PATVIRTINTA
Valstybės dokumentų technologinės apsaugos tarnybos prie Finansų ministerijos direktoriaus 2024 m. birželio 12 d. įsakymu Nr. 1-90

SAUGIŲJŲ DOKUMENTŲ IR SAUGIŲJŲ DOKUMENTŲ BLANKŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Saugiųjų dokumentų ir saugiųjų dokumentų blankų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Saugiųjų dokumentų ir saugiųjų dokumentų blankų registro (toliau – Registras) elektroninės informacijos saugos ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) politikas, nustato organizacinius, techninius ir personalui keliamus reikalavimus, užtikrinančius saugų Registro elektroninės informacijos tvarkymą.

2. Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos saugiųjų dokumentų ir saugiųjų dokumentų blankų gamybos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, (toliau – Bendrųjų reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, (toliau – Kibernetinio saugumo reikalavimų aprašas), Saugiųjų dokumentų ir saugiųjų dokumentų blankų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2003 m. gruodžio 22 d. nutarimu Nr. 1648 „Dėl Saugiųjų dokumentų ir saugiųjų dokumentų blankų registro nuostatų patvirtinimo“, (toliau – Registro nuostatai).

3. Registro elektroninės informacijos saugos užtikrinimo prioritetinės kryptys yra:

3.1. organizacinių, techninių ir personalui keliamų reikalavimų, skirtų Registro elektroninės informacijos saugai užtikrinti, įgyvendinimas ir kontrolė;

3.2. Registro elektroninės informacijos vientisumo, konfidencialumo ir prieinamumo užtikrinimas;

3.3. Registro veiklos tęstinumo užtikrinimas;

3.4. Registro naudotojų mokymas elektroninės informacijos saugos klausimais.

4. Registro elektroninės informacijos saugos užtikrinimo tikslai yra:

4.1. sudaryti sąlygas saugiai tvarkyti Registro elektroninę informaciją automatiniu būdu;

4.2. užtikrinti Registro elektroninės informacijos saugos ir kibernetinių incidentų (toliau – elektroninės informacijos saugos incidentas) valdymą ir tyrimą;

4.3. užtikrinti tinkamą Registro programinės ir techninės įrangų, Registro naudotojų kompiuterizuotų darbo vietų, kompiuterių tinklo įrangos funkcionavimą.

5. Saugos nuostatų reikalavimai taikomi:

5.1. Valstybės dokumentų technologinės apsaugos tarnybai prie Finansų ministerijos (toliau – Tarnyba), kuri yra Registro valdytoja ir tvarkytoja, buveinės adresas – L. Sapiegos g. 17, Vilnius;

5.2. Registro naudotojams;

5.3. Registro saugos įgaliotiniui;

5.4. Registro priežiūros administratoriui ir Registro duomenų bazių administratoriui (toliau kartu – Registro administratoriai).

6. Tarnyba, valdydama ir tvarkydama Registrą:

6.1. atsako už Registro elektroninės informacijos saugą, elektroninės informacijos saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir Registro elektroninės informacijos tvarkymo teisėtumą;

6.2. atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka;

6.3. rengia ir tvirtina su Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos (toliau – Nacionalinis kibernetinio saugumo centras) suderintus Registro elektroninės informacijos saugos politiką įgyvendinančius dokumentus (toliau – Registro saugos dokumentai), kitus Registro elektroninės informacijos saugos politiką įgyvendinančius teisės aktus, prižiūri, kaip jų laikomasi;

6.4. teikia Nacionaliniam kibernetinio saugumo centrui techninę informaciją, reikalingą Registro kibernetiniam saugumui įvertinti, Nacionalinio kibernetinio saugumo centro reikalavimu nurodytais formatais ir terminais arba savo iniciatyva;

6.5. organizuoja Registro rizikos įvertinimą, informacinių technologijų saugos atitikties bei atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimus (toliau kartu – atitikties vertinimai);

6.6. skiria Registro saugos įgaliotinį ir Registro administratorius;

6.7. prižiūri Registro techninę ir programinę įrangas;

6.8. užtikrina nepertraukiamą Registro veikimą ir Registro elektroninės informacijos saugą;

6.9. tvarko ir teikia Registro duomenis;

6.10. užtikrina Registro saugos įgaliotinio, Registro administratorių ir Registro naudotojų mokymus ir kvalifikacijos kėlimą elektroninės informacijos saugos klausimais;

6.11. atlieka kitas Registro nuostatuose nustatytas funkcijas.

7. Registro saugos įgaliotinis:

7.1. koordinuoja ir prižiūri elektroninės informacijos saugos politikos įgyvendinimą saugos dokumentuose nustatyta tvarka;

7.2. teikia Tarnybos direktoriui pasiūlymus dėl:

7.2.1. Registro administratorių paskyrimo ir reikalavimų jiems nustatymo;

7.2.2. Registro rizikos įvertinimo;

7.2.3. atitikties vertinimų atlikimo;

7.2.4. Registro saugos dokumentų priėmimo, keitimo;

7.3. koordinuoja Registro elektroninės informacijos saugos incidentų tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos sauga, išskyrus tuos atvejus, kai šią funkciją atlieka Tarnybos direktoriaus įsakymu sudarytos elektroninės informacijos saugos darbo grupės;

7.4. teikia Registro administratoriams ir Registro naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Registro elektroninės informacijos saugos politikos įgyvendinimu;

7.5. turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus kitiems Tarnybos darbuotojams, jeigu tai būtina Registro elektroninės informacijos saugos politikai įgyvendinti;

7.6. parengia vertinimų ataskaitas bei vertinimų metu nustatytų trūkumų šalinimo planus;

7.7. organizuoja Registro veiklos tęstinumo valdymo plano išbandymą;

7.8. supažindina Registro administratorius ir Registro naudotojus su Registro saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą;

7.9. planuoja, periodiškai organizuoja ir vykdo Registro naudotojų mokymą Registro elektroninės informacijos saugos klausimais, informuoja juos apie Registro elektroninės informacijos saugos problemas;

7.10. atlieka kitas Registro saugos dokumentuose, kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, nustatytas ir Bendrųjų reikalavimų apraše jam priskirtas funkcijas.

8. Saugos įgaliotinis negali atlikti administratoriaus funkcijų.

9. Registro priežiūros administratorius:

9.1. užtikrina Registrui funkcionuoti reikalingų techninės ir programinės įrangų įdiegimą, funkcionavimą ir saugą;

9.2. užtikrina Tarnybos interneto svetainės įdiegimą, funkcionavimą ir saugą.

10. Registro duomenų bazių administratorius:

10.1. įdiegia, administruoja ir tvarko Registro duomenų bazę;

10.2. diegia Registro programinę įrangą, techniškai aptarnauja ir prižiūri Registro techninę ir programinę įrangas;

10.3. užtikrina Registro duomenų bazės saugą;

10.4. atsako už Registro duomenų bazės atsarginių kopijų darymą ir duomenų atkūrimą;

10.5. administruoja Registro naudotojų prieigą prie Registro elektroninės informacijos, suteikia jiems teises ir identifikuoja tapatumą;

10.6. analizuoja Registro naudotojų veiksmų registracijos žurnalų įrašus.

11. Registro administratoriai pagal kompetenciją:

11.1. vykdo Registro elektroninės informacijos saugos reikalavimų atitikties nustatymą ir stebėseną;

11.2. vykdo Registro pažeidžiamų vietų nustatymą;

11.3. teikia Tarnybos direktoriui siūlymus dėl Registro priežiūros, techninės ir programinės įrangų modernizavimo ir Registro elektroninės informacijos saugos užtikrinimo;

11.4. reaguoja į Registro elektroninės informacijos saugos incidentus, informuoja apie juos Registro saugos įgaliotinį;

11.5. užtikrina užkardos ir įsilaužimų aptikimo sistemų įdiegimą, funkcionavimą ir stebėseną, teikia Registro saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;

11.6. atlieka kitas Tarnybos direktoriaus, Registro saugos įgaliotinio pavestas, Registro saugos dokumentuose jam priskirtas funkcijas.

12. Registro sąrankos pakeitimus Registro administratoriai atlieka laikydamiesi Registro pokyčių valdymo tvarkos, nustatytos Tarnybos direktoriaus tvirtinamose Registro elektroninės informacijos tvarkymo taisyklėse.

13. Registro administratoriai privalo peržiūrėti Registro sąranką ir Registro būsenos rodiklius reguliariai, ne rečiau kaip kartą per metus arba po Registro pokyčio.

14. Registro elektroninė informacija tvarkoma ir Registro elektroninės informacijos sauga užtikrinama vadovaujantis:

14.1. Valstybės informacinių išteklių valdymo įstatymu;

14.2. Kibernetinio saugumo įstatymu;

14.3. Kibernetinio saugumo reikalavimų aprašu;

14.4. Bendrųjų reikalavimų aprašu;

14.5. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ patvirtinta Informacinių technologijų saugos atitikties vertinimo metodika;

14.6. Lietuvos standartais LST ISO/IEC 27001 ir LST ISO/IEC 27002, taip pat kitais naujausiais Lietuvos ir tarptautiniais grupės „Informacinės technologijos. Saugumo metodai“ standartais, apibūdinančiais saugų elektroninės informacijos tvarkymą;

14.7. Registro nuostatais;

14.8. Registro saugos dokumentais;

14.9. kitais teisės aktais, reglamentuojančiais saugų ir teisėtą Registro elektroninės informacijos tvarkymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. Registras, atlikus valstybės informacinio ištekliaus svarbos vertinimą, priskiriamas vidutinės svarbos valstybės informaciniams ištekliams.

16. Registro saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja Registro rizikos įvertinimą, o prireikus (po esminių organizacinių ar sisteminių Registro pokyčių) ir neeilinį rizikos įvertinimą. Tarnybos direktoriaus rašytiniu pavedimu Registro rizikos įvertinimą gali atlikti pats Registro saugos įgaliotinis arba rizikos įvertinimo paslaugas teikiantis subjektas, su kuriuo sudaryta rizikos įvertinimo paslaugų teikimo sutartis.

17. Rizikos vertintojai turi teisę nuotoliniu būdu arba lokaliai prisijungti prie tikrinamų kompiuterizuotų darbo vietų ar Registro tarnybinių stočių, diegti ir naudoti grėsmių ir pažeidžiamumų, galinčių turėti įtakos Registro elektroninės informacijos saugai, nustatymams skirtą programinę įrangą, šalinti tikrinimo metu rastus pažeidžiamumus. Draudžiama pasinaudoti rizikos įvertinimo metu rastais pažeidžiamumais, atlikti veiksmus, galinčius pakenkti Registro funkcionalumui, Registro elektroninės informacijos ar asmens duomenų apsaugai.

18. Rizikos įvertinimo metu:

18.1. nustatomos grėsmės ir pažeidžiamumai, galintys turėti įtakos Registro elektroninės informacijos saugai, jų poveikio Registro veiklai sritys;

18.2. įvertinamos Registro pažeidimo grėsmių tikimybė ir pasekmės;

18.3. nustatomas rizikos lygis, įvertinama identifikuotų grėsmių tikimybė ir jos išdėstomos prioriteto tvarka pagal svarbą, nustatytą rizikos įvertinimo metu.

19. Registro rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama Tarnybos direktoriui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos Registro elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausieji rizikos veiksniai yra šie:

19.1. subjektyvūs netyčiniai (Registro 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);

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

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

20. Tarnybos direktorius, atsižvelgdamas į Registro rizikos įvertinimo ataskaitą, prireikus tvirtina Registro rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomos techninės ir administracinės rizikos veiksnius šalinančios priemonės, priemonių vykdymo terminai, vykdytojai, kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti. Nustačius kibernetinių incidentų valdymo ir šalinimo, Tarnybos nepertraukiamos veiklos užtikrinimo trūkumų, Registro rizikos įvertinimo ir rizikos valdymo priemonių plane numatomas ir Registro veiklos tęstinumo valdymo plano tobulinimas.

21. Ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip, organizuojami ir atliekami atitikties vertinimai:

21.1. Registro informacinių technologijų saugos atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka;

21.2. atitikties vertinimai gali būti atliekami kartu su Registro rizikos įvertinimu;

21.3. atlikus atitikties vertinimus, rengiamos Registro informacinių technologijų saugos atitikties vertinimo ataskaita ir Registro atitikties kibernetinio saugumo reikalavimams vertinimo ataskaita, kurios pateikiamos Tarnybos direktoriui, taip pat parengiamas atitikties vertinimų metu pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Tarnybos direktorius.

22. Techninės, programinės ir organizacinės Registro elektroninės informacijos saugos priemonės pasirenkamos taip, kad būtų užtikrintas Registro veiklos tęstinumas, patiriant kuo mažiau išlaidų, Registro informacijos saugos priemonės diegimo kaina būtų adekvati saugomos informacijos vertei, liekamoji rizika būtų sumažinta iki priimtino lygio.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

23. Registro tarnybinėse stotyse ir Registro naudotojų kompiuterizuotose darbo vietose privalo būti įdiegta centralizuotai valdoma programinė įranga, realiu laiku vykdanti apsaugą nuo kenksmingos programinės įrangos (virusų, įsibrovimo, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir panašiai). Jos naudojimo nuostatos ir jos atnaujinimo reikalavimai (ilgiausias leistinas neatnaujinimo laikas) nustatomi Registro saugaus elektroninės informacijos tvarkymo taisyklėse.

24. Registro tarnybinėse stotyse ir Registro naudotojų kompiuterizuotose darbo vietose turi būti naudojama tik legali programinė įranga. Šios programinės įrangos naudojimo nuostatos, atnaujinimo ir kiti reikalavimai nustatomi Registro saugaus elektroninės informacijos tvarkymo taisyklėse.

25. Registro tarnybinės stotys ir Registro naudotojų kompiuterizuotos darbo vietos turi būti apsaugotos kompiuterių tinklo filtravimo įranga (užkardomis, turinio kontrolės sistemomis, įgaliotaisiais serveriais (angl. *proxy*) ir kita). Kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos Registro saugaus elektroninės informacijos tvarkymo taisyklėse.

26. Leistinos Registro naudotojų kompiuterizuotų darbo vietų naudojimo ribos:

26.1. Registro naudotojų kompiuterizuotos darbo vietos įrengiamos tik Tarnybos patalpose;

26.2. ne Tarnybos darbuotojams draudžiama naudotis Tarnybos kompiuterizuotomis darbo vietomis, išskyrus atvejus, kai tai būtina atliekant mokymus ar prezentacijas;

26.3. mobilieji įrenginiai (tarp jų ir nešiojamieji kompiuteriai) darbui su Registro elektronine informacija nenaudojami;

26.4. Registro tarnybinių stočių ir kompiuterizuotų darbo vietų gedimai šalinami Tarnybos patalpose. Jei gedimo pašalinti vietoje nepavyksta, iš perduodamų remontuoti ar nurašomų kompiuterių turi būti pašalinta visa su Registru susijusi elektroninė informacija.

27. Metodai, kuriais leidžiama užtikrinti saugų Registro elektroninės informacijos teikimą ir (ar) gavimą:

27.1. prieiga prie Registro elektroninės informacijos suteikiama įgyvendinus Registro naudotojų administravimo taisyklėse nurodytas Registro naudotojų tapatybės nustatymo ir patvirtinimo priemones;

27.2. prieiga prie Registro iš vidaus ir iš išorės yra ribojama užkardomis;

27.3. prieiga prie Registro belaidžiais tinklais yra draudžiama;

27.4. elektroninė informacija Registro naudotojams perduodama HTTPS protokolu;

27.5. elektroninė informacija nuotoliniams Registro duomenų gavėjams perduodama Saugiu valstybiniu duomenų perdavimo tinklu pagal Registro elektroninės informacijos teikimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, saugaus elektroninės informacijos perdavimo sąlygos ir tvarka;

27.6. elektroninė informacija iš kitų valstybės institucijų gaunama Registro nuostatuose nustatyta tvarka;

27.7. per metus Registro ir Tarnybos interneto svetainės prieinamumas turi būti užtikrinamas ne mažiau kaip 96 proc. laiko darbo metu darbo dienomis.

28. Pagrindiniai Registro atsarginių elektroninės informacijos kopijų (toliau – kopijos) darymo ir atkūrimo reikalavimai:

28.1. kopijos daromos automatiniu būdu kiekvieną dieną ir saugomos Registro tarnybinėse stotyse ir atskiroje kopijų saugojimo tarnybinėje stotyje;

28.2. atkurti elektroninę informaciją iš kopijų turi teisę tik Registro duomenų administratorius ar jį pavaduojantis asmuo;

28.3. kopijų darymo ir saugojimo tvarka nustatyta Registro saugaus elektroninės informacijos tvarkymo taisyklėse.

29. Tarnybos interneto svetainė turi atitikti Kibernetinio saugumo reikalavimų aprašo priede valstybės informacinį išteklių ar ypatingos svarbos informacinės infrastruktūros naudojamos interneto svetainės, pasiekiamos iš viešųjų elektroninių ryšių tinklų, saugumui ir kontrolei keliamus reikalavimus.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

30. Registro saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Registro saugos dokumentų, Bendrųjų reikalavimų aprašo, Kibernetinio saugumo reikalavimų aprašo, Informacinių technologijų saugos atitikties vertinimo metodikos, kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą.

31. Registro administratoriai privalo išmanyti pagrindinius elektroninės informacijos saugos politikos principus, darbą su duomenų perdavimo tinklais, užtikrinti jų saugumą, turėti naudojamų operacinių sistemų ir duomenų bazių administravimo ir priežiūros patirties, būti susipažinę su Registro nuostatais, Registro saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais elektroninės informacijos saugą.

32. Registro saugos įgaliotiniu, Registro administratoriumi 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 vieni metai.

33. Registro naudotojai privalo turėti darbo kompiuteriu įgūdžių, saugaus darbo su duomenimis pagrindus, mokėti tvarkyti Registro elektroninę informaciją Registro nuostatų nustatyta tvarka, būti susipažinę su Saugos nuostatais bei kitais Registro elektroninės informacijos saugos politiką įgyvendinančiais teisės aktais.

34. Registro saugos įgaliotinio, Registro administratorių ir Registro naudotojų mokymus ir kvalifikacijos tobulinimą užtikrina Tarnyba.

35. Registro saugos įgaliotinis ne rečiau kaip kartą per metus suplanuoja ir inicijuoja Registro naudotojų mokymą elektroninės informacijos saugos klausimais, periodiškai įvairiais būdais primena apie saugumo problemas (pvz., pranešimai elektroniniu paštu, naujų darbuotojų instruktavimas ir pan.). Mokymai gali būti vykdomi tiesioginiu ar nuotoliniu būdu.

36. Tarnybos sprendimu mokymai gali būti organizuojami ir atsiradus poreikiui.

V SKYRIUS
REGISTRO NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

37. Registro saugos įgaliotinis, Registro administratoriai ir Registro naudotojai privalo būti susipažinę su Saugos nuostatais ir kitais Registro saugos dokumentais bei dokumentų valdymo

sistemos priemonėmis patvirtinę, kad laikysis šiuose dokumentuose nustatytų reikalavimų prieš jiems suteikiant teisę dirbti su Registru.

38. Registro administratorius ir Registro naudotojus su Saugos nuostatais ir kitais Registro saugos dokumentais bei atsakomybę už šiuose dokumentuose nustatytų reikalavimų nesilaikymą dokumentų valdymo sistemos priemonėmis supažindina Registro saugos įgaliotinis.

39. Atlikus Saugos nuostatų ar kitų Registro saugos dokumentų pakeitimus, su šiais dokumentais Registro naudotojai pakartotinai supažindinami per 10 darbo dienų pasirašytinai.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

40. Registro saugos įgaliotinis Registro saugos dokumentus turi peržiūrėti ir prireikus inicijuoti pakeitimą ne rečiau kaip kartą per kalendorinius metus, taip pat ir atlikus Registro rizikos įvertinimą, Registro informacinių technologijų saugos atitikties vertinimą, pasikeitus Tarnybos struktūrai.

41. Registro saugos dokumentai turi būti derinami su Nacionaliniu kibernetinio saugumo centru, išskyrus atvejus, kai keičiant minėtus dokumentus atliekami tik redakciniai ar nedideli nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika.

42. Patvirtinus Registro saugos dokumentus ar jų pakeitimus, Registro rizikos įvertinimo ataskaitą, rizikos įvertinimo ir rizikos valdymo priemonių planą, saugos atitikties vertinimo ataskaitą ir pastebėtų trūkumų šalinimo planą, jų kopijas Tarnyba ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

43. Patvirtinus Saugos nuostatus ar jų pakeitimus, Tarnyba Registrų ir valstybės informacinių sistemų registro nuostatų nustatyta tvarka pateikia šiam registrui reikiamus duomenis ar dokumentų kopijas.

44. Patvirtinus Registro veiklos tęstinumo valdymo plano veiksmingumo išbandymo ir pastebėtų trūkumų ataskaitą, jos kopiją Tarnyba ne vėliau kaip per penkias darbo dienas pateikia Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos.

45. Registro saugos įgaliotinis, Registro administratoriai ir Registro naudotojai, pažeidę Registro saugos dokumentuose nustatytus reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____