

PATVIRTINTA
Sveikatos apsaugos ministro
2013 m. *gaminio 21* d.
įsakymu Nr. V- 70

ŽMOGAUS AUDINIŲ, LAŠTELIŲ IR ORGANŲ DONORŲ BEI RECIPIENTŲ REGISTRO VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. BENDROSIOS NUOSTATOS

1. Žmogaus audinių, lašelių ir organų donorų bei recipientų registro veiklos tęstinumo valdymo planas (toliau – Planas) nustato Žmogaus audinių, lašelių ir organų donorų bei recipientų registro (toliau – Registras) veiklos tęstinumo užtikrinimą, o jo reikalavimai privalomi visiems informacinės sistemos naudotojams ir turi būti parengtas kiekvienam pastatui, kuriame tvarkomi institucijos informacinės sistemos duomenys.

2. Šis Planas parengtas vadovaujantis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, patvirtintais Lietuvos Respublikos Vyriausybės 1997 m. rugsėjo 4 d. nutarimu Nr. 952 (Žin., 1997, Nr. 83-2075; 2007, Nr. 49-1891), Saugos dokumentų turinio gairėmis, patvirtintomis Lietuvos Respublikos vidaus reikalų ministro 2007 m. gegužės 8 d. įsakymu Nr. 1V-172 (Žin., 2007, Nr. 53-2070), Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techniniais saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr. 127-4866), Žmogaus audinių, lašelių ir organų donorų bei recipientų registro duomenų saugos nuostatais, patvirtintais Lietuvos Respublikos sveikatos ministro 2012 m. rugsėjo 28 d. įsakymu Nr. V-920 (Žin., 2012 Nr. 116-5888) ir kitais teisės aktais, reglamentuojančiais duomenų tvarkymą.

3. Šiame Plane vartojamos sąvokos atitinka Bendruosiuose elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimuose, Saugos dokumentų turinio gairėse, kituose elektroninės informacijos tvarkymą reglamentuojančiuose teisės aktuose, Lietuvos standartuose LST ISO/IEC 27002:2009 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas“ ir LST ISO/IEC 27001:2006 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ apibrėžtas sąvokas.

4. Šis Planas įsigalioja esant elektroninės informacijos saugos incidentui – įvykiui ar veiksmui, kuris gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti

ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

5. Šis Planas pagrįstas šiais principais:

5.1. Registro naudotojų gyvybės ir sveikatos apsauga (būtina užtikrinti visų Registro naudotojų gyvybės ir sveikatos apsaugą ir saugumą, kol trunka elektroninės informacijos saugos incidentas bei likviduojami avarijų padariniai);

5.2. Registro veiklos atkūrimas per 1 valandą (atkuriama pagal šiame Plane numatytą prioritetą (1 priedas));

5.3. Registro naudotojai turi būti pasirašytinai supažindinami su šiuo Planu ir teisės aktais, nustatančiais Registro naudotojų atsakomybę;

5.4. šio Plano veiksmingumas turi būti reguliariai išbandomas.

6. Registro saugos įgaliotinio, Registro administratoriaus, Duomenų valdymo įgaliotinio, Registro naudotojų funkcijos, įgaliojimai ir veiksmai pagal Planą išdėstyti Registro veiklos tęstinumo detalajame Plane (2 priedas).

7. Informacijos, saugos incidentų, įvykusių Registre, tyrimas Biure vyksta vadovaujantis Žmogaus audinių, ląstelių ir organų donorų bei recipientų registro elektroninės informacijos saugos incidentų tyrimo tvarka (3 priedas).

8. Registro veiklos atkūrimas finansuojamas iš Lietuvos Respublikos valstybės biudžeto ir kitų teisės aktuose nustatytų finansavimo šaltinių.

9. Registro veikla laikoma atkurta, jeigu yra atkurtas sistemos prieinamumas (ne mažiau kaip 96 procentus paros laiko) autorizuotiems Registro naudotojams.

II. ORGANIZACINĖS NUOSTATOS

10. Elektroninės informacijos saugos incidentams valdyti ir veiklos atkūrimui organizuoti Biuro direktoriaus įsakymu tvirtinamos 2 grupės: Registro veiklos tęstinumo valdymo grupė (toliau – Valdymo grupė) ir Veiklos atkūrimo grupė (toliau – Atkūrimo grupė).

11. Valdymo grupės tikslas – tirti elektroninės informacijos saugos incidentus, ieškoti priemonių ir būdų sukeltiems padariniams bei žalai likviduoti, užtikrinti Registro veiklos tęstinumą.

12. Valdymo grupę sudaro:

12.1. Valdymo grupės vadovas – Biuro direktoriaus pavaduotojas;

12.2. Valdymo grupės vadovo pavaduotojas – Biuro Teisės ir veiklos priežiūros skyriaus vedėjas;

- 12.3. Valdymo grupės vadovo pavaduotojas – Biuro Komunikacijos skyriaus vedėjas;
- 12.4. Valdymo grupės narys – Registro administratorius.
- 13. Valdymo grupės funkcijos, užtikrinant veiklos tęstinumą:
 - 13.1. nenumatytos situacijos analizė ir sprendimų Registro veiklos tęstinumo valdymo klausimais priėmimas;
 - 13.2. bendravimas su kitų informacinių sistemų veiklos tęstinumo valdymo grupėmis;
 - 13.3. bendravimas su teisėsaugos ir kitomis institucijomis, institucijų darbuotojais ir kitomis interesų grupėmis;
 - 13.4. finansinių ir kitų išteklių, reikalingų Registro veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, nustatymas ir naudojimo kontrolė;
 - 13.5. Registro duomenų fizinė sauga įvykus elektroninės informacijos saugos incidentui;
 - 13.6. logistika (žmonių, daiktų, įrangos gabenimo organizavimas ir jų gabenimas);
 - 13.7. kitos pavestos funkcijos.
- 14. Atkūrimo grupę sudaro:
 - 14.1. Atkūrimo grupės vadovas – Registro saugos įgaliotinis;
 - 14.2. Atkūrimo grupės vadovo pavaduotojas – Registro administratorius;
 - 14.3. Atkūrimo grupės nariai – Biuro Komunikacijos skyriaus vyriausiasis specialistas.
- 15. Atkūrimo grupės veiksmai, įvykus esminiams pokyčiams Registre:
 - 15.1. Registro veiklos atkūrimo priežiūra ir koordinavimas;
 - 15.2. Registro tarnybinės stoties veiklos atkūrimo organizavimas;
 - 15.3. kompiuterių tinklo veikimo atkūrimo organizavimas;
 - 15.4. Registro duomenų atkūrimo organizavimas;
 - 15.5. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;
 - 15.6. darbo kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;
 - 15.7. kitos pavestos funkcijos.
- 16. Valdymo grupė organizuoja posėdį kartą per metus arba įvykus esminiams pokyčiams. Atkūrimo grupė organizuoja posėdį įvykus elektroninės informacijos saugos incidentui. Grupių nariai į posėdžius kviečiami telefonu. Posėdžiai protokoluojami. Valdymo grupėje ir Atkūrimo grupėje bendravimas vyksta telefonu, elektroniniu paštu ar žodžiu esant poreikiui.
- 17. Įvykus saugos incidentui patalpose, kuriose yra Registro tarnybinės stoties administravimo techninė ir programinė įranga:

17.1. Registro administratorius nedelsdamas informuoja apie saugos incidentą Registro saugos įgaliotinį ir Biuro direktoriaus pavaduotoją;

17.2. Biuro direktoriaus pavaduotojas apie saugos incidentą nedelsdamas informuoja Biuro direktorių;

17.3. Biuro direktoriaus pavaduotojas informaciją įrašo Registro saugos incidentų registravimo žurnale (6 priedas), vadovauja Plane nurodytiems veiksams;

17.4. Registro administratorius atkuria Registro tarnybinės stoties darbą, kompiuterių tinklo veiklą, Registro duomenis, Registro techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir apie tai nedelsdamas informuoja Biuro direktoriaus pavaduotoją ir Registro saugos įgaliotinį;

17.5. Biuro direktoriaus pavaduotojas organizuoja žalos Registro duomenims, Registro techninei, programinei įrangai vertinimą, koordinuoja techninės, sisteminės ir taikomosios programinės įrangos, reikalingos Registro veiklai atkurti, išigijimą.

18. Įvykus saugos incidentui patalpose, kuriose yra Registro techninė ir programinė įranga:

18.1. Registro naudotojai apie kritinę situaciją informuoja Registro saugos įgaliotinį, baigia darbą su Registru, šalindami gedimą vykdo saugos įgaliotinio ar Registro administratorių nurodymus;

18.2. Registro saugos įgaliotinis, sužinojęs apie kritinę situaciją, dėl kurios Registro veiklos atkūrimas gali užtrukti ilgiau nei 24 valandas, raštu informuoja Biuro direktorių apie kritinę situaciją, informuoja visus Registro naudotojus, paveda Registro administratoriui atkurti Registro veiklą, informaciją įrašo Registro saugos incidentų registravimo žurnale;

18.3. Registro administratorius, gavęs pranešimą apie kritinę situaciją iš Registro saugos įgaliotinio, imasi visų įmanomų priemonių Registro veiklai atkurti. Apie Registro veiklos atkūrimo darbus ir Registro veiklos atkūrimą informuoja Registro saugos įgaliotinį;

19. Registro duomenų tvarkytojų, Registro administratoriaus, Registro saugos įgaliotinio telefono numeriai, elektroninio pašto adresai nuolat atnaujinami ir skelbiami įstaigos interneto svetainėje.

20. Įstaigos patalpų, kuriose yra Registro tarnybinės stoties administravimo techninė, sisteminė ir taikomoji programinė įranga, detalūs planai saugomi Biuro administracinėse patalpose.

21. Reikalavimai, kurie keliami atsarginėms patalpoms, naudojamoms Registro veiklai atkurti elektroninės informacijos saugos incidento atveju, aprašyti 4 priede.

22. Saugos incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga įsigyjama Viešųjų pirkimų įstatymo nustatyta tvarka, įsigijimo ištekliai padengiami iš valstybės biudžeto ir kitų šaltinių.

23. Įvykus saugos incidentui įstaigos patalpose, duomenys tvarkomi laikantis įstaigos Saugaus informacinės sistemos elektroninės informacijos tvarkymo taisyklėse nurodytų reikalavimų.

III. APRAŠOMOSIOS NUOSTATOS

24. Registro tarnybinės stoties administravimo, Registro techninės ir programinės įrangos sąrašai, Registro specifikacija saugomi Biuro administracinėse patalpose. Už šios įrangos priežiūrą atsakingas Registro administratorius. Nesant sąraše nurodyto atsakingo administratoriaus, jį gali pavaduoti kitas darbuotojas, turintis aukštąjį techninį išsilavinimą ir ne mažesnę kaip 2 metų patirtį informacinių technologijų srityje.

25. Už Registro atsarginių duomenų kopijų darymą, saugojimą, duomenų iš Registro atsarginių duomenų kopijų atkūrimą atsako Biuro direktoriaus įsakymu paskirtas atsakingas asmuo. Programinės įrangos laikmenos ir laikmenos su atsarginėmis duomenų kopijomis saugomos Biuro patalpose. Saugomi duomenys periodiškai archyvuojami, užtikrinamas duomenų atkūrimas įvykus techniniams gedimams.

26. Biuro Teisės ir veiklos priežiūros skyriuje saugomi duomenų teikimo bei kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašai, visų Biuro darbuotojų darbo telefonų numeriai, o Valdymo bei Atkūrimo grupių narių – papildomai dar ir mobiliojo bei namų telefono numeriai, el. pašto ir gyvenamosios vietos adresai.

27. Atsarginių patalpų, naudojamų Registrui atkurti saugos incidento atveju, adresas yra Santariškių g. 2, Vilnius (nuvykti galima automobiliu arba viešuoju transportu).

IV. PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

28. Planas turi būti išbandomas kartą per metus. Plano bandymo metu Veiklos atkūrimo grupė išanalizuoja galimą (sumodeliuotą) elektroninės informacijos saugos incidentą, numato galimus jo sprendimo būdus (5 priedas).

29. Saugos įgaliotinis yra atsakingas už Plano veiksmingumo bandymo metu pastebėtų trūkumų ataskaitos parengimą ir pateikimą Biuro direktoriui bei Plano atnaujinimą po Plano veiksmingumo bandymų ar rizikos veiksnių įvertinimo.

30. Saugos įgaliotinis patvirtintos ataskaitos kopiją el. paštu siunčia Registro valdytojui.

31. Plano veiksmingumo bandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

V. BAIGIAMOSIOS NUOSTATOS

32. Asmenys, pažeidę šio Plano reikalavimus, atsako teisės aktų nustatyta tvarka.
