų duomenų bazių priėjimas turi būti suteiktas tik iš konkrečių kompiuterių, kurie identifikuojami pagal išorinius IP adresus.

9. Jeigu vartotojų identifikavimas vykdomas naudojant slaptažodžius, jie administruojami pagal nustatytas taisykles, kurias paruošia atsakingas už Įstaigos IT asmuo.

Slaptažodžių naudojimo taisyklėse turi būti apibrėžtas jų sudėtingumas, keitimo dažnumas, naikinimas, priminimas, saugojimas ir pan.

10. Esant reikalui ar būtinybei apsunkinti duomenų subjekto identifikavimą ar atskirais atvejais pagal duomenų subjekto prašymą, duomenų subjektui turi būti priskiriami pseudonimai. Pseudonimų suteikimo tvarką paruošia ir įgyvendina atsakingas už Įstaigos IT ūkį asmuo.

IV SKYRIUS
ATSARGINĖS DUOMENŲ KOPIJOS

11. Asmuo atsakingas už IT ūkį, parengia duomenų ir informacinių sistemų programinės įrangos atsarginių kopijų darymo ir duomenų atstatymo politiką, bei atsarginių kopijų saugojimo laikotarpių tvarką. Joje nustatomi išsaugojimo ir apsaugos reikalavimai.

12. Atsarginių kopijų kūrimo metu yra užtikrinama, kad atsarginių kopijų kūrimo procesas atliekamas iki galo. Šis procesas stebimas ir atkreipiamas dėmesys į nepavykusius, nors suplanuotus, atsarginių kopijų kūrimo atvejus.

V SKYRIUS
DUOMENŲ PERDAVIMO SAUGUMAS

13. Atsakingas už IT ūkį paruošia duomenų šifravimo tvarką ir ją įgyvendina. Duomenų šifravimas turi užtikrinti:

13.1. duomenų perdavimo saugumą. Šifravimas taikomas perduodant asmens duomenis bet kuriuo būdu: vidiniu Įstaigos tinklu, interneto tinklu, elektroniniu paštu ar išorinėse duomenų laikmenose. Šifravimo būdas ir jo priemonės taikomos priklausomai nuo asmens duomenų rizikos analizės rezultatų.

13.2. asmens duomenų siuntimą elektroniniu paštu. Asmens duomenys siunčiami elektroniniu paštu, tik panaudojus dvipusius šifravimo raktus tarp adresatų, abiejose pusėse įdiegus atitinkamą programinę įrangą.

13.3. Duomenų perdavimą išorinėse laikmenose. Siunčiant ar perduodant asmens duomenis išorinėje duomenų laikmenoje, duomenys turi būti apsaugoti šifravimo priemonėmis.

VI SKYRIUS
FIZINĖS DUOMENŲ APSAUGOS PRIEMONĖS

14. Saugumo zonos saugomos tinkamomis įėjimo valdymo priemonėmis, kurios užtikrina tik įgalioto personalo įleidimą. Patekti į vietas, kuriose apdorojami arba saugomi konfidencialūs duomenys, turi teisę tik leidimą turintys asmenys, įgyvendinus atitinkamas įėjimo valdymo priemones, pvz., įgyvendinus dviejų veiksnių tapatumo nustatymo mechanizmą.

15. Patekimas į saugumo zonas registruojamas registracijos knygoje arba elektroniniame žurnale.

16. Prieiga prie saugumo zonų arba prie konfidencialių duomenų apdorojimo vietų, trečios šalies (kitų Įstaigų) priežiūros paslaugų personalui suteikiama tik esant poreikiui. Šiai prieigai išduodamas atskiras leidimas.

VII SKYRIUS
DARBUOTOJŲ INFORMAVIMAS IR MOKYMAI

17. Visi Įstaigos darbuotojai informuojami apie Įstaigoje taikomus saugumo reikalavimus ir procedūras. Mokymo medžiagą paruošia ir apmoko asmuo atsakingas už Įstaigos informacines sistemas.