LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS
DĖL VALSTYBĖS JONIZUOJANČIOSIOS SPINDULIUOTĖS ŠALTINIŲ IR DARBUOTOJŲ APŠVITOS REGISTRO IR RADIACINĖS SAUGOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2018 m. gruodžio 3 d. Nr. V-1387
Vilnius

Vadovaudamasis Lietuvos Respublikos kibernetinio saugumo įstatymu, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu, 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 12 ir 19 punktais ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, 5 ir 7 punktais:

1. T v i r t i n u Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro ir Radiacinės saugos informacinės sistemos duomenų saugos nuostatus (pridedama).

2. P a v e d u Radiacinės saugos centro direktoriui:

2.1. paskirti kibernetinio saugumo vadovą;

2.2. paskirti Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro ir Radiacinės saugos informacinės sistemos duomenų valdymo įgaliotinį, saugos įgaliotinį ir administratorių (-ius);

2.3. per 6 mėnesius nuo Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro ir Radiacinės saugos informacinės sistemos duomenų saugos nuostatų patvirtinimo dienos parengti Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro ir Radiacinės saugos informacinės sistemos elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančių dokumentų projektus.

3. P r i p a ž į s t u netekusiais galios:

3.1. Lietuvos Respublikos sveikatos apsaugos ministro 2009 m. birželio 23 d. įsakymą Nr. V-509 „Dėl Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro duomenų saugos nuostatų patvirtinimo“;

3.2. Lietuvos Respublikos sveikatos apsaugos ministro 2010 m. liepos 1 d. įsakymo Nr. V-600 „Dėl Radiacinės saugos informacinės sistemos nuostatų ir Radiacinės saugos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ 1.2 papunktį.

Sveikatos apsaugos ministras Aurelijus Veryga

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2018 m. gruodžio 3 d. įsakymu Nr. V-1387

VALSTYBĖS JONIZUOJANČIOSIOS SPINDULIUOTĖS ŠALTINIŲ IR DARBUOTOJŲ APŠVITOS REGISTRO IR RADIACINĖS SAUGOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro ir Radiacinės saugos informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro (toliau – Registras) ir Radiacinės saugos informacinės sistemos (toliau – RSIS) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Registro ir RSIS elektroninės informacijos saugos ir kibernetinio saugumo tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti Registro ir RSIS elektroninę informaciją, užtikrinti elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir kibernetinį saugumą.

3. Registro ir RSIS elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo prioritetinės kryptys:

3.1. organizacinių ir techninių reikalavimų, skirtų Registro ir RSIS elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas;

3.2. Registro ir RSIS duomenų tvarkymo ir naudojimo kontrolė;

3.3. elektroninių ryšių tinklų, techninės ir programinės įrangos veikimo kontrolė;

3.4. Registre tvarkomų asmens duomenų apsauga;

3.5. Registro ir RSIS veiklos tęstinumo užtikrinimas.

4. Saugos nuostatuose vartojamos sąvokos apibrėžtos 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1) (toliau – Reglamentas (ES) 2016/679), Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo 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, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Saugos reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas).

5. Elektroninės informacijos saugos ir kibernetinio saugumo politika įgyvendinama pagal Registro ir RSIS valdytojo tvirtinamus Registro ir RSIS elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančius dokumentus:

5.1. Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro ir Radiacinės saugos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisykles;

5.2. Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro ir Radiacinės saugos informacinės sistemos naudotojų administravimo taisykles;

5.3. Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro ir Radiacinės saugos informacinės sistemos veiklos tęstinumo valdymo planą.

6. Registro ir RSIS elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti kompleksiškai naudojamos teisinės, organizacinės, techninės ir programinės priemonės.

7. Saugos nuostatai taikomi:

7.1. Registro ir RSIS valdytojai – Lietuvos Respublikos sveikatos apsaugos ministerijai (adresas: Vilniaus g. 33, LT-01506 Vilnius);

7.2. Registro ir RSIS tvarkytojui – Radiacinės saugos centrui (toliau – RSC) (adresas: Kalvarijų g. 153, LT-08352 Vilnius);

7.3. asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą RSC (toliau – kibernetinio saugumo vadovas);

7.4. Registro ir RSIS saugos įgaliotiniui (toliau – saugos įgaliotinis);

7.5. Registro ir RSIS administratoriui (-ams) (toliau – administratorius (-iai);

7.6. Registro ir RSIS duomenų valdymo įgaliotiniui (toliau – duomenų valdymo įgaliotinis);

7.7. Registro ir RSIS naudotojams (toliau – naudotojai);

7.8. paslaugų, susijusių su elektroninių ryšių tinklų, Registro ir RSIS veikimu, teikėjams (toliau – paslaugų teikėjai).

8. Už Registro ir RSIS elektroninės informacijos saugą pagal kompetenciją atsako Registro ir RSIS valdytoja ir Registro ir RSIS tvarkytojas.

9. Registro ir RSIS valdytoja atsako už Registro ir RSIS elektroninės informacijos saugos ir kibernetinio saugumo politikos formavimą, jos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą ir atlieka šias funkcijas:

9.1. tvirtina Registro ir RSIS elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančius dokumentus, kontroliuoja, kaip jų laikomasi;

9.2. nagrinėja Registro ir RSIS tvarkytojo pasiūlymus dėl Registro ir RSIS elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo ir priima dėl jų sprendimus;

9.3. priima sprendimus dėl Registro ir RSIS techninių ir programinių priemonių, būtinų Registro ir RSIS elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įsigijimo, įdiegimo ir atnaujinimo;

9.4. atlieka kitas Saugos nuostatuose, Saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše ir kituose teisės aktuose nustatytas funkcijas, susijusias su Registro ir RSIS elektroninės informacijos sauga ir kibernetiniu saugumu.

10. Registro ir RSIS tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių elektroninės informacijos saugos ir kibernetinio saugumo priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose, elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančiuose dokumentuose nustatyta tvarka ir atlieka šiais funkcijas:

10.1. skiria kibernetinio saugumo vadovą, saugos įgaliotinį, administratorių (-ius), duomenų valdymo įgaliotinį;

10.2. tvirtina Radiacinės saugos centro ryšių ir informacinių sistemų techninių kibernetinio saugumo reikalavimų įgyvendinimo priemonių planą;

10.3. atlieka kitas Saugos nuostatuose, Saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugos ir kibernetinio saugumo politiką, nustatytas funkcijas, susijusias su Registro ir RSIS elektroninės informacijos sauga ir kibernetiniu saugumu.

11. Kibernetinio saugumo vadovas atlieka šiais funkcijas:

11.1. pagal kompetenciją vykdo kibernetinio saugumo stebėseną RSC;

11.2. teikia RSC direktoriui pasiūlymus dėl techninių kibernetinio saugumo reikalavimų įgyvendinimo priemonių parinkimo;

11.3. teikia naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su kibernetinio saugumo reikalavimų įgyvendinimu;

11.4. įvertina kibernetinius ir saugos incidentus, teikia pasiūlymus dėl šių incidentų šalinimo;

11.5. organizuoja kibernetinių incidentų imitavimo pratybas;

11.6. atlieka kitas Saugos nuostatuose, Kibernetinio saugumo reikalavimų apraše ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugos ir kibernetinio saugumo politiką, nustatytas funkcijas, susijusias su kibernetinio saugumo organizavimu ir užtikrinimu.

12. Saugos įgaliotinis vykdo šias funkcijas:

12.1. teikia RSC direktoriui pasiūlymus dėl:

12.1.1. administratoriaus (-ių) skyrimo;

12.1.2. Saugos nuostatų, Registro ir RSIS saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

12.1.3. Registro ir RSIS informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

12.2. organizuoja Registro ir RSIS rizikos vertinimą;

12.3. koordinuoja elektroninės informacijos saugos incidentų Registre ir RSIS tyrimą;

12.4. teikia administratoriui (-iams) ir naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Registro ir RSIS elektroninės informacijos saugos politikos įgyvendinimu;

12.5. atlieka kitas Saugos nuostatuose, Saugos reikalavimų apraše ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugos ir kibernetinio saugumo politiką, nustatytas funkcijas, susijusias su Registro ir RSIS elektroninės informacijos sauga.

13. Administratorius, vykdantis Registro ir RSIS priežiūrą, atlieka šias funkcijas:

13.1. pagal kompetenciją užtikrina Registro ir RSIS veikimą;

13.2. atsako už saugų duomenų perdavimą elektroninių ryšių tinklais;

13.3. atlieka Registro ir RSIS komponentų (elektroninių ryšių tinklų įrangos, tarnybinių stočių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimo aptikimo sistemų) priežiūrą ir teikia duomenų valdymo įgaliotiniui pasiūlymus dėl jų atnaujinimo;

13.4. vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su Registro ir RSIS elektroninės informacijos saugos užtikrinimu;

13.5. registruoja Registro ir RSIS elektroninės informacijos saugos incidentus ir informuoja apie juos saugos įgaliotinį;

13.6. atlieka kitas Saugos nuostatuose, Saugos reikalavimų apraše ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugos ir kibernetinio saugumo politiką, nustatytas funkcijas, susijusias su elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimu.

14. Administratorius, tvarkantis Registro ir RSIS naudotojų prieigas, atlieka šias funkcijas:

14.1. pagal kompetenciją atsako už Registro asmens duomenų konfidencialumą, prieinamumą ir vientisumą, teikia saugos įgaliotiniui pasiūlymus dėl asmens duomenų saugos užtikrinimo;

14.2. suteikia, keičia ir panaikina naudotojams prieigos prie Registro ir RSIS duomenų teises;

14.3. teikia konsultacijas naudotojams Registro ir RSIS naudojimosi klausimais;

14.4. analizuoja naudotojų veiksmų registracijos žurnalo įrašus;

14.5. pagal kompetenciją atlieka Registro ir RSIS parametrų ir klasifikatorių tvarkymą;

14.6. vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su Registro ir RSIS saugos užtikrinimu;

14.7. atlieka kitas Saugos nuostatuose, Saugos reikalavimų apraše ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugos ir kibernetinio saugumo politiką, nustatytas funkcijas, susijusias su Registro ir RSIS elektroninės informacijos sauga.

15. Duomenų valdymo įgaliotinis atlieka Valstybės informacinių išteklių valdymo įstatyme ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugos ir kibernetinio saugumo politiką, nustatytas funkcijas, susijusias su Registro ir RSIS plėtra.

16. Naudotojai, tvarkantys Registro ir RSIS duomenis, privalo įsipareigoti saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir nutraukus su duomenų tvarkymu susijusią veiklą.

17. Paslaugų teikėjai privalo įsipareigoti saugoti duomenų ir informacijos paslaptį bei pasirašyti konfidencialumo pasižadėjimą. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir pasibaigus paslaugų teikimo laikui ar nutraukus šią veiklą.

18. Teisės aktai, kuriais vadovaujantis tvarkomi Registro ir RSIS duomenys ir užtikrinama jų sauga:

18.1. Reglamentas (ES) 2016/679;

18.2. Kibernetinio saugumo įstatymas;

18.3. Valstybės informacinių išteklių valdymo įstatymas;

18.4. Kibernetinio saugumo reikalavimų aprašas;

18.5. Saugos reikalavimų aprašas;

18.6. 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

18.7. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas);

18.8. Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 1999 m. gegužės 25 d. nutarimu Nr. 651 „Dėl Valstybės jonizuojančiosios spinduliuotės šaltinių ir darbuotojų apšvitos registro nuostatų patvirtinimo“;

18.9. Radiacinės saugos informacinės sistemos nuostatai, patvirtinti Lietuvos Respublikos sveikatos apsaugos ministro 2010 m. liepos 1 d. įsakymu Nr. V-600 „Dėl Radiacinės saugos informacinės sistemos nuostatų ir Radiacinės saugos informacinės sistemos duomenų saugos nuostatų patvirtinimo“;

18.10. 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“;

18.11. Lietuvos standartai LST ISO/IEC 27001, LST ISO/IEC 27002 ir kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys informacijos saugumą;

18.12. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugos ir kibernetinio saugumo politiką.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

19. Registro ir RSIS tvarkoma elektroninė informacija priskirtina svarbios elektroninės informacijos kategorijai, vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo 8.1, 8.4 ir 8.5 papunkčiais.

20. Registras ir RSIS pagal juose tvarkomos elektroninės informacijos svarbą priskiriami antrajai informacinių sistemų kategorijai, vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo 12.2 papunkčiu.

21. Saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja Registro ir RSIS rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį Registro ir RSIS rizikos įvertinimą.

22. Įvertinus Registro ir RSIS riziką, parengiama Registro ir RSIS rizikos vertinimo ataskaita. Registro ir RSIS rizikos vertinimo ataskaita rengiama atsižvelgiant į Registro ir RSIS rizikos veiksnius, galinčius turėti įtakos informacijos saugai.

23. Svarbiausi rizikos veiksniai, kurie gali pažeisti Registro ir RSIS duomenų ir parengtos pagal juos informacijos saugą, yra:

23.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, fiziniai informacijos technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

23.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Registru ir RSIS duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

23.3. 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.

24. Atsižvelgdamas į rizikos vertinimo ataskaitą, Registro ir RSIS tvarkytojas prireikus tvirtina rizikos vertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

25. Siekiant užtikrinti saugos dokumentų nuostatų laikymosi kontrolę, Lietuvos Respublikos krašto apsaugos ministro patvirtintos Informacinių technologijų saugos atitikties vertinimo metodikos nustatyta tvarka kasmet atliekamas Registro ir RSIS informacinių technologijų saugos reikalavimų atitikties vertinimas, kurio metu:

25.1. inventorizuojama Registro ir RSIS techninė ir programinė įranga;

25.2. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų naudotojų kompiuterizuotų darbo vietų, tarnybinėse stotyse įdiegtos programos ir jų sąranka;

25.3. įvertinama naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;

25.4. įvertinamas pasirengimas užtikrinti Registro ir RSIS veiklos tęstinumą įvykus elektroninės informacijos saugos ar kibernetinio saugumo incidentui;

25.5. atliekamas kibernetinių atakų imitavimas ir įvertinamos grėsmės ir pažeidžiamumai, galintys turėti įtakos kibernetiniam saugumui;

25.6. įvertinama Registro ir RSIS rizikos įvertinimo ir valdymo būklė;

25.7. patikrinama realios informacijos saugos situacijos atitiktis saugos ir kibernetinio saugumo dokumentams.

26. Atlikus Registro ir RSIS informacinių technologijų saugos reikalavimų atitikties vertinimą, prireikus rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus Registro ir RSIS tvarkytojas.

27. Kibernetinio saugumo vadovas, vykdydamas kibernetinio saugumo stebėseną, ne rečiau kaip kartą per mėnesį atlieka elektroninių ryšių tinklų, Registro ir RSIS tarnybinių stočių, užkardų (saugasienių) užfiksuotų įvykių, naudotojų veiksmų žurnalo analizę, šalina saugumo reikalavimų neatitikimus, įvertina kibernetiniam saugumui užtikrinti naudojamų priemonių programinius atnaujinimus, klaidų taisymus.

28. Prireikus rengiamas Radiacinės saugos centro ryšių ir informacinių sistemų kibernetinio saugumo užtikrinimo planas, kurį tvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus RSC direktorius.

29. Registro ir RSIS rizikos vertinimas, Registro ir RSIS informacinių technologijų saugos atitikties vertinimas ir Radiacinės saugos centro ryšių ir informacinių sistemų atitikties Kibernetinio saugumo reikalavimų apraše nustatytiems techniniams kibernetinio saugumo reikalavimams vertinimas gali būti atliekamas nepriklausomų ekspertų.

30. Patvirtintų Registro ir RSIS elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas Registro ir RSIS valdytoja ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo dienos pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Lietuvos Respublikos krašto apsaugos ministro patvirtintų Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

31. Registro ir RSIS rizikos vertinimo ataskaitos, rizikos vertinimo ir rizikos valdymo priemonių plano, Registro ir RSIS informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas Registro ir RSIS valdytoja ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo dienos pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Lietuvos Respublikos krašto apsaugos ministro patvirtintų Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

32. Registro ir RSIS elektroninės informacijos saugos priemonės parenkamos vadovaujantis konfidencialumo, vientisumo ir prieinamumo principais.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

33. Tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai) aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą, kurios turi būti nuolat atnaujinamos automatiniu būdu ne rečiau kaip kartą per 48 valandas.

34. Programinės įrangos, įdiegtos tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

34.1. Registro ir RSIS darbui turi būti naudojama tik legali programinė įranga;

34.2. programinė įranga ir priemonės kibernetiniam saugumui užtikrinti atnaujinamos laikantis gamintojo reikalavimų;

34.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka tik administratorius (-iai) arba paslaugų teikėjai;

34.4. Registro ir RSIS programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims;

34.5. Registro ir RSIS tarnybinėse stotyse neturi veikti programinė įranga, nesusijusi su Registro ir RSIS duomenų tvarkymu, naudotojų ir pačios įrangos administravimu;

34.6. Registro ir RSIS programinė įranga testuojama naudojant atskirą testavimui skirtą aplinką;

34.7. ne rečiau kaip kartą per 3 mėnesius, administratorius (-iai) patikrina kompiuterizuotose darbo vietose naudojamą programinę įrangą; rasta nelegali programinė įranga turi būti nedelsiant pašalinta.

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

35.1. kompiuterių tinklas nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirtas užkardų (saugasienių);

35.2. visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

35.3. naudojamos turinio filtravimo sistemos.

36. Leistinos kompiuterių ir kitų mobiliųjų įrenginių naudojimo ribos:

36.1. Registro ir RSIS duomenų tvarkymui leidžiama naudoti tik leistinus nešiojamuosius kompiuterius, atitinkančius Registro ir RSIS valdytojos nustatytus elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus;

36.2. jeigu nešiojamasis kompiuteris naudojamas ne tik RSC patalpose, turi būti įdiegtos papildomos saugos priemonės, taikytinos tokiems kompiuteriams (šifravimas, papildomas tapatybės patvirtinimas, prisijungimo ribojimai, rakinimo įrenginių naudojimas ir panašiai);

36.3. nešiojamuosiuose kompiuteriuose neturi būti jokios svarbios informacijos, išskyrus naudotojo darbo dokumentus;

36.4. naudotojams, savo tarnybinėms funkcijoms vykdyti, leidžiama naudoti tik su kibernetinio saugumo vadovu suderintus belaidžio tinklo įrenginius, atitinkančius techninius kibernetinio saugumo reikalavimus.

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

37.1. viešaisiais tinklais perduodamos elektroninės informacijos konfidencialumas užtikrinamas naudojant virtualų privatų tinklą (angl. *virtual private network*) arba šifravimą;

37.2. elektroninė informacija, perduodama ne per Saugų valstybinį duomenų perdavimo tinklą, turi būti šifruojama;

37.3. elektroninė informacija perduodama automatiniu būdu naudojant TCP/IP, HTTPS, IMAPS, SMTPS protokolus realiame laike arba asinchroniniu režimu pagal duomenų teikimo sutartis, kuriose turi būti nustatytos elektroninės informacijos perdavimo sąlygos ir tvarka, kitos elektroninės informacijos perdavimo specifikacijos;

37.4. belaidės prieigos taškai diegiami tik atskirame potinklyje, kontroliuojamoje zonoje;

37.5. visos naudotojų kompiuterizuotos darbo vietos valdomos naudojant centralizuoto valdymo priemonę „Active directory“;

37.6. prieiga prie Registro ir RSIS duomenų suteikiama įgyvendinus naudotojų autentifikavimo priemones; teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam naudotojui arba naudotojų grupei;

37.7. tiesioginė prieiga prie Registro ir RSIS duomenų leistina tik per Registro vidinį portalą iš RSC tinklo (RSC patalpose);

37.8. Registro išorinis portalas pasiekiamas nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą).

38. Pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

38.1. elektroninės informacijos kopijos turi būti daromos automatiškai kiekvieną dieną; prireikus jas atkurti turi teisę administratorius (-iai) arba paslaugų teikėjai;

38.2. elektroninės informacijos atkūrimas iš kopijų privalo būti išbandomas;

38.3. elektroninės informacijos kopijos saugomos kitoje patalpoje nei Registro ir RSIS tarnybinės stotys.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

39. Kibernetinio saugumo vadovas turi išmanyti kibernetinio saugumo organizavimo ir užtikrinimo principus, savo darbe vadovautis elektroninės informacijos saugos ir kibernetinio saugumo dokumentais bei kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, standartais ir kitais dokumentais, reglamentuojančiais elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimą.

40. Saugos įgaliotinis turi išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis saugos dokumentais bei kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, standartais ir kitais dokumentais, reglamentuojančiais saugos ir kibernetinio saugumo politikos įgyvendinimą.

41. Administratorius (-iai) privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo politikos principus, elektroninių ryšių tinklų, techninės ir programinės įrangos veikimą, mokėti užtikrinti jų saugą, taip pat administruoti ir prižiūrėti registrus ir informacines sistemas.

42. Administratorius (-iai) ir naudotojai turi būti susipažinę su Saugos nuostatais, elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančiais dokumentais, pagal kompetenciją ir kitais teisės aktais bei standartais, reglamentuojančiais elektroninės informacijos saugą ir kibernetinį saugumą.

43. Naudotojai, tvarkantys elektroninę informaciją, privalo įsipareigoti saugoti informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą bei valstybės tarnybos ar darbo santykius.

44. Naudotojai, atliekantys tarnybines funkcijas, susijusias su asmens duomenų tvarkymu bei teikimu, raštu pasirašytinai įpareigojami saugoti asmens duomenų paslaptį. Asmens duomenų paslaptį jie privalo saugoti ir pasibaigus valstybės tarnybos ar darbo santykiams, per visą asmens duomenų teisinės apsaugos laiką.

45. Naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti saugiai tvarkyti elektroninę informaciją.

46. Naudotojai, pastebėję elektroninės informacijos saugos ir kibernetinio saugumo dokumentų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai kibernetinio saugumo vadovui, saugos įgaliotiniui arba administratoriui (-iams).

47. Naudotojams draudžiama:

47.1. atskleisti Registro ir RSIS duomenis ar suteikti kitokią galimybę bet kokia forma su jais susipažinti tokios teisės neturintiems asmenims;

47.2. savavališkai diegti taikomąją programinę įrangą, jos pakeitimus ir naujas versijas neturint tam suteiktos teisės;

47.3. atskleisti kitiems asmenims prisijungimo prie centralizuoto valdymo priemonės „Active directory“ vardą, slaptažodį ar kitaip sudaryti sąlygas jais pasinaudoti;

47.4. naudoti Registro ir RSIS duomenis kitokiais nei jų nuostatuose nurodytais tikslais bei savo pareigybės aprašyme nustatytų funkcijų vykdymo tikslais;

47.5. sudaryti sąlygas pasinaudoti Registro ir RSIS tvarkymui naudojamą techninę ir programinę įrangą tokios teisės neturintiems asmenims (paliekant darbo vietą būtina užrakinti darbalaukį arba išjungti darbo stotį);

47.6. atlikti veiksmus, dėl kurių gali būti neteisėtai pakeisti, sunaikinti ar atskleisti Registro ir RSIS duomenys, taip pat neatlikti būtinų veiksmų, kurie apsaugo Registro ir RSIS duomenis;

47.7. atlikti bet kokius kitus neteisėtus Registro ir RSIS tvarkymo veiksmus.

48. Saugos įgaliotinis kartu su kibernetinio saugumo vadovu periodiškai organizuoja naudotojų elektroninės informacijos saugos ir kibernetinio saugumo mokymus, įvairiais būdais informuoja naudotojus apie elektroninės informacijos saugą ir kibernetinį saugumą.

V SKYRIUS
NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

49. Tvarkyti Registro ir RSIS elektroninę informaciją gali tik naudotojai, susipažinę su Saugos nuostatais, elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugą, taip pat atsakomybe už saugos dokumentų nuostatų pažeidimus, ir sutikę laikytis saugos dokumentuose nustatytų reikalavimų. Pakartotinis supažindinimas yra vykdomas pasikeitus minėtiems dokumentams ir teisės aktams.

50. Naudotojų supažindinimą ir prireikus pakartotinį supažindinimą su Saugos nuostatais, elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančiais dokumentais ir atsakomybe už jų nustatytų reikalavimų nesilaikymą organizuoja saugos įgaliotinis.

51. Naudotojai su Saugos nuostatais ir elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančiais dokumentais bei atsakomybe už jų reikalavimų nesilaikymą supažindinami pasirašytinai.

52. Saugos įgaliotinis ir kibernetinio saugumo vadovas pagal kompetenciją organizuoja elektroninės informacijos saugos ir kibernetinio saugumo dokumentų peržiūrą ne rečiau kaip kartą per metus. Elektroninės informacijos saugos ir kibernetinio saugumo dokumentai turi būti peržiūrimi atlikus rizikos analizę ar informacinių technologijų saugos atitikties vertinimą arba RSC įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

53. Kibernetinio saugumo vadovas, saugos įgaliotinis, administratorius (-iai), naudotojai, pažeidę Saugos nuostatų ar kitų elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.

_____