Suvestinė redakcija nuo 2020-06-27 iki 2023-01-11

Įsakymas paskelbtas: TAR 2018-10-16, i. k. 2018-16241

LIETUVOS RESPUBLIKOS KULTŪROS MINISTRAS

ĮSAKYMAS DĖL VIEŠOSIOS INFORMACIJOS RENGĖJŲ IR SKLEIDĖJŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ TVIRTINIMO, SAUGOS ĮGALIOTINIO IR ADMINISTRATORIŲ SKYRIMO BEI SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ RENGIMO

2018 m. spalio 10 d. Nr. ĮV-728
Vilnius

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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinės sistemos, registrų ir kitų informacinės sistemos klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 12, 19, 26 punktais, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 6 punktu:

Preambulės pakeitimai:
Nr. IV-842, 2020-06-25, paskelbta TAR 2020-06-26, i. k. 2020-14035

1. T v i r t i n u Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos duomenų saugos nuostatus (pridedama).

2. P a v e d u valstybės įmonei Registrų centrui per 3 mėnesius nuo šio įsakymo įsigaliojimo:

2.1. paskirti Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos saugos įgaliotinį ir administratorius;

2.2. parengti ir pateikti Lietuvos Respublikos kultūros ministerijai informacinės Viešosios informacijos rengėjų ir skleidėjų sistemos elektroninės informacijos saugos politiką įgyvendinančių dokumentų projektus.

Kultūros ministrė Liana Ruokytė-Jonsson

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2018 m. birželio 5 d. raštu Nr. 1D-2887

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos

2018 m. birželio 12 d. raštu Nr. (4.2) 6K-348

PATVIRTINTA
Lietuvos Respublikos kultūros ministro
2018 m. spalio 10 d. įsakymu Nr. ĮV-728
(Lietuvos Respublikos kultūros ministro
2020 m. birželio 25 d. įsakymo Nr. ĮV-842
redakcija)

VIEŠOSIOS INFORMACIJOS RENGĖJŲ IR SKLEIDĖJŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos (toliau – VIRSIS) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Saugos nuostatuose vartojamos sąvokos apibrėžtos 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 – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas) ir Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose 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“ (toliau – Techniniai elektroninės informacijos saugos reikalavimai).

3. Saugos nuostatų, Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos veiklos tęstinumo valdymo plano, Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos naudotojų administravimo taisyklių (toliau visi kartu – saugos dokumentai) taikymas ir naudojimas:

3.1. Saugos dokumentai taikomi:

3.1.1. Lietuvos Respublikos kultūros ministerijai (J. Basanavičiaus g. 5, 01118 Vilnius) – VIRSIS valdytojui;

3.1.2. valstybės įmonei Registrų centrui (Lvovo g. 25-101, 09320 Vilnius) – VIRSIS tvarkytojui;

3.1.3. VIRSIS saugos įgaliotiniui, VIRSIS administratoriams, VIRSIS naudotojams, VIRSIS funkcionuoti reikalingų paslaugų teikėjams;

3.1.4. Saugos nuostatai yra vieši ir skelbiami Teisės aktų registre. Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos veiklos tęstinumo valdymo plano (toliau – Planas), Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos naudotojų administravimo taisyklių (toliau visi kartu – saugos politiką įgyvendinantys dokumentai) naudojimas yra ribojamas – VIRSIS naudotojams, VIRSIS funkcionuoti reikalingų paslaugų teikėjams ir kitiems tretiesiems asmenims suteikiama teisė susipažinti tik su jų santrauka, Saugos nuostatų V skyriuje nustatyta tvarka;

4. Saugos politiką įgyvendinančių dokumentų santrauka rengiama vadovaujantis būtinumo žinoti principu. Saugos politiką įgyvendinančių dokumentų santrauką tvirtina VIRSIS tvarkytojas;

5. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo prioritetinės kryptys:

5.1. VIRSIS elektroninės informacijos saugos – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo – užtikrinimas;

5.2. VIRSIS kibernetinio saugumo užtikrinimas;

5.3. asmens duomenų apsauga;

5.4. VIRSIS naudotojų mokymas.

6. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

6.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti VIRSIS elektroninę informaciją;

6.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

6.3. vykdyti elektroninės informacijos saugos ir kibernetinių incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos ir kibernetinius incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

7. VIRSIS valdytojo funkcijos:

7.1. atlikti Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos nuostatuose (toliau – VIRSIS nuostatai) nustatytas funkcijas;

7.2. tvirtinti saugos dokumentus ir kitus teisės aktus, susijusius su VIRSIS elektroninės informacijos sauga ir kibernetiniu saugumu;

7.3. koordinuoti VIRSIS tvarkytojo darbą įgyvendinant elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus;

7.4. atlikti elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų laikymosi priežiūrą ir kontrolę;

7.5. nagrinėti VIRSIS tvarkytojo pasiūlymus dėl VIRSIS elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo ir priimti dėl jų sprendimus;

7.6. skirti VIRSIS saugos įgaliotinį ir VIRSIS administratorius arba pavesti juos paskirti VIRSIS tvarkytojui;

7.7. teikti Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – Nacionalinis kibernetinio saugumo centras) techninę informaciją, reikalingą VIRSIS kibernetiniam saugumui įvertinti, Nacionalinio kibernetinio saugumo centro reikalavimu nurodytais formatais ir terminais arba savo iniciatyva;

7.8. atlikti kitas Saugos nuostatuose ir Saugos nuostatų 20 punkte nurodytuose teisės aktuose nustatytas VIRSIS valdytojo funkcijas.

8. VIRSIS tvarkytojo funkcijos:

8.1. atlikti VIRSIS nuostatuose nustatytas funkcijas;

8.2. užtikrinti saugos dokumentų ir kitų VIRSIS valdytojo priimtų teisės aktų, susijusių su VIRSIS elektroninės informacijos sauga ir kibernetiniu saugumu, tinkamą įgyvendinimą;

8.3. prižiūrėti VIRSIS komponentus (ugniasienes, įsilaužimų aptikimo sistemas ir kitus VIRSIS komponentus, nurodytus Saugos nuostatų 15.3 papunktyje), užtikrinti jų veikimą;

8.4. įgyvendinti VIRSIS elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus;

8.5. užtikrinti VIRSIS elektroninės informacijos saugą ir kibernetinį saugumą;

8.6. teikti VIRSIS valdytojui pasiūlymus dėl VIRSIS elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo;

8.7. VIRSIS valdytojui pavedus, skirti VIRSIS saugos įgaliotinį ir VIRSIS administratorius;

8.8. atlikti kitas Saugos nuostatuose ir Saugos nuostatų 20 punkte nurodytuose teisės aktuose nustatytas VIRSIS tvarkytojo funkcijas.

9. Už elektroninės informacijos saugą ir kibernetinį saugumą pagal kompetenciją atsako VIRSIS valdytojas ir VIRSIS tvarkytojas.

10. VIRSIS valdytojas atsako už elektroninės informacijos saugos ir kibernetinio saugumo politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

11. VIRSIS tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi saugos dokumentuose nustatyta tvarka.

12. VIRSIS saugos įgaliotinis ir VIRSIS administratorius gali būti paskiriami keliems VIRSIS posistemiams, funkciškai savarankiškoms sudedamosioms dalims ar tam tikroms VIRSIS saugos įgaliotinio ir VIRSIS administratoriaus funkcijoms atlikti, tačiau turi būti užtikrintas tinkamas VIRSIS saugos įgaliotinio ir VIRSIS administratoriaus funkcijų atlikimas. Jeigu skiriami VIRSIS saugos įgaliotiniai ir VIRSIS administratoriai atskiram VIRSIS posistemiui, funkciškai savarankiškoms sudedamosioms dalims ar tam tikroms VIRSIS saugos įgaliotinio ir VIRSIS administratoriaus funkcijoms atlikti, turi būti aiškiai nurodyta, kokiam VIRSIS posistemiui, funkciškai savarankiškoms sudedamosioms dalims ar kurioms VIRSIS saugos įgaliotinio ir VIRSIS administratoriaus funkcijoms atlikti paskiriamas konkretus saugos įgaliotinis ir administratorius, taip pat vienam iš VIRSIS saugos įgaliotinių ir VIRSIS administratorių pavedama koordinuoti šių saugos įgaliotinių ir administratorių veiklą.

13. VIRSIS saugos įgaliotinio funkcijos:

13.1. koordinuoti ir prižiūrėti elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimą saugos dokumentuose nustatyta tvarka;

13.2. teikti VIRSIS tvarkytojo vadovui pasiūlymus dėl:

13.2.1. VIRSIS administratorių paskyrimo ir reikalavimų jiems nustatymo;

13.2.2. informacinių technologijų saugos atitikties vertinimo atlikimo pagal Informacinių technologijų saugos atitikties vertinimo metodiką, nustatytą Lietuvos Respublikos krašto apsaugos ministro;

13.3. teikti VIRSIS valdytojo vadovui pasiūlymus dėl saugos dokumentų priėmimo, keitimo;

13.4. koordinuoti elektroninės informacijos saugos ir kibernetinių incidentų tyrimą ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos ir kibernetinius incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos ir kibernetiniais incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos ir kibernetinio saugumo darbo grupės;

13.5. teikti VIRSIS administratoriams ir VIRSIS naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimo. VIRSIS saugos įgaliotinis, atlikdamas funkcijas, turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems VIRSIS valdytojo ir VIRSIS tvarkytojo darbuotojams, jeigu tai būtina elektroninės informacijos saugos ir kibernetinio saugumo politikai įgyvendinti;

13.6. organizuoti rizikos ir informacinių technologijų saugos atitikties įvertinimą;

13.7. atlikti 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 – Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas) nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

13.8. atlikti kitas saugos dokumentuose ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše VIRSIS saugos įgaliotiniui priskirtas funkcijas.

14. VIRSIS saugos įgaliotinis negali atlikti VIRSIS administratoriaus funkcijų.

15. VIRSIS administratoriai pagal atliekamas funkcijas skirstomi į grupes:

15.1. koordinuojantysis administratorius, kuris prižiūri VIRSIS administratorių veiklą, siekdamas užtikrinti tinkamą VIRSIS administratorių funkcijų vykdymą;

15.2. VIRSIS naudotojų administratoriai, kurie atlieka funkcijas, susijusias su VIRSIS naudotojų teisių valdymu;

15.3. VIRSIS komponentų administratoriai, kurie atlieka funkcijas, susijusias su VIRSIS komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazėmis ir jų valdymo sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo ir prevencijos sistemomis, elektroninės informacijos perdavimo tinklais, duomenų saugyklomis, bylų serveriais ir kita technine ir programine įranga, kurios pagrindu funkcionuoja VIRSIS ir užtikrinama joje tvarkomos elektroninės informacijos sauga ir kibernetinis saugumas bei VIRSIS komponentų sąranka);

15.4. VIRSIS saugos administratoriai, kurie atlieka funkcijas, susijusias su VIRSIS pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena;

16. VIRSIS administratoriai yra atsakingi už tinkamą saugos dokumentuose jiems nustatytų funkcijų vykdymą.

17. VIRSIS administratoriai privalo vykdyti visus VIRSIS saugos įgaliotinio nurodymus ir pavedimus dėl VIRSIS saugos ir kibernetinio saugumo užtikrinimo, pagal kompetenciją reaguoti į elektroninės informacijos saugos ir kibernetinius incidentus ir nuolat teikti VIRSIS saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

18. Atlikdami VIRSIS sąrankos pakeitimus, VIRSIS komponentų administratoriai turi laikytis VIRSIS valdytojo patvirtinto Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos pokyčių valdymo tvarkos aprašo.

19. VIRSIS komponentų administratoriai privalo patikrinti (peržiūrėti) VIRSIS sąranką ir VIRSIS būsenos rodiklius reguliariai – ne rečiau kaip kartą per metus ir (arba) po VIRSIS pokyčio.

20. Teisės aktai, kuriais vadovaujamasi tvarkant VIRSIS elektroninę informaciją ir užtikrinant jos saugą:

20.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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);

20.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

20.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

20.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

20.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

20.6. 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 – Klasifikavimo gairių aprašas);

20.7. Techniniai elektroninės informacijos saugos reikalavimai;

20.8. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas;

20.9. Lietuvos standartai LST EN ISO/IEC 27002 ir LST EN ISO/IEC 27001.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

21. VIRSIS tvarkoma elektroninė informacija priskiriama vidutinės svarbos elektroninės informacijos kategorijai. Elektroninė informacija šiai kategorijai priskiriama vadovaujantis Klasifikavimo gairių aprašo 9.1 ir 9.3 papunkčiais.

22. VIRSIS pagal joje tvarkomos elektroninės informacijos svarbą, vadovaujantis Klasifikavimo gairių aprašo 12.3 papunkčiu, priskiriama trečiajai kategorijai.

23. Rizikos vertinimo organizavimas:

23.1. VIRSIS saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir

tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus, kasmet arba po esminių organizacinių ar sisteminių pokyčių, organizuoja VIRSIS rizikos įvertinimą. VIRSIS rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu. Prireikus, VIRSIS saugos įgaliotinis gali organizuoti neeilinį VIRSIS rizikos įvertinimą. VIRSIS tvarkytojo rašytiniu pavedimu VIRSIS rizikos įvertinimą gali atlikti pats VIRSIS saugos įgaliotinis. Organizuojant rizikos vertinimą, rekomenduojama VIRSIS rizikos vertinimą įtraukti į VIRSIS tvarkytojo veiklos rizikos vertinimo procesus.

23.2. Organizuojant rizikos vertinimą turi būti paskirtas (paskirti) už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą atsakingas asmuo (asmenys) ir nustatytas jam (jiems) taikomi kvalifikaciniai reikalavimai. Atsakingu asmeniu gali būti skiriamas VIRSIS valdytojo arba VIRSIS tvarkytojo darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugas teikiančiu subjektu.

23.3. Rizikos vertinimo metu turi būti:

23.3.1. nustatomos grėsmės ir pažeidžiamumai, galintys turėti įtakos VIRSIS elektroninės informacijos saugai ir kibernetiniam saugumui;

23.3.2. nustatomos galimos grėsmių ir pažeidžiamumų poveikio vykdomai veiklai sritys;

23.3.3. įvertinamos VIRSIS pažeidimo grėsmių tikimybė ir pasekmės;

23.3.4. nustatomas rizikos lygis ir įvertinamos identifikuotos grėsmių tikimybės, kurios išdėstomos prioriteto tvarka pagal svarbą, kuri nustatoma atsižvelgiant į atliktą rizikos vertinimą.

23.4. VIRSIS rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama VIRSIS valdytojo vadovui ir VIRSIS tvarkytojo vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos VIRSIS elektroninės informacijos saugai ir kibernetiniam saugumui, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Rizikos veiksniai rizikos įvertinimo ataskaitoje išdėstomi pagal prioritetus ir priimtiną rizikos lygį. Svarbiausi rizikos veiksniai yra šie:

23.4.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais triktys, programinės įrangos klaidos, netinkamas veikimas ir kita);

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

23.4.3. 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;

23.5. Atsižvelgdamas į rizikos įvertinimo ataskaitą, VIRSIS valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti;

23.6. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas VIRSIS valdytojas ne vėliau kaip per 5 (penkias) darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams sistemos nuostatų patvirtinimo“, nustatyta tvarka;

23.7. Atsižvelgiant į atlikto rizikos vertinimo rezultatus, taip pat jeigu Saugos nuostatų 24 punkte nustatyta tvarka atliekamo informacinių technologijų saugos atitikties vertinimo metu nustatoma kibernetinių incidentų valdymo ir šalinimo, organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, atitinkamai turi būti tobulinamas Planas ir (arba) Kibernetinių ir elektroninės informacijos saugos incidentų valdymo tvarkos aprašas. Plano veiksmingumo išbandymo rezultatai

išdėstomi Plano veiksmingumo išbandymo ir pastebėtų trūkumų ataskaitose, kurio kopija ne vėliau kaip per 5 (penkias) darbo dienas nuo šio dokumentų priėmimo pateikiama Nacionaliniam kibernetinio saugumo centrui.

24. Informacinių technologijų saugos atitikties vertinimo organizavimas:

24.1. Siekiant užtikrinti saugos dokumentuose nustatytų elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų įgyvendinimo organizavimą ir kontrolę, ne rečiau kaip kartą per 2 (dvejus) metus, jei teisės aktuose nenustatyta kitaip, turi būti organizuojamas VIRSIS informacinių technologijų saugos atitikties vertinimas;

24.2. Informacinių technologijų saugos atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka. Atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas atliekamas informacinių technologijų saugos atitikties vertinimo metu;

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

24.4. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas VIRSIS valdytojas ne vėliau kaip per 5 (penkias) darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams sistemos nuostatų nustatyta tvarka.

25. Elektroninės informacijos saugos ir kibernetinio saugumo būklės gerinimas:

25.1. Techninės, programinės, organizacinės ir kitos VIRSIS elektroninės informacijos saugos ir kibernetinio saugumo priemonės pasirenkamos atsižvelgiant į VIRSIS valdytojo turimus išteklius, vadovaujantis šiais principais:

25.1.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

25.1.2. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei.

25.2. Atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegtos prevencinės, detekcinės ir korekcinės elektroninės informacijos saugos ir kibernetinio saugumo priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

26. Organizaciniai ir techniniai elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai nustatomi pagal Saugos nuostatų 22 punkte nustatytą VIRSIS svarbos kategoriją vadovaujantis Saugos nuostatų 20 punkte nurodytais teisės aktais ir standartais.

27. Kibernetinio saugumo priemonės, nurodytos Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo priede, turi būti diegiamos atsižvelgiant į naujausius technikos laimėjimus, vadovaujantis gamintojo pateikiama bent viena gerąja saugumo praktikos rekomendacija.

28. Organizacinių ir techninių elektroninės informacijos saugos ir kibernetinio saugumo priemonių užtikrinimas turi būti grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos VIRSIS elektroninės informacijos saugai ir kibernetiniam saugumui, rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus.

29. Pagrindiniai organizaciniai ir techniniai elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai:

29.1. organizaciniai ir techniniai elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai detalizuojami saugos politiką įgyvendinančiuose dokumentuose;

29.2. turi būti naudojama ir operatyviai atnaujinama programinė įranga, skirta apsaugoti informacinę sistemą nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir pan.). Detalios šios programinės įrangos naudojimo nuostatos ir jos atnaujinimo reikalavimai (ilgiausias leistinas neatnaujinimo laikas ir kita) nustatomi Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse;

29.3. VIRSIS techninėje įrangoje ir vidinių VIRSIS naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga. Detalios programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos, jos atnaujinimo reikalavimai nustatomi Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse;

29.4. turi būti naudojama kompiuterių tinklo filtravimo įranga (užkardos, turinio kontrolės sistemos, įgaliotieji serveriai (angl. *proxy*) ir kita). Detalios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse;

29.5. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą, turi būti naudojamas šifravimas, virtualus privatus tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą (nuotolinio prisijungimo prie VIRSIS būdai, protokolai, elektroninės informacijos keitimosi formatai, šifravimo, elektroninės informacijos kopijų skaičiaus reikalavimai, reikalavimai teikti ir (ar) gauti elektroninę informaciją automatiniu būdu tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas ir panašiai), nustatyti Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse;

29.6. stacionarius kompiuterius leidžiama naudoti tik VIRSIS valdytojo ir VIRSIS tvarkytojų patalpose. Nešiojamiesiems kompiuteriams, išnešamiems iš VIRSIS valdytojo ar VIRSIS tvarkytojo patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas ir panašiai).

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

30.1. atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į priimtiną elektroninės informacijos praradimą (angl. *recovery point objective*) ir priimtiną VIRSIS neveikimo laikotarpį (angl. *recovery time objective*);

30.2. atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokia apimtimi, kad VIRSIS veiklos sutrikimo, elektroninės informacijos saugos incidento, kibernetinio incidento ar elektroninės informacijos vientisumo praradimo atvejais VIRSIS neveikimo laikotarpis nebūtų ilgesnis, nei teisės aktais nustatyta VIRSIS svarbos kategorijai, nurodytai Saugos nuostatų 22 punkte, o elektroninės informacijos praradimas atitiktų priimtinumo kriterijus;

30.3. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai periodiškai, bet ne rečiau nei nustatyta Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse;

30.4. elektroninė informacija atsarginėse elektroninės informacijos kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo atsarginių elektroninės informacijos kopijų) arba turi būti imtasi kitų priemonių, dėl kurių nebūtų galima neteisėtai atkurti elektroninės informacijos;

30.5. atsarginių elektroninės informacijos kopijų laikmenos turi būti žymimos taip, kad jas būtų galima identifikuoti, ir saugomos nedegioje spintoje kitose patalpose, nei yra VIRSIS tarnybinės stotys ar įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate;

30.6. periodiškai, bet ne rečiau kaip kartą per pusmetį, turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai;

30.7. patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

31. VIRSIS naudotojų, VIRSIS administratorių, VIRSIS saugos įgaliotinio kvalifikacijos ir patirties reikalavimai:

31.1. VIRSIS naudotojų, VIRSIS administratorių, VIRSIS saugos įgaliotinio kvalifikacija turi atitikti reikalavimus, nustatytus jų pareiginiuose nuostatuose;

31.2. visi VIRSIS naudotojai privalo turėti pagrindinių darbo kompiuteriu, taikomosiomis programomis įgūdžių, mokėti tvarkyti elektroninę informaciją, būti susipažinę su teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, VIRSIS elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo laikyti jų paslaptį ir būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą;

31.3. VIRSIS saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, tobulinti elektroninės informacijos saugos ir kibernetinio saugumo srities kvalifikaciją, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų, reglamentuojančių elektroninės informacijos saugą ir kibernetinį saugumą, nuostatomis. VIRSIS tvarkytojas turi sudaryti sąlygas VIRSIS saugos įgaliotiniui kelti kvalifikaciją;

31.4. VIRSIS saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikalstamas veikas ar paskirtą administracinę nuobaudą už administracinius nusižengimus, nurodytus Valstybės informacinių išteklių valdymo įstatymo 42 straipsnio 1 dalyje;

31.5. VIRSIS administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, mokėti užtikrinti VIRSIS ir joje tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą, administruoti ir prižiūrėti VIRSIS komponentus (stebėti VIRSIS komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti VIRSIS komponentų nepertraukiamą funkcionavimą ir pan.). VIRSIS administratoriai turi būti susipažinę su saugos dokumentais.

32. VIRSIS naudotojų ir VIRSIS administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

32.1. VIRSIS naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos ir kibernetinio saugumo problemas (pavyzdžiui, priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems VIRSIS naudotojams, VIRSIS administratoriams ir pan.);

32.2. mokymai elektroninės informacijos saugos ir kibernetinio saugumo klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), saugos įgaliotinio, VIRSIS naudotojų ar VIRSIS administratorių poreikius;

32.3. mokymai gali būti vykdomi tiesioginiu (pavyzdžiui, paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu būdu (pavyzdžiui, vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.);

32.4. mokymai VIRSIS naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už VIRSIS naudotojų mokymų organizavimą atsakingas saugos įgaliotinis;

32.5. mokymai VIRSIS saugos įgaliotiniui ir VIRSIS administratoriams turi būti organizuojami pagal poreikį.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

33. VIRSIS administratorių supažindinimą su saugos dokumentais, VIRSIS naudotojų supažindinimą su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka, atsakomybe už saugos dokumentų nuostatų pažeidimus organizuoja VIRSIS saugos įgaliotinis.

34. VIRSIS naudotojų supažindinimo su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka būdai turi būti pasirenkami atsižvelgiant į VIRSIS specifiką (pavyzdžiui, VIRSIS ir jos naudotojų lokaciją, organizacinių ir (ar) techninių priemonių, leidžiančių identifikuoti su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka susipažinusį asmenį ir užtikrinančių supažindinimo procedūros įrodomąją (teisinę) galią, panaudojimo galimybes ir pan.). VIRSIS naudotojai su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka turi būti supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą.

35. VIRSIS funkcionuoti reikalingų paslaugų teikėjų ir kitų trečiųjų asmenų supažindinimą su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka, atsakomybe už saugos dokumentų reikalavimų pažeidimus organizuoja VIRSIS saugos administratorius.

36. Pakartotinai su saugos dokumentais ar Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka Saugos nuostatų 33 ir 35 punktuose nurodyti asmenys supažindinami tik iš esmės pasikeitus VIRSIS arba elektroninės informacijos saugą ar kibernetinį saugumą reglamentuojantiems teisės aktams.

37. Tvarkyti VIRSIS elektroninę informaciją gali tik VIRSIS naudotojai, kurie yra susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančių dokumentų santrauka ir sutikę laikytis jų reikalavimų.

38. VIRSIS naudotojai atsako už VIRSIS ir joje tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą pagal kompetenciją. VIRSIS naudotojai, VIRSIS administratoriai, VIRSIS saugos įgaliotinis ir kiti asmenys, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

39. VIRSIS valdytojas saugos dokumentus gali keisti savo arba VIRSIS saugos įgaliotinio iniciatyva. Saugos dokumentai turi būti derinami su Nacionaliniu kibernetinio saugumo centru. Keičiami saugos dokumentai gali būti nederinami su Nacionaliniu kibernetinio saugumo centru tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos ir kibernetinio saugumo politikos nekeičiantys pakeitimai arba taisoma teisės technika. Tokiais atvejais Nacionaliniam kibernetinio saugumo centrui turi būti pateiktos šių dokumentų kopijos.

40. VIRSIS valdytojas ir VIRSIS tvarkytojas saugos dokumentus turi persvarstyti (peržiūrėti) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos įvertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems VIRSIS valdytojo ar tvarkytojo pokyčiams. Persvarsčius (peržiūrėjus) saugos dokumentus, turi būti nustatoma, kuriuos iš juose nustatytų elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų būtina atnaujinti ir (ar) įgyvendinti pirmiausia, siekiant užtikrinti VIRSIS saugą ir kibernetinį saugumą.

_____

Pakeitimai:

1.
Lietuvos Respublikos kultūros ministerija, Įsakymas
Nr. ĮV-842, 2020-06-25, paskelbta TAR 2020-06-26, i. k. 2020-14035
Dėl kultūros ministro 2018 m. spalio 10 d. įsakymo Nr. ĮV-728 „Dėl Viešosios informacijos rengėjų ir skleidėjų informacinės sistemos duomenų saugos nuostatų tvirtinimo, saugos įgaliotinio ir administratorių skyrimo bei saugos politiką įgyvendinančių dokumentų rengimo“ pakeitimo