PATVIRTINTA
Lietuvos Respublikos ekonomikos ir inovacijų ministro
2019 m. d. įsakymu Nr.

VALSTYBĖS INFORMACINIŲ TECHNOLOGIJŲ PASLAUGŲ VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybės informacinių technologijų paslaugų valdymo informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Valstybės informacinių technologijų paslaugų valdymo informacinės sistemos (toliau – VIPVIS) elektroninės informacijos saugos (kibernetinio saugumo) (toliau – elektroninės informacijos sauga) politiką.

2. Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas 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. Elektroninės informacijos saugos politika įgyvendinama pagal Lietuvos Respublikos ekonomikos ir inovacijų ministro tvirtinamus VIPVIS saugos politikos įgyvendinamuosius dokumentus, nurodytus Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 7.2–7.4 papunkčiuose (toliau – saugos politiką įgyvendinantys dokumentai). Saugos nuostatai kartu su saugos politiką įgyvendinančiais dokumentais sudaro VIPVIS saugos dokumentus (toliau – Saugos dokumentai).

4. Saugos dokumentų taikymas ir naudojimas:

4.1. Saugos dokumentai taikomi:

4.1.1. Lietuvos Respublikos ekonomikos ir inovacijų ministerijai (Gedimino pr. 38, 01104 Vilnius) – VIPVIS valdytojai (toliau – VIPVIS valdytojas);

4.1.2. Informacinės visuomenės plėtros komitetui (Gedimino pr. 7, 01103 Vilnius) – VIPVIS tvarkytojui (toliau – VIPVIS tvarkytojas);

4.1.3. IT paslaugų gavėjams, IT paslaugų teikėjams, VIPVIS saugos įgaliotiniui, VIPVIS administratoriams, VIPVIS naudotojams.

4.2. Saugos nuostatai yra skelbiami Lietuvos Respublikos teisės aktų registre. Saugos politikos įgyvendinimo dokumentų naudojimas yra ribojamas – VIPVIS naudotojams, IT paslaugų teikėjams, IT paslaugų gavėjams suteikiama teisė susipažinti su Saugos nuostatais ir Saugos politiką įgyvendinančiais dokumentais Saugos nuostatų V skyriuje nustatyta tvarka.

5. VIPVIS elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

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

5.2. VIPVIS kibernetinio saugumo užtikrinimas;

5.3. asmens duomenų apsauga;

5.4. VIPVIS veiklos tęstinumo užtikrinimas.

6. Elektroninės informacijos saugos užtikrinimo tikslai:

6.1. Sudaryti sąlygas saugiai automatiniu būdu tvarkyti VIPVIS elektroninę informaciją.

6.2. Užtikrinti, kad VIPVIS 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 (toliau – saugos incidentai), asmens duomenų saugumo pažeidimų prevenciją, reaguoti į saugos incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

7. VIPVIS valdytojo funkcijos:

7.1. Atlikti VIPVIS nuostatuose nustatytas funkcijas.

7.2. Tvirtinti Saugos nuostatus, saugos dokumentus ir kitus su VIPVIS elektroninės informacijos sauga susijusius teisės aktus.

7.3. Koordinuoti VIPVIS tvarkytojo darbą, siekiant įgyvendinti elektroninės informacijos saugos reikalavimus.

7.4. Atlikti elektroninės informacijos saugos reikalavimų laikymosi priežiūrą ir kontrolę.

7.5. Nagrinėti VIPVIS tvarkytojo pasiūlymus dėl VIPVIS elektroninės informacijos saugos tobulinimo ir priimti dėl jų sprendimus.

7.6. Pavesti VIPVIS tvarkytojui paskirti VIPVIS saugos įgaliotinį, VIPVIS administratorius.

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

7.8. Atlikti kitas Saugos nuostatuose ir Saugos nuostatų 19 punkte nurodytuose teisės aktuose nustatytas VIPVIS valdytojo funkcijas.

8. VIPVIS tvarkytojo funkcijos:

8.1. Atlikti VIPVIS nuostatuose nustatytas funkcijas.

8.2. Užtikrinti saugos dokumentų ir kitų VIPVIS valdytojo priimtų teisės aktų, susijusių su VIPVIS elektroninės informacijos sauga, įgyvendinimą.

8.3. Pagal kompetenciją prižiūrėti VIPVIS komponentus (kompiuterius, operacines sistemas ir kitus VIPVIS komponentus, nurodytus Saugos nuostatų 14.3 papunktyje), užtikrinti jų veikimą.

8.4. Įgyvendinti VIPVIS elektroninės informacijos saugos reikalavimus.

8.5. Užtikrinti VIPVIS elektroninės informacijos saugą.

8.6. Teikti VIPVIS valdytojui pasiūlymus dėl VIPVIS elektroninės informacijos saugos tobulinimo.

8.7. VIPVIS valdytojo pavedimu skirti VIPVIS saugos įgaliotinį ir VIPVIS administratorius.

8.8. Savo institucijose atlikti kitas Saugos nuostatuose ir Saugos nuostatų 19 punkte nurodytuose teisės aktuose nustatytas VIPVIS tvarkytojo funkcijas.

9. Už elektroninės informacijos saugą pagal kompetenciją atsako VIPVIS valdytojas ir VIPVIS tvarkytojas.

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

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

12. VIPVIS saugos įgaliotinio funkcijos:

12.1. Koordinuoti ir prižiūrėti elektroninės informacijos saugos politikos įgyvendinimą saugos dokumentuose nustatyta tvarka.

12.2. Teikti VIPVIS valdytojo vadovui pasiūlymus dėl:

12.2.1. saugos dokumentų priėmimo, keitimo;

12.2.2. informacinių technologijų saugos atitikties vertinimo atlikimo pagal Informacinių technologijų saugos atitikties vertinimo metodiką, patvirtintą Lietuvos Respublikos krašto apsaugos ministro.

12.3. Teikti VIPVIS tvarkytojo vadovui pasiūlymus dėl VIPVIS administratorių paskyrimo ir reikalavimų jiems nustatymo.

12.4. Organizuoti rizikos ir informacinių technologijų saugos atitikties įvertinimą.

12.5. Koordinuoti elektroninės informacijos saugos incidentų tyrimą, bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės.

12.6. Teikti VIPVIS administratoriams ir VIPVIS naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos politikos įgyvendinimo.

12.7. 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 aprašas), nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas, atlikti kitas saugos dokumentuose ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše saugos įgaliotiniui priskirtas funkcijas.

13. VIPVIS administratoriai pagal atliekamas funkcijas skirstomi į grupes:

13.1. VIPVIS koordinuojantis administratorius, kuris prižiūri VIPVIS administratorių veiklą, siekdamas užtikrinti tinkamą VIPVIS administratorių funkcijų atlikimą;

13.2. VIPVIS naudotojų administratoriai, kurie atlieka funkcijas, susijusias su VIPVIS naudotojų teisių valdymu savo institucijose;

13.3. VIPVIS komponentų administratoriai, kurie atlieka funkcijas, susijusias su VIPVIS komponentais (techninė ir programinė įranga, kurios pagrindu funkcionuoja VIPVIS ir užtikrinama joje tvarkomos elektroninės informacijos sauga) ir VIPVIS komponentų sąranka;

14. VIPVIS administratoriai yra atsakingi už tinkamą saugos dokumentuose nustatytų funkcijų atlikimą.

15. VIPVIS administratoriai privalo vykdyti VIPVIS saugos įgaliotinio nurodymus ir pavedimus dėl VIPVIS saugos ir kibernetinio saugumo užtikrinimo, pagal kompetenciją reaguoti į elektroninės informacijos saugos incidentus ir teikti VIPVIS saugos įgaliotiniui informaciją apie pagrindinių saugos užtikrinimo komponentų būklę.

16. Atlikdamas VIPVIS sąrankos pakeitimus, VIPVIS komponentų administratorius turi laikytis VIPVIS pokyčių valdymo tvarkos, nustatytos VIPVIS valdytojo tvirtinamose VIPVIS saugaus elektroninės informacijos tvarkymo taisyklėse.

17. VIPVIS komponentų administratorius privalo patikrinti (peržiūrėti) VIPVIS sąranką ir VIPVIS būsenos rodiklius reguliariai – ne rečiau kaip kartą per metus ir (arba) atlikus VIPVIS pakeitimus.

18. Tvarkant VIPVIS elektroninę informaciją ir užtikrinant jos saugą, vadovaujamasi šiais teisės aktais:

18.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Reglamentas);

18.2. Kibernetinio saugumo įstatymu;

18.3. Valstybės informacinių išteklių valdymo įstatymu;

18.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

18.5. Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymu;

18.6. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

18.7. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu 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);

18.8. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu;

18.9. Techniniais elektroninės informacijos saugos reikalavimais;

18.10. VIPVIS nuostatais;

18.11. Lietuvos standartais LST EN ISO/IEC 27001:2017, LST EN ISO/IEC 27002:2017.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

19. VIPVIS tvarkoma elektroninė informacija priskiriama vidutinės svarbos elektroninės informacijos kategorijai. Elektroninė informacija šiai kategorijai priskiriama vadovaujantis Klasifikavimo gairių aprašo 9.2 ir 9.3 papunkčiais

20. VIPVIS pagal joje tvarkomos informacijos svarbą, vadovaujantis Klasifikavimo gairių aprašo 12.3 papunkčiu, yra priskiriama trečiai informacinių sistemų kategorijai.

21. Rizikos vertinimo organizavimas:

21.1. VIPVIS saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Saugos nuostatų 19.11 papunktyje nurodytus Lietuvos standartus, kasmet arba po esminių organizacinių ar sisteminių pokyčių organizuoja VIPVIS rizikos

įvertinimą. VIPVIS rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu. Prireikus VIPVIS saugos įgaliotinis gali organizuoti neeilinį VIPVIS rizikos įvertinimą.

21.2. Organizuojant rizikos vertinimą turi būti paskirti už rizikos vertinimą, rizikos vertinimo proceso priežiūrą ir nuolatinį tobulinimą atsakingas asmuo arba asmenys ir nustatyti jiems taikomi kvalifikaciniai reikalavimai. Už rizikos vertinimą, rizikos vertinimo proceso priežiūrą ir nuolatinį tobulinimą atsakingu asmeniu gali būti skiriamas VIPVIS valdytojo arba VIPVIS tvarkytojo darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros ir nuolatinio tobulinimo paslaugas teikiančiu subjektu.

21.3. Rizikos vertinimo metu turi būti:

21.3.1. nustatomos grėsmės ir pažeidžiamumas, galintys turėti įtakos VIPVIS elektroninės informacijos saugai;

21.3.2. nustatomos galimos grėsmių ir pažeidžiamumo poveikio vykdomai veiklai sritys;

21.3.3. įvertinama VIPVIS pažeidimo grėsmių tikimybė ir pasekmės;

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

21.4. VIPVIS rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama VIPVIS valdytojo vadovui ir VIPVIS tvarkytojo vadovui. Rengiant rizikos įvertinimo ataskaitą, nustatomi elektroninės informacijos saugai įtakos galintys turėti rizikos veiksniai, jų galima žala, pasireiškimo tikimybė ir pobūdis, galimi rizikos valdymo būdai, rizikos priimtinumo kriterijai. Svarbiausi rizikos veiksniai yra šie:

21.4.1. subjektyvūs netyčiniai (VIPVIS tvarkymo klaidos ir apsirikimai, ištrynimas, klaidingas teikimas, fiziniai informacinių technologijų sutrikimai, perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas);

21.4.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis VIPVIS elektronine informacija, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės);

21.4.3. 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.

21.5. Rizikos veiksniai rizikos įvertinimo ataskaitoje turi būti išdėstyti pagal prioritetus ir priimtiną rizikos lygį.

21.6. Atsižvelgdamas į rizikos įvertinimo ataskaitą, VIPVIS 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.

21.7. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas VIPVIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.

21.8. Atsižvelgiant į atlikto rizikos vertinimo rezultatus, taip pat jeigu Saugos nuostatų 23 punkte nustatyta tvarka atliekamo informacinių technologijų saugos atitikties vertinimo metu nustatoma kibernetinių incidentų valdymo ir šalinimo, institucijos nepertraukiamos veiklos užtikrinimo trūkumų, atitinkamai turi būti tobulinamas VIPVIS veiklos tęstinumo valdymo planas ir (arba) kibernetinių incidentų valdymo planas. Šių planų veiksmingumo išbandymo rezultatai išdėstomi šių planų veiksmingumo išbandymo ataskaitose ir pastebėtų trūkumų ataskaitose, kurių kopijos ne vėliau kaip per 5 darbo dienas nuo šių dokumentų priėmimo pateikiamos Nacionaliniam kibernetinio saugumo centrui.

22. Informacinių technologijų saugos atitikties vertinimo organizavimas:

22.1. Siekiant užtikrinti saugos dokumentuose nustatytų elektroninės informacijos saugos reikalavimų įgyvendinimo organizavimą ir kontrolę, ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip, turi būti organizuojamas VIPVIS informacinių technologijų saugos atitikties vertinimas.

22.2. Informacinių technologijų saugos atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka.

22.3. VIPVIS atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

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

22.5. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas VIPVIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.

23. Elektroninės informacijos saugos būklės gerinimas:

23.1. Techninės, programinės, organizacinės VIPVIS elektroninės informacijos saugos priemonės pasirenkamos atsižvelgiant į VIPVIS valdytojo turimus išteklius, vadovaujantis šiais principais:

23.1.1. Liekamoji rizika turi būti sumažinta iki priimtino lygio.

23.1.2. Saugos priemonės diegimo kaina turi būti tapati tvarkomos elektroninės informacijos vertei.

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

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

24. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai nustatomi pagal Saugos nuostatų 20 punkte nustatytą VIPVIS svarbos kategoriją, vadovaujantis Saugos nuostatų 18 punkte nurodytais teisės aktais ir standartais.

25. Organizaciniai ir techniniai elektroninės informacijos saugos reikalavimai:

25.1. Naudojama ir operatyviai atnaujinama programinė įranga, skirta VIPVIS nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto) apsaugoti. Šios programinės įrangos naudojimo nuostatos ir jos atnaujinimo reikalavimai (ilgiausias leidžiamas neatnaujinimo laikas) nustatomi VIPVIS saugaus elektroninės informacijos tvarkymo taisyklėse.

25.2. VIPVIS techninėje įrangoje ir VIPVIS naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos, atnaujinimo ir kt. reikalavimai nustatomi VIPVIS saugaus elektroninės informacijos tvarkymo taisyklėse.

25.3. Turi būti naudojama kompiuterių tinklo filtravimo įranga (užkardos, turinio kontrolės sistemos, įgaliotieji serveriai (angl. *proxy server*) ir kt.). Išsamios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos VIPVIS saugaus elektroninės informacijos tvarkymo taisyklėse.

25.4. Užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą, turi būti naudojamas šifravimas, virtualus privatusis tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas. Metodų, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą (nuotolinio prisijungimo prie VIPVIS 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), aprašymai pateikiami VIPVIS saugaus elektroninės informacijos tvarkymo taisyklėse.

25.5. Stacionariuosius kompiuterius leidžiama naudoti tik VIPVIS valdytojo ir VIPVIS tvarkytojo patalpose. Nešiojamiesiems kompiuteriams, išnešamiems iš VIPVIS valdytojo ar VIPVIS tvarkytojo patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas).

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

26.1. Prieiga prie VIPVIS elektroninės informacijos suteikiama įgyvendinus VIPVIS naudotojų administravimo taisyklėse nurodytas VIPVIS naudotojų autentifikavimo priemones.

26.2. Per metus turi būti užtikrintas VIPVIS prieinamumas ne mažiau kaip 95 proc. laiko darbo metu darbo dienomis.

26.3. VIPVIS elektroninė informacija perduodama automatiniu būdu arba asinchroniniu režimu pagal duomenų teikimo sutartis, kuriose nustatytos perduodamos elektroninės informacijos specifikacijos, kopijų skaičius ir kitos elektroninės informacijos perdavimo sąlygos ir tvarka.

26.4. VIPVIS duomenų srautas, perduodamas per duomenų perdavimo linijas, šifruojamas.

26.5. VIPVIS elektroninei informacijai perduoti naudojamas Saugus valstybinis duomenų perdavimo tinklas arba kitas šifruotas perdavimo kanalas, užtikrinantis saugų informacijos perdavimą.

27. Atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

27.1. Atsarginės elektroninės informacijos kopijos daromos kiekvieną dieną automatiškai.

27.2. Elektroninė informacija kopijose turi būti užšifruota.

27.3. Laikmena, kurioje yra kopija, pažymima specialia etikete.

27.4. Už elektroninės informacijos atsarginių kopijų darymą ir saugojimą atsakingi VIPVIS administratoriai, kurių pareigybės aprašymuose nurodyta ši funkcija.

27.5. Atkurti informaciją iš elektroninės informacijos kopijų gali tik VIPVIS administratoriai.

27.6. Atkurti informaciją iš elektroninės informacijos kopijų turi būti įmanoma per 24 valandas. Atsarginės elektroninės informacijos kopijos turi būti saugomos ne mažiau kaip 5 darbo dienas.

27.7. Bandymą atkurti VIPVIS elektroninę informaciją bent kartą per metus atlieka VIPVIS administratoriai. Šio bandymo metu VIPVIS elektroninė informacija atkuriama taip, kaip ji būtų atkuriama tuo atveju, jei būtų netikėtai prarasti duomenys.

27.8. Atsarginės elektroninės informacijos kopijos saugomos kitoje patalpoje nei VIPVIS serveriai. Patalpos, kuriose saugomos atsarginės VIPVIS elektroninės informacijos kopijos, turi

atitikti patalpoms, kuriose saugoma VIPVIS elektroninė informacija, nustatytus reikalavimus. Patalpų, kuriose saugoma VIPVIS elektroninė informacija, reikalavimai nustatomi VIPVIS saugaus elektroninės informacijos tvarkymo taisyklėse.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

28. VIPVIS saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti elektroninės informacijos saugos srities kvalifikaciją, savo darbe vadovautis Saugos dokumentais, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą. VIPVIS tvarkytojas turi sudaryti sąlygas kelti VIPVIS saugos įgaliotinio kvalifikaciją.

29. VIPVIS saugos įgaliotiniu negali būti skiriamas asmuo, neatitinkantis Valstybės informacinių išteklių valdymo įstatymo 42 straipsnio reikalavimų.

30. VIPVIS saugos įgaliotiniui kasmet turi būti organizuojami mokymai kibernetinio saugumo klausimais arba sudaromos sąlygos kelti kvalifikaciją individualiai.

31. VIPVIS administratoriai pagal kompetenciją privalo išmanyti informacijos saugos principus, mokėti užtikrinti VIPVIS ir joje tvarkomos elektroninės informacijos saugą, administruoti ir prižiūrėti VIPVIS komponentus (stebėti VIPVIS komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, gebėti užtikrinti nepertraukiamą VIPVIS komponentų funkcionavimą). VIPVIS administratoriai turi būti susipažinę su Saugos dokumentais.

32. VIPVIS administratoriais skiriami VIPVIS tvarkytojo darbuotojai, išmanantys darbą su VIPVIS taikomąja programine įranga ir gebantys atlikti funkcijas, susijusias su VIPVIS naudotojų teisių valdymu. VIPVIS administratoriai turi būti pasirašę konfidencialumo pasižadėjimą saugoti asmens duomenų paslaptį.

33. VIPVIS administratoriai turi būti susipažinę su duomenų bazių administravimo ir priežiūros pagrindais ir kontroliuoti paslaugų teikėjus, administruojančius ir prižiūrinčius VIPVIS techninę ir programinę įrangą.

34. VIPVIS naudotojai privalo turėti darbo kompiuteriu įgūdžių, būti susipažinę su Saugos dokumentais.

35. VIPVIS tvarkytojo darbuotojai (išskyrus VIPVIS saugos įgaliotinį ir VIPVIS administratorius), kurie dalyvauja prižiūrint, valdant ir tobulinant VIPVIS, privalo gerai išmanyti VIPVIS veiklos principus, būti susipažinę ir vykdyti Saugos dokumentuose nustatytus reikalavimus bei atlikti Saugos dokumentuose nurodytas procedūras.

36. VIPVIS saugos įgaliotinis įvairiais būdais (priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems VIPVIS naudotojams, VIPVIS administratoriams) VIPVIS naudotojams primena apie elektroninės informacijos saugos ar kibernetinio saugumo problemas.

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

38. Mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje) būdu.

39. VIPVIS naudotojų, VIPVIS administratorių mokymai turi būti organizuojami periodiškai, ne rečiau kaip kartą per dvejus kalendorinius metus. Už mokymų organizavimą atsakingas VIPVIS saugos įgaliotinis.

V SKYRIUS
VIPVIS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

40. Tvarkyti ir naudoti VIPVIS elektroninę informaciją gali tik VIPVIS naudotojai, susipažinę su VIPVIS Saugos dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, ir raštu sutikę laikytis šių teisės aktų reikalavimų. Už VIPVIS naudotojų supažindinimą su šiais Saugos dokumentais pagal kompetenciją yra atsakingas VIPVIS saugos įgaliotinis. Asmenys, kurie tvarko asmens duomenis, privalo laikytis Reglamente nustatytų asmens duomenų tvarkymo principų ir reikalavimų.

41. VIPVIS naudotojų supažindinimas su saugos dokumentais ir atsakomybe už saugos dokumentuose nustatytų reikalavimų nesilaikymą bei su informacija apie saugos dokumentų priėmimą, pakeitimą ar pripažinimą netekusiais galios užtikrinamas programinėmis VIPVIS tvarkytojo priemonėmis.

42. VIPVIS administratorius su Saugos nuostatais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai supažindina VIPVIS saugos įgaliotinis per 10 darbo dienų nuo VIPVIS įteisinimo, o su kitais saugos dokumentais – per 10 darbo dienų nuo šių dokumentų patvirtinimo.

43. Su saugos dokumentais pakartotinai supažindinama tik iš esmės pasikeitus VIPVIS arba elektroninės informacijos saugą reguliuojantiems teisės aktams.

44. VIPVIS naudotojų supažindinimas su saugos dokumentais ir atsakomybe už saugos dokumentuose nustatytų reikalavimų nesilaikymą bei informacija apie saugos dokumentų priėmimą,

pakeitimą ar pripažinimą netekusiais galios užtikrinamas programinėmis VIPVIS tvarkytojo priemonėmis.

45. VIPVIS naudotojai, VIPVIS administratoriai ir VIPVIS saugos įgaliotinis, pažeidę Saugos dokumentų ir saugų elektroninės informacijos tvarkymą reguliuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

46. VIPVIS valdytojas saugos dokumentus gali keisti savo arba 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 pakeitimai, susiję su teisės technika. Nacionaliniam kibernetinio saugumo centrui turi būti pateiktos keičiamų saugos dokumentų kopijos.

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

Ekonomikos ir inovacijų
viceministras
Civilis

Ekonomikos ir inovacijų ministerijos
Teisės departamento
direktorė
2018 12 27
Rūta Jovaišienė