LIETUVOS RESPUBLIKOS ŠVIETIMO IR MOKSLO MINISTRAS

ĮSAKYMAS
DĖL ŠVIETIMO IR MOKSLO MINISTRO 2006 M. BALANDŽIO 28 D. ĮSAKYMO NR. ISAK-812 „DĖL STUDIJŲ IR MOKYMO PROGRAMŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2016 m. gegužės 20 d. Nr. V-456
Vilnius

1. P a k e i č i u Lietuvos Respublikos švietimo ir mokslo ministro 2006 m. balandžio 28 d. įsakymą Nr. ISAK-812 „Dėl Studijų ir mokymo programų registro duomenų saugos nuostatų patvirtinimo“ ir išdėstau jį nauja redakcija:

„LIETUVOS RESPUBLIKOS ŠVIETIMO IR MOKSLO MINISTRAS

ĮSAKYMAS
DĖL STUDIJŲ, MOKYMO PROGRAMŲ IR KVALIFIKACIJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu 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 elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7 punktu:

T v i r t i n u Studijų, mokymo programų ir kvalifikacijų registro duomenų saugos nuostatus (pridedama).“

2. P a v e d u Švietimo informacinių technologijų centrui per 3 mėnesius nuo šio įsakymo įsigaliojimo dienos:

2.1. pateikti švietimo ir mokslo ministrui tvirtinti Studijų, mokymo programų ir kvalifikacijų registro saugaus elektroninės informacijos tvarkymo taisykles, Studijų, mokymo programų ir kvalifikacijų registro veiklos tęstinumo valdymo planą, Studijų, mokymo programų ir kvalifikacijų registro naudotojų administravimo taisykles;

2.2. paskirti Studijų, mokymo programų ir kvalifikacijų registro saugos įgaliotinį.

Švietimo ir mokslo ministrė Audronė Pitrėnienė

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2016 m. gegužės 6 d. raštu Nr. 1D-2874

PATVIRTINTA
Lietuvos Respublikos švietimo ir mokslo
ministro 2006 m. balandžio 28 d. įsakymu
Nr. ISAK-812
(Lietuvos Respublikos švietimo ir mokslo
ministro 2016 m. gegužės 20 d.
įsakymo Nr. V-456 redakcija)

STUDIJŲ, MOKYMO PROGRAMŲ IR KVALIFIKACIJŲ REGISTRO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Studijų, mokymo programų ir kvalifikacijų registro duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato Studijų, mokymo programų ir kvalifikacijų registro (toliau – Registras) tvarkomos elektroninės informacijos saugos tikslus, elektroninės informacijos saugos užtikrinimo prioritetines kryptis, saugų elektroninės informacijos valdymą, organizacinius, techninius ir personalui keliamus reikalavimus, naudotojų supažindinimo su“ saugos dokumentais principus, apibrėžia elektroninės informacijos saugos politiką.

2. Saugos nuostatuose vartojamos sąvokos apibrėžtos Saugos nuostatų 14.1, 14.2, 14.5 ir 14.11 papunkčiuose išvardintuose teisės aktuose ir Studijų, mokymo programų ir kvalifikacijų registro nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2015 m. rugpjūčio 26 d. nutarimu Nr. 895 „Dėl Studijų, mokymo programų ir kvalifikacijų registro reorganizavimo ir studijų, mokymo programų ir kvalifikacijų registro nuostatų patvirtinimo“, (toliau – Registro nuostatai).

3. Registro elektroninės informacijos saugumas užtikrinamas, vadovaujantis šiomis prioritetinėmis kryptimis:

3.1. įgyvendinant atliekamų veiksmų su Registro elektronine informacija automatinį stebėjimą ir įrašų kaupimą;

3.2. suteikiant naudotojams prieigos teises prie Registro elektroninės informacijos ir identifikuojant Registro naudotojų tapatumą;

3.3. kopijuojant Registro duomenų bazę, saugant archyve esančias kopijas;

3.4. saugant Registro elektroninę informaciją nuo žalingos programinės įrangos poveikio;

3.5. įrengiant saugias Registrui tvarkyti skirtas patalpas ir kompiuterizuotas darbo vietas jose;

3.6. tobulinant Registro naudotojų kvalifikaciją;

3.7. įgyvendinant Registro elektroninės informacijos integralumą su švietimo ir mokslo registrais ir informacinėmis sistemomis;

3.8. įgyvendinant Registro elektroninės informacijos saugos priemones nuo nesankcionuoto poveikio Registro programinei, techninei įrangai ir (ar) Registro programinės įrangos modifikavimo;

3.9. įgyvendinant Registro veiklos tęstinumą.

4. Registro elektroninės informacijos saugumo užtikrinimo tikslas – sudaryti sąlygas automatizuotu būdu saugiai rinkti, apdoroti, kaupti, saugoti Registro elektroninę informaciją ir ją teikti švietimo ir mokslo registrams, informacinėms sistemoms, suinteresuotiems juridiniams ir fiziniams asmenims.

5. Saugos nuostatai nustato Registro saugos politiką (toliau – saugos politika). Saugos politika įgyvendinama, vadovaujantis Studijų, mokymo programų ir kvalifikacijų registro saugaus elektroninės informacijos tvarkymo taisyklėmis, Studijų, mokymo programų ir kvalifikacijų registro

veiklos tęstinumo valdymo planu, Studijų, mokymo programų ir kvalifikacijų registro naudotojų administravimo taisyklėmis, Studijų, mokymo programų ir kvalifikacijų registro duomenų kopijų kūrimo tvarkos aprašu ir kitais teisės aktais, reglamentuojančiais Registro duomenų tvarkymo teisėtumą ir saugos valdymą.

6. Saugos nuostatai ir saugos politiką įgyvendinantys teisės dokumentai privalomi:

6.1. Registro valdytojui – Lietuvos Respublikos švietimo ir mokslo ministerijai, buveinės adresas – A. Volano g. 2, LT-01516 Vilnius;

6.2. Registro tvarkytojui – Švietimo informacinių technologijų centrui, buveinės adresas – Suvalkų g. 1, LT-03113 Vilnius;

6.3. Registro naudotojams;

6.4. Registro saugos įgaliotiniui;

6.5. Registro administratoriui.

7. Registro valdytojas:

7.1. pagal kompetenciją atsako už saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą;

7.2. tvirtina Studijų, mokymo programų ir kvalifikacijų registro saugos nuostatus, Studijų, mokymo programų ir kvalifikacijų registro saugaus elektroninės informacijos tvarkymo taisykles, Studijų, mokymo programų ir kvalifikacijų registro veiklos tęstinumo valdymo planą, Studijų, mokymo programų ir kvalifikacijų registro naudotojų administravimo taisykles (toliau visi kartu – saugos dokumentai) ir kitus teisės aktus, kuriuose reglamentuojamas Registro tvarkymo teisėtumas ir Registro elektroninės informacijos sauga;

7.3. koordinuoja Registro tvarkytojo darbą;

7.4. analizuoja Registro tvarkytojo pateiktus siūlymus, priima sprendimus dėl Registro techninių ir programinių priemonių, būtinų Registro elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

7.5. atlieka kitas Registro nuostatų ir saugos dokumentų jam priskirtas funkcijas.

8. Registro tvarkytojas:

8.1. pagal kompetenciją atsako už Registro elektroninės informacijos tvarkymo teisėtumą ir saugą;

8.2. užtikrina tinkamų organizacinių ir techninių priemonių, skirtų elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo, įgyvendinimą;

8.3. pagal kompetenciją vykdo reikalavimus, nustatytus saugos dokumentuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose;

8.4. teikia siūlymus Registro valdytojui dėl Registro elektroninės informacijos saugos tobulinimo, Registro saugos dokumentų priėmimo, keitimo arba panaikinimo, taip pat rengia saugos dokumentų projektus;

8.5. užtikrina, kad Registro naudotojai, turintys teisę naudotis Registro elektronine informacija, laikytųsi reikalavimų, nustatytų saugos dokumentuose;

8.6. atlieka Registro duomenų bazės techninę priežiūrą ir užtikrina nepertraukiamą Registro veikimą;

8.7. užtikrina saugią Registro sąveiką su susijusiais registrais ir informacinėmis sistemomis;

8.8. užtikrina saugų Registro funkcijų pokyčių įgyvendinimą;

8.9. teikia siūlymus Registro valdytojui dėl Registro techninių ir programinių priemonių, būtinų Registro elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo, organizuoja jų įdiegimą ir modernizavimą;

8.10. Registro valdytojo pavedimu skiria Registro duomenų valdymo įgaliotinį, paveda jam atlikti Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme nustatytas informacinių išteklių valdymo funkcijas;

8.11. skiria Registro saugos įgaliotinį, paveda jam organizuoti Registro saugos politiką ir kontroliuoti jos įgyvendinimą;

8.12. skiria Registro administratorių, paveda jam vykdyti administravimo funkcijas, nustatytas Saugos nuostatuose ir kituose Registro saugos politiką įgyvendinančiuose teisės aktuose;

8.13. teisės aktų nustatyta tvarka teikia informaciją apie Registro saugos politikos įgyvendinimą;

8.14. atlieka kitas Registro valdytojo pavestas, Registro nuostatuose, saugos dokumentuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose jam priskirtas funkcijas.

9. Registro saugos įgaliotinis:

9.1. atsako už tinkamą Registro elektroninės informacijos saugos priemonių įgyvendinimą;

9.2. teikia Registro tvarkytojo vadovui siūlymus dėl Registro administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo;

9.3. teikia Registro tvarkytojo vadovui siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo;

9.4. teikia Registro valdytojui siūlymus dėl saugos dokumentų priėmimo arba keitimo;

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

9.6. organizuoja Registro rizikos įvertinimą ir parengia Registro rizikos įvertinimo ataskaitą (toliau – Rizikos įvertinimo ataskaita);

9.7. teikia Registro administratoriui ir Registro naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

9.8. turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems Registro tvarkytojo darbuotojams, jeigu tai būtina saugos politikai įgyvendinti;

9.9. supažindina Registro administratorių ir Registro naudotojus su saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą, organizuoja Registro naudotojų mokymą elektroninės informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

9.10. atlieka kitas Registro tvarkytojo vadovo pavestas, saugos dokumentuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose jam priskirtas funkcijas.

10. Registro administratoriaus funkcijas pagal kompetenciją vykdo Registro sisteminės priežiūros administratorius ir Registro tvarkymo administratorius.

11. Registro sisteminės priežiūros administratorius:

11.1. užtikrina Registro techninės ir programinės įrangos įdiegimą ir funkcionavimą;

11.2. diegia ir prižiūri programinę įrangą, reikalingą Registro naudotojų funkcijoms vykdyti;

11.3. suteikia teisę Registro naudotojams naudotis elektronine informacija, kurios reikia jų funkcijoms atlikti;

11.4. užtikrina Registro duomenų bazėje naudojamų klasifikatorių atnaujinimą automatiniu būdu;

11.5. užtikrina Registro komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimų aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą, pagal kompetenciją nustato Registro pažeidžiamas vietas;

11.6. užtikrina sąveikos su susijusiais registrais ir informacinėmis sistemomis technologinį funkcionavimą;

11.7. užtikrina, kad Registro elektroninė informacija, gauta iš susijusių registrų ir informacinių sistemų, būtų nuolat atnaujinama ir atitiktų susijusiuose registruose ir informacinėse sistemose esančią elektroninę informaciją;

11.8. pagal kompetenciją dalyvauja, vykdant saugumo reikalavimų įgyvendinimo stebėseną;

11.9. pagal kompetenciją teikia Registro tvarkytojo vadovui siūlymus dėl Registro palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

11.10. informuoja Registro saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

11.11. atsako už Registro duomenų bazės saugų atsarginių kopijų darymą ir archyve esančių kopijų saugojimą;

11.12. atlieka kitas Registro tvarkytojo vadovo, Registro saugos įgaliotinio pavestas, saugos dokumentuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose jam priskirtas funkcijas.

12. Registro tvarkymo administratorius:

12.1. administruoja ir tvarko Registro duomenų bazę, užtikrina tinkamą ir nepertraukiamą Registro veikimą;

12.2. administruoja Registro naudotojų prieigą prie Registro elektroninės informacijos – suteikia jiems teises ir identifikuoja tapatumą;

12.3. administruoja Registro naudotojų veiksmų automatinį stebėjimą;

12.4. informuoja Registro duomenų gavėjus, kuriems buvo perduota neteisinga, netiksli, neišsami Registro elektroninė informacija, apie ištaisytus netikslumus;

12.5. pagal kompetenciją dalyvauja, vykdant elektroninės informacijos saugos reikalavimų įgyvendinimo stebėseną;

12.6. pagal kompetenciją teikia Registro tvarkytojo vadovui siūlymus dėl Registro palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

12.7. informuoja Registro saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

12.8. atlieka kitas Registro tvarkytojo vadovo, Registro saugos įgaliotinio pavestas, saugos dokumentuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose jam priskirtas funkcijas.

13. Registro tvarkytojas užtikrina, kad naudotojai laikytųsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose teisės aktuose nurodytų reikalavimų.

14. Teisės aktai, kuriais vadovaujamasi, tvarkant Registro elektroninę informaciją ir užtikrinant jos saugumą:

14.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

14.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

14.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

14.4. Lietuvos Respublikos dokumentų ir archyvų įstatymas;

14.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu 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 elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

14.6. Saugos dokumentų turinio gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu 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 elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

14.7. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu 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 elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

14.8. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl

Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

14.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

14.10. Bendrieji reikalavimai organizacinėmis ir techninėmis duomenų saugumo priemonėms, patvirtinti Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“;

14.11. Lietuvos standartai LST ISO/IEC 27002:2014, LST ISO/IEC 27001:2013, kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, nustatantys saugų elektroninės informacijos tvarkymą;

14.12. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą valstybės institucijose.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. Vadovaujantis Saugos nuostatų 14.5 punkte nurodyto aprašo 4.3 papunkčiu, Registre tvarkoma informacija priskiriama žinybinės svarbos elektroninės informacijos kategorijai. Priskyrimo šiai elektroninės informacijos svarbos kategorijai kriterijai: Registro elektroninės informacijos praradimas gali padaryti žalą vieno ar kelių fizinių ar juridinių asmenų teisėtiems interesams, gali turėti neigiamų padarinių institucijos veiklai.

16. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.3 papunkčiu, Registras priskiriamas trečiajai informacinių sistemų kategorijai. Priskyrimo šiai informacinių sistemų kategorijai kriterijus – Registre apdorojama žinybinės svarbos elektroninė informacija.

17. Registro saugos įgaliotinis:

17.1. atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja Registro rizikos įvertinimą. Pasikeitus Registro duomenų bazės struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų šalinimas ir kt.) ar nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis Registro rizikos įvertinimas;

17.2. Registro rizikos įvertinimą išdėsto Rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama, atsižvelgus į rizikos veiksnius, galinčius turėti ar turinčius įtakos Registro elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę, galimus rizikos valdymo būdus. Svarbiausieji rizikos veiksniai yra šie:

17.2.1. subjektyvūs netyčiniai (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, netinkamas veikimas ir kita);

17.2.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis elektronine informacija, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

17.2.3. 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;

17.3. patvirtintą Rizikos įvertinimo ataskaitos kopiją paštu išsiunčia Registro valdytojui.

18. Registro tvarkytojo vadovui patvirtinus Rizikos įvertinimo ataskaitą, prireikus rengiamas rizikos įvertinimo ir rizikos valdymo priemonių planas, kuriame numatomos techninės ir administracinės veiksnius šalinančios priemonės, priemonių vykdymo terminai, vykdytojai ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti. Šį planą tvirtina Registro valdytojas.

19. Registro elektroninei informacijai, techninei, programinei įrangai, patalpoms Registro tvarkytojo įstaigoje vertinti naudojama penkiabalė rizikos veiksnių tikėtumo ir žalos vertinimo metodika:

19.1. nereikšminga rizikos veiksnių tikimybė, žala – 1 balas;

19.2. maža rizikos veiksnių tikimybė, žala – 2 balai;

19.3. vidutinė rizikos veiksnių tikimybė, žala – 3 balai;

19.4. didelė rizikos veiksnių tikimybė, žala – 4 balai;

19.5. labai didelė rizikos veiksnių tikimybė, žala – 5 balai.

20. Saugos priemonės parenkamos, įvertinus galimus rizikos veiksnius Registro elektroninės informacijos vientisumui ir prieinamumui.

21. Registro elektroninės informacijos saugos priemonių parinkimo pagrindiniai principai yra tokie:

21.1. saugos priemonės turi būti valdomos centralizuotai;

21.2. saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;

21.3. likutinė rizika turi būti sumažinta iki priimtino lygio;

21.4. kur galima, būtina įdiegti prevencines informacijos saugos priemones;

21.5. Registro veiklos tęstinumo ir elektroninės informacijos sauga turi būti užtikrinama, patiriant kuo mažiau išlaidų.

22. Siekiant įvertinti saugos dokumentų nuostatų įgyvendinimo kontrolę, kartą per dvejus metus organizuojamas informacinių technologijų saugos atitikties vertinimas:

22.1. įvertinama saugos dokumentų ir realios informacijos saugos situacijos atitiktis;

22.2. inventorizuojama Registro techninė ir programinė įranga;

22.3. patikrinama (įvertinama) Registro naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis saugos dokumentams;

22.4. įvertinamas pasirengimas užtikrinti Registro veiklos tęstinumą, įvykus saugos incidentui.

23. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Registro tvarkytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus skiria ir įgyvendinimo terminus nustato Registro valdytojo vadovas.

24. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano, informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas Registro valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų įsigaliojimo dienos turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

25. Programinės įrangos, skirtos Registrui nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

25.1. Registro tarnybinių stočių ir kompiuterinėse darbo vietose turi būti įdiegtos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos automatiniu būdu;

25.2. turi būti naudojamos priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą, veikiančią sisteminiuose kataloguose esančiose tarnybinės stoties rinkmenose ir visuose kompiuterių tinklo kompiuteriuose;

25.3. turi būti naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų;

25.4. apsaugai naudojama programinė įranga privalo atsinaujinti ne rečiau kaip kartą per 24 valandas.

26. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo nuostatos:

26.1. turi būti naudojama tik legali, Registro funkcijoms vykdyti būtina programinė įranga, tik iš Registro saugos įgaliotinio parengto ir su Registro valdytojo vadovu suderinto leistinos programinės įrangos sąrašo, atnaujinamo ne rečiau kaip kartą per metus;

26.2. programinė įranga turi būti nuolatos atnaujinama, laikantis gamintojo reikalavimų;

26.3. programinę įrangą diegti, šalinti ir konfigūruoti gali tik Registro administratorius;

26.4. turi būti įdiegta prieigos prie Registro elektroninės informacijos per registravimąsi, teisių suteikimą ir slaptažodžius sistema;

26.5. turi būti įgyvendinta prievolė ne rečiau kaip kas 3 mėnesius keisti slaptažodžius;

26.6. turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie Registro elektroninės informacijos, atliktus veiksmus.

27. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita) pagrindinės naudojimo nuostatos:

27.1. Registro elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų, naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami;

27.2. Registro programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. SQL *injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. DOS), dedikuoto atkirtimo nuo paslaugos (angl. DDOS);

27.3. informacinės sistemos tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių Registro naudotojų kompiuterinę įrangą nuo kenksmingo kodo.

28. Leistinos kompiuterių naudojimo ribos:

28.1. stacionarūs ir nešiojamieji Registro naudotojų kompiuteriai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi Registro duomenys ir Registro informacija;

28.2. nešiojamieji kompiuteriai gali būti naudojami tik suvestiniams (viešiems) Registro duomenims ir negali būti naudojami Registro duomenims registruoti, kaupti ir apdoroti;

28.3. nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis;

28.4. Registro naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo;

28.5. kai nešiojamieji kompiuteriai nenaudojami, jie turi būti saugomi saugioje vietoje;

28.6. Registro tvarkytojo stacionarų kompiuterį prijungti prie Registro kompiuterių tinklo gali tik Registro administratorius.

29. Metodai, kuriais užtikrinamas saugus Registro elektroninės informacijos teikimas ir (ar) gavimas:

29.1. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų valdytojų valdomų susijusių registrų ir informacinių sistemų, naudojami saugūs ryšio kanalai, kuriais perduodami šifruoti duomenys;

29.2. elektroninė informacija iš su Registru susijusių registrų gaunama tik pagal duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

29.3. prieigos prie Registro elektroninės informacijos teises gali suteikti tik Registro administratorius. Registro naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

29.4. prieiga prie Registro elektroninės informacijos leidžiama tik per registravimosi slaptažodžių sistemą. Prieigos prie Registro elektroninės informacijos valdymas apibrėžtas Studijų, mokymo programų ir kvalifikacijų registro naudotojų administravimo taisyklėse;

29.5. pasibaigus Registro naudotojo darbo sutarčiai, teisė naudotis Registro elektronine informacija turi būti panaikinta. Registro naudotojui prieiga prie Registro turi būti ribojama ar sustabdoma, kai vyksta Registro naudotojo veiklos tyrimas, naudotojas yra ilgalaikėse atostogose arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos.

30. Registro atsarginės duomenų bazės kopijos daromos automatiniu būdu kiekvieną dieną, esant aktyviai Registro duomenų bazei. Kopijos turi būti saugomos kitoje patalpoje, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota. Prireikus jas atkurti turi teisę tik administratorius ar jį pavaduojantis asmuo. Kopijų darymo ir saugojimo tvarka detaliai aprašyta Studijų, mokymo programų ir kvalifikacijų registro saugaus elektroninės informacijos tvarkymo taisyklėse.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

31. Registro saugos įgaliotiniu 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, arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jo paskyrimo praėję mažiau kaip vieneri metai.

32. Registro saugos įgaliotinis turi:

32.1. išmanyti elektroninės informacijos saugos užtikrinimo principus;

32.2. sugebėti vertinti rizikos veiksnių tikėtumus ir žalos galimybes, organizuoti ir kontroliuoti trūkumų šalinimą;

32.3. tobulinti kvalifikaciją elektroninės informacijos saugos srityje;

32.4. savo darbe vadovautis saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

33. Registro administratorius turi:

33.1. išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugą;

33.2. mokėti administruoti ir prižiūrėti duomenų bazes;

33.3. būti susipažinęs su Registro nuostatais, saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

34. Registro naudotojai turi:

34.1. turėti pagrindinius darbo kompiuteriu įgūdžius;

34.2. mokėti tvarkyti Registro elektroninę informaciją Registro nuostatų nustatyta tvarka;

34.3. būti susipažinę su Saugos nuostatais bei teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

35. Registro naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti Registro saugos įgaliotiniui.

36. Registro elektroninę informaciją tvarkyti ir teikti Registro nuostatuose nurodytiems Registro duomenų gavėjams gali asmenys, turintys pagrindinius darbo kompiuteriu įgūdžius, mokantys tvarkyti Registro elektroninę informaciją Registro nuostatuose, Registro funkcinėje sistemos specifikacijoje, patvirtintoje Registro valdytojo, Studijų, mokymo programų ir kvalifikacijų registro naudotojų administravimo taisyklėse nustatyta tvarka ir susipažinę su Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų reikalavimais.

37. Registro saugos įgaliotinis ne rečiau kaip kartą per dvejus metus inicijuoja Registro naudotojų mokymą elektroninės informacijos saugos klausimais, periodiškai įvairiais būdais primena apie saugumo problemas (pvz., pranešimai elektroniniu paštu, naujų darbuotojų instruktavimas ir pan.).

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

38. Registro naudotojus su saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai supažindina Registro saugos įgaliotinis. Registro saugos įgaliotinis, Registro naudotojai, Registro administratorius raštu įsipareigoja nepažeisti Saugos nuostatų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą.

39. Pakartotinai su saugos dokumentais Registro naudotojai supažindinami tada, kai šie pakeičiami.

40. Saugos nuostatai bei kiti dokumentai, reglamentuojantys saugų elektroninės informacijos tvarkymą, skelbiami Registro tvarkytojo interneto svetainėje.

41. Už Registro naudotojų mokymo organizavimą atsakingas Registro saugos įgaliotinis.

42. Registro naudotojų supažindinimo su saugos dokumentais tvarka aprašyta Studijų, mokymo programų ir kvalifikacijų registro naudotojų administravimo taisyklėse.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

43. Saugos nuostatai ir kiti saugos dokumentai iš esmės peržiūrimi ir prireikus keičiami ne rečiau kaip kartą per metus.

44. Registro tvarkytojas privalo įgyvendinti Saugos nuostatuose ir kituose teisės aktuose, reglamentuojančiuose Registro elektroninės informacijos saugų tvarkymą, nustatytas organizacines, technines ir kitas priemones.

45. Duomenys apie Registro naudotojų, Registro administratoriaus atliktus veiksmus su Registro elektronine informacija saugomi ne trumpiau negu vienerius metus.

46. Asmenys, pažeidę Saugos nuostatų, kitų teisės aktų, reglamentuojančių Registro elektroninės informacijos saugų tvarkymą, reikalavimus, atsako registrų saugą reglamentuojančių teisės aktų nustatyta tvarka.

_____