PATVIRTINTA
Akcinės bendrovės „Via Lietuva“ generalinio direktoriaus

2025 m. d. įsakymu Nr.

VALSTYBINĖS REIKŠMĖS KELIŲ EISMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės reikšmės kelių eismo informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Valstybinės reikšmės kelių eismo informacinės sistemos (toliau – EIS) kibernetinio saugumo politiką, kurios tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti EIS duomenis ir užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo netyčinio ar neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jos.

2. Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme ir Lietuvos Respublikos standartuose LST ISO/IEC 27002 ir LST ISO/IEC 27001.

3. EIS kibernetinio saugumo politiką nustato šie akcinės bendrovės „Via Lietuva“ (toliau – Via Lietuva) generalinio direktoriaus tvirtinami teisės aktai:

3.1. Valstybinės reikšmės kelių eismo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės;

3.2. Valstybinės reikšmės kelių eismo informacinės sistemos naudotojų administravimo taisyklės;

3.3. Valstybinės reikšmės kelių eismo informacinės sistemos veiklos tęstinumo valdymo planas.

4. Saugos nuostatai kartu su Saugos nuostatų 3 punkte nurodytais teisės aktais sudaro EIS kibernetinio saugumo politikos dokumentus.

5. EIS kibernetinio saugumo užtikrinimo tikslai – sudaryti sąlygas automatizuotomis priemonėmis saugiai tvarkyti EIS elektroninę informaciją, užtikrinti EIS elektroninės informacijos patikimumą, konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterinės, programinės ir ryšių įrangos funkcionavimą, bei vykdyti elektroninės informacijos saugos ir kibernetinių incidentų prevenciją.

6. Užtikrinant saugų EIS veikimą, nustatomos elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

6.1. administracinių, techninių ir kitų priemonių, skirtų duomenų saugai užtikrinti, įgyvendinimas ir kontrolė;

6.2. EIS veiklos tęstinumo užtikrinimas;

6.3. EIS elektroninės informacijos tvarkymo kontrolė;

6.4. saugaus darbo su EIS elektronine informacija kontrolė;

6.5. fizinė EIS elektroninės informacijos tvarkymo priemonių (tarnybinių stočių, informacijos perdavimo įrangos, programinės įrangos) ir patalpų apsauga.

6.6. EIS tvarkomų asmens duomenų apsauga.

7. Saugos nuostatais privalo vadovautis Via Lietuva darbuotojai, dirbantys pagal darbo sutartis (toliau – EIS vidiniai naudotojai), kibernetinio saugumo vadovas, EIS saugos įgaliotinis

(toliau – saugos įgaliotinis), EIS administratorius, EIS duomenų valdymo įgaliotinis (toliau – duomenų valdymo įgaliotinis), kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai.

8. EIS valdytoja, duomenų valdytoja yra Via Lietuva, EIS pagrindinė tvarkytoja, duomenų tvarkytoja – Via Lietuva.

9. EIS valdytojo, duomenų valdytojo funkcijos ir atsakomybė:

9.1. atsako už EIS kibernetinio saugumo politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo, bei duomenų teikimo gavėjams teisėtumą;

9.2. rengia ir tvirtina EIS kibernetinio saugumo politikos dokumentus, prižiūri ir kontroliuoja, kad EIS būtų tvarkoma vadovaujantis šiais dokumentais, EIS nuostatais ir kitais teisės aktais, reglamentuojančiais kibernetinį saugumą;

9.4. atsižvelgdamas į rizikos vertinimo ataskaitą, prireikus tvirtina rizikos valdymo planą;

9.5. priima sprendimą dėl EIS atitikties Kibernetinio saugumo įstatymui, Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Aprašas) ir EIS kibernetinio saugumo politikos dokumentuose nustatytiems reikalavimams vertinimo (toliau – EIS atitikties vertinimas) atlikimo;

9.6. prireikus tvirtina EIS atitikties vertinimo metu identifikuotų neatitikčių šalinimo planą;

9.7. atsako už EIS pokyčių ir plėtros įgyvendinimą;

9.8. pagal kompetenciją atsako už EIS kibernetinį saugumą;

9.9. paskiria saugos įgaliotinį, duomenų valdymo įgaliotinį, EIS administratorių, kibernetinio saugumo vadovą;

9.10. vykdo kitas Saugos nuostatų ir kitų teisės aktų, reglamentuojančių kibernetinį saugumą, nustatytas funkcijas;

9.11 priima sprendimus dėl techninių ir programinių priemonių, būtinų elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

9.12 koordinuoja EIS tvarkytojų darbą įgyvendinant elektroninės informacijos saugos reikalavimus;

9.13 priima sprendimus dėl EIS elektroninės informacijos saugos priemonių finansavimo.

10. Via Lietuvos, kaip EIS tvarkytojos ir duomenų tvarkytojos, funkcijos ir atsakomybės:

10.1. atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą ir EIS kibernetinio saugumo reikalavimų atitiktį kibernetinio saugumo politikos dokumentams;

10.2. teikia EIS valdytojui, duomenų valdytojui pasiūlymus dėl EIS plėtros, saugos ir funkcionalumo;

10.3. organizuoja plėtrą ir EIS pakeitimų įdiegimą;

10.4. atsako už EIS elektroninės informacijos saugumą, užtikrina tinkamą EIS administravimą ir nepertraukiamą EIS veiklą;

10.5. pagal kompetenciją atsako už EIS elektroninės informacijos tvarkymo teisėtumą, saugumą;

10.6. sukuria automatinių duomenų mainų su duomenų teikėjais ir gavėjais sąsajas ir vykdo jų priežiūrą;

10.7. gauna duomenis iš kitų informacinių sistemų, teikia informaciją registrų informacinėms sistemoms ir kitoms informacinėms sistemoms;

10.8. analizuoja EIS procesus ir audituoja EIS vidinių naudotojų bei asmenų, besinaudojančių EIS paslaugomis (toliau – EIS išorės naudotojai), veiksmus;

10.9. atlieka kitas EIS valdytojo, duomenų valdytojo pavestas, EIS kibernetinio saugumo politikos dokumentuose bei teisės aktuose, reglamentuojančiuose kibernetinį saugumą, priskirtas funkcijas.

11. Lietuvos transporto saugos administracijos, kaip EIS tvarkytojos ir duomenų tvarkytojos, funkcijos ir atsakomybės:

11.1. atsako už administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą ir kibernetinio saugumo reikalavimų atitiktį EIS kibernetinio saugumo politikos dokumentams;

11.2. teikia EIS valdytojui, duomenų valdytojui pasiūlymus dėl EIS plėtros, saugos ir funkcionalumo;

11.3. paskiria EIS administratorių;

11.4. pagal kompetenciją atsako už EIS elektroninės informacijos tvarkymo teisėtumą, saugumą;

11.5. atlieka kitas EIS valdytojo, duomenų valdytojo pavestas, EIS kibernetinio saugumo politikos dokumentuose bei teisės aktuose, reglamentuojančiuose kibernetinį saugumą, priskirtas funkcijas.

12. Kibernetinio saugumo vadovo ir saugos įgaliotinio funkcijos:

12.1. organizuoja EIS atitikties Aprašo reikalavimams vertinimą Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) patvirtintos Kibernetinio saugumo auditų atlikimo metodikos nustatyta tvarka;

12.2. užtikrina, kad EIS kibernetinio saugumo politikos dokumentai būtų parengti ir periodiškai atnaujinami remiantis Kibernetinio saugumo įstatymo ir jį įgyvendinančių teisės aktų reikalavimais;

12.3. koordinuoja EIS kibernetinių incidentų tyrimus ir bendradarbiauja su kompetentingomis institucijoms, tiriančiomis kibernetinius incidentus bei neteisėtas veikas, susijusias su kibernetiniais incidentais;

12.4. teikia EIS administratoriui (-iams) ir (ar) EIS vidiniams naudotojams bei EIS išorės naudotojams (toliau kartu – EIS naudotojai) privalomus vykdyti nurodymus ir pavedimus, susijusius su EIS kibernetinio saugumo politikos dokumentuose nustatytų reikalavimų įgyvendinimu;

12.5. organizuoja rizikos vertinimą ir dalyvauja rizikos vertinimo procese, rengia ir teikia tvirtinti Via Lietuvos vadovui ar jo įgaliotam asmeniui rizikos vertinimo ataskaitas ir rizikos valdymo planus;

12.6. organizuoja EIS vidinių naudotojų mokymus kibernetinio saugumo klausimais;

12.7. atlieka kitas EIS kibernetinio saugumo politikos dokumentuose ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

13. Kibernetinio saugumo vadovas ir saugos įgaliotinis negali atlikti EIS administratoriaus funkcijų ar kitų pareigybių funkcijų, susijusių su techninės kompiuterinės įrangos ar programinės įrangos priežiūra ir valdymu.

14. kibernetinio saugumo vadovas gali vykdyti saugos įgaliotinio funkcijas.

15. IS administratoriaus funkcijos ir atsakomybė:

15.1. atsako už EIS sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių ir jų valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo ir prevencijos sistemų, elektroninės informacijos perdavimo tinklų, duomenų saugyklų, bylų serverių ir kitos techninės ir programinės įrangos, kurios pagrindu funkcionuoja EIS ir užtikrinama joje tvarkomos elektroninės informacijos sauga ir kibernetinis saugumas bei EIS komponentų sąranka) administravimą, EIS komponentų sąrankos aprašymo dokumentacijos parengimą ir atnaujinimą, saugos priemonių EIS pažeidžiamoms vietoms parinkimą ir jų atitiktį EIS kibernetinio saugumo politikos dokumentų reikalavimams;

15.2. kontroliuoja EIS veikimą;

15.3. registruoja EIS naudotojus sistemoje, tvarko jų duomenis, prieigos teises ir leidžiamus veiksmus EIS;

15.4. dalyvauja svarstant teikimus dėl EIS pokyčių projektavimo, konstravimo ir diegimo, dalyvauja aptariant EIS plėtrą ir vykdant EIS plėtros specifikavimo, projektavimo, konstravimo ir diegimo etapų darbus;

15.5. teikia kibernetinio saugumo vadovui ir (ar) saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;

15.6. atsako už nepertraukiamą EIS veikimą;

15.7. konsultuoja EIS naudotojus;

15.8. teikia kibernetinio saugumo vadovui ir (ar) saugos įgaliotiniui pasiūlymus dėl EIS palaikymo, priežiūros ir kibernetinio saugumo;

15.9. ne rečiau kaip kartą per metus ir (arba) atlikus EIS pakeitimus tikrina (peržiūri) EIS sąranką ir EIS būsenos rodiklius;

15.10. kontroliuoja ir prižiūri programinės ir kompiuterinės įrangos diegimo procesus;

15.11. tvarko EIS veikimo parametrų įrašus;

15.12. atsako už EIS elektroninės informacijos atsarginių kopijų darymą, tinkamumą ir saugojimą;

15.13. dalyvauja atkuriant EIS elektroninę informaciją iš elektroninės informacijos atsarginių kopijų;

15.14. perkelia EIS elektroninę informaciją į EIS duomenų archyvą ir tvarko elektroninės informacijos perkėlimo įrašų žurnalą EIS nuostatuose nustatyta tvarka;

15.15. naikina EIS elektroninę informaciją EIS duomenų archyvuose ir tvarko elektroninės informacijos naikinimo įrašų žurnalą EIS nuostatuose nustatyta tvarka;

15.16. tvarko EIS eksploatacijos žurnalą;

15.17. vykdo kibernetinio saugumo vadovo ir (ar) saugos įgaliotinio nurodymus ir pavedimus, susijusius su EIS kibernetinio saugumo politikos įgyvendinimu;

15.18. reaguoja į EIS kibernetinius incidentus, registruoja EIS kibernetinius incidentus ir informuoja apie juos kibernetinio saugumo vadovą ir (ar) saugos įgaliotinį, teikia pasiūlymus dėl minėtų incidentų šalinimo, taip pat informuoja kibernetinio saugumo vadovą ir (ar) saugos įgaliotinį apie nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

15.19. atsako už EIS funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugų administravimą, EIS naudotojų ir registravimo vardų skyrimą, prieigos prie EIS teisių nustatymą;

15.20. atlieka kitas EIS kibernetinio saugumo politikos dokumentuose administratoriui priskirtas funkcijas ir kitus Via Lietuva nurodymus ir pavedimus, susijusius su EIS kibernetinio saugumo užtikrinimu

16. Tvarkant EIS elektroninę informaciją ir užtikrinant jos kibernetinę saugą vadovaujamasi šiais teisės aktais:

16.1. Valstybės informacinių išteklių valdymo įstatymu;

16.2. 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 (Bendrasis duomenų apsaugos reglamentas);

16.3. Kibernetinio saugumo įstatymu;

16.4. Aprašu;

16.5. Valstybės informacinių išteklių svarbos vertinimo metodika, patvirtinta Lietuvos Respublikos ekonomikos ir inovacijų ministro 2023 m. liepos 19 d. įsakymu Nr. 4-418 „Dėl Valstybės informacinių išteklių svarbos vertinimo metodikos patvirtinimo“ (toliau – Metodika);

16.6. Lietuvos standartais LST ISO/IEC 27002, LST ISO/IEC 27001 ir kitais Lietuvos Respublikos ir tarptautiniais grupės „Informacijos technologija. Saugumo metodai“ standartais, naudojamais kaip elektroninės informacijos saugos užtikrinimo rekomendacinės priemonės;

16.7. kitais teisės aktais ir dokumentais, reglamentuojančiais kibernetinį saugumą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

17. Vadovaujantis Metodikos 8.5.3. papunkčiu, EIS tvarkoma elektroninė informacija priskiriama vidutinės svarbos valstybės informacinių išteklių rūšiai.

18. Pagrindiniai rizikos veiksniai, galintys turėti įtakos EIS kibernetiniam saugumui:

18.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai

elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas kita);

18.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis EIS elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymas, saugos pažeidimai, vagystės ir kita);

18.3. 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.

19. EIS rizikos vertinimas atliekamas vadovaujantis šiomis nuostatomis:

19.1. Kibernetinio saugumo vadovas ar saugos įgaliotinis organizuoja EIS rizikos vertinimą ne rečiau kaip kartą per metus, įvykus esminiams Via Lietuva organizaciniams ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliam kibernetiniam incidentui. EIS rizikos vertinimas atliekamas pagal kokybinį rizikos vertinimo metodą.

19.2. Atliekant rizikos vertinimą, atsižvelgiama į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacinės technologijos. Saugumo metodai“ grupės standartus (LST ISO/IEC 27002, LST ISO/IEC 27001 ir LST ISO/IEC TR 15443 ar naujesnius tarptautinius standartus), gerosios praktikos pavyzdžius (COBIT ar kitais) ir elektroninės informacijos saugą reglamentuojančius teisės aktus.

19.3. sutartiniais pagrindais gali būti samdomi tretieji asmenys.

20. EIS rizikos vertinimo metu atliekamos veiklos:

20.1. EIS sudarančių informacinių išteklių inventorizacija;

20.2. įtakos EIS veiklai vertinimas;

20.3. grėsmės ir pažeidimų analizė;

20.4. liekamosios rizikos vertinimas.

21. EIS rizikos vertinimo rezultatai pateikiami rizikos vertinimo ataskaitoje ir ji pateikiama tvirtinimui Via Lietuva vadovui ar jo įgaliotam asmeniui. EIS rizikos vertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos EIS kibernetiniam saugumui, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. EIS rizikos vertinimo ataskaitą rengia arba, jei vertinimą atlieka trečioji šalis, dalyvauja rengiant kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

22. Atsižvelgdamas į rizikos vertinimo ataskaitą, Via Lietuva vadovas ar jo įgaliotas asmuo prireikus tvirtina EIS rizikos valdymo planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis EIS rizikos valdymo priemonėms įgyvendinti, ir įvertina ar reikalingi pokyčiai EIS saugos nuostatuose.

23. Rizikos vertinimo ataskaitos, rizikos valdymo plano kopijas EIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia NKSC į Kibernetinio saugumo informacinę sistemą (toliau – KSIS).

24. Kibernetinio saugumo atitikties reikalavimams vertinimo metu taip pat turi būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinių sistemų kibernetiniam saugumui, vertinimas, kurio metu imituojamos kibernetinės atakos ir vykdomos kibernetinių incidentų imitavimo pratybos.

25. Kibernetinių atakų imitavimas turi būti atliekamas šiais etapais:

25.1. planavimo etapas. Parengiamas pažeidžiamumų nustatymo planas, kuriame apibrėžiami kibernetinių atakų imitavimo tikslai ir darbų apimtis, pateikiamas darbų grafikas, aprašomi planuojamų imituoti kibernetinių atakų tipai (išorinės ir (ar) vidinės), kibernetinių atakų imitavimo būdai (juodosios dėžės (angl. Black Box), baltosios dėžės (angl. White Box) ir (ar) pilkosios dėžės (angl. Grey Box), galima neigiama įtaka veiklai, kibernetinių atakų imitavimo metodologija, programiniai ir (ar) techniniai įrankiai ir priemonės, naudojamos pažeidžiamumams nustatyti, nurodomos už pažeidžiamumų nustatymo plano vykdymą atsakingų asmenų teisės ir pareigos;

25.2. žvalgybos (angl. Reconnaissance) ir aptikimo (angl. Discovery) etapas. Surenkama informacija apie perimetrą, tinklo mazgus, tinklo mazguose veikiančių tarnybinių stočių ir kitų tinklo įrenginių operacines sistemas ir programinę įrangą, paslaugas (angl. *Services*), pažeidžiamumą, konfigūracijas ir kitą sėkmingai kibernetinei atakai įvykdyti reikalingą informaciją;

25.3. kibernetinių atakų imitavimo etapas. Atliekami pažeidžiamumų nustatymo plane numatyti testai;

25.4. ataskaitos parengimo etapas. Kibernetinių atakų imitavimo rezultatai turi būti pateikti kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitoje. Pažeidžiamumų nustatymo plane numatyti testų rezultatai turi būti detalizuojami ataskaitoje ir lyginami su planuotais. Kiekvienas aptiktas pažeidžiamumas turi būti detalizuojamas, klasifikuojamas ir pateikiamos rekomendacijos jam pašalinti. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos vertinimu. Jeigu nustatoma incidentų valdymo ir šalinimo, taip pat organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinami veiklos tęstinumo planai.

26. Siekdamas užtikrinti EIS kibernetinio saugumo politikos dokumentų nuostatų įgyvendinimo kontrolę ne rečiau kaip kartą per metus kibernetinio saugumo vadovas ar saugos įgaliotinis organizuoja EIS atitikties vertinimą pagal Informacinių technologijų saugos atitikties vertinimo metodikos, patvirtintos Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, reikalavimus.

27. Atliekant EIS atitikties vertinimą:

27.1. įvertinama esamos EIS elektroninės informacijos saugos situacijos atitiktis Kibernetinio saugumo įstatymui, Aprašo, EIS kibernetinio saugumo politikos dokumentuose nustatytiems reikalavimams ir kitiems kibernetinį saugumą reglamentuojantiems teisės aktams;

27.2. inventorizuojama EIS techninė ir programinė įranga;

27.3. peržiūrima EIS administratoriui, EIS naudotojams suteiktų teisių atitiktis jų atliekamoms funkcijoms;

27.4. duomenų saugos požiūriu patikrinama EIS techninė ir programinė įranga: visos tarnybinės stotys ir ne mažiau kaip 10 proc. atsitiktinai parinktų EIS vidinių naudotojų darbo vietų;

27.5. įvertinamas pasirengimas užtikrinti EIS veiklos tęstinumą įvykus kibernetiniam incidentui.

28. Atlikus EIS atitikties vertinimą, parengiama EIS atitikties vertinimo ataskaita ir pateikiama tvirtinti Via Lietuva vadovui ar jo įgaliotam asmeniui, taip pat prireikus parengiamas identifikuotų neatitikčių šalinimo planas. Via Lietuva vadovas ar jo įgaliotas asmuo patvirtina šį planą, paskiria atsakingus vykdytojus, reikalingus išteklius ir nustato įgyvendinimo terminus.

29. NKSC prašymu EIS valdytojas ne vėliau kaip per 5 darbo dienas nuo NKSC prašymo gavimo dienos turi pateikti į KSIS EIS atitikties vertinimo ataskaitos, identifikuotų neatitikčių šalinimo plano kopijas.

30. Elektroninės informacijos saugos priemonėms parinkti taikomi šie principai:

30.1. parenkamos priemonės, kurios leidžia užtikrinti patalpų saugą;

30.2. parenkamos priemonės, kurios leidžia užtikrinti kompiuterinės ir programinės įrangos veikimo saugą;

30.3. parenkamos priemonės, kurios leidžia užtikrinti kompiuterių tinklų veikimo saugą;

30.4. parenkamos priemonės, kurios leidžia užtikrinti EIS vidinių naudotojų mokymą ir informavimą apie elektroninės informacijos tvarkymo saugą;

30.5. svarbiausia EIS kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima.

31. informacijos saugos priemonės turi garantuoti:

31.1. elektroninės informacijos saugą jos registravimo ir perdavimo ryšio kanalais, saugojimo, apdorojimo, teikimo ir naudojimo metu;

31.2. elektroninės informacijos saugą nuo nesankcionuoto ar neteisėto naudojimo, kaupimo, keitimo, perdavimo, skelbimo ir sunaikinimo;

31.3. elektroninės informacijos saugą nuo jos pažeidimo esant Saugos nuostatų 18 punkte nurodytiems rizikos veiksniams.

32. Pokyčiai, galintys daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos EIS.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

33. Nustatomi šie EIS naudojamos programinės įrangos reikalavimai:

33.1. IS naudojama programinė įranga turi atitikti programinės įrangos kibernetinio saugumo gerąją praktiką, kuriant programinę įrangą taikomą kibernetinio saugumo gerąją praktiką, programinės įrangos kūrimo struktūras, standartus.

33.2. Specifiniai kibernetinio saugumo reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.

33.3. Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.

33.4. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius kibernetinio saugumo reikalavimus.

33.5.Prieš pradedant naudoti programinę įrangą, turi būti atliktas šios programinės įrangos pažeidžiamumo, pritaikomumo ir infrastruktūros atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti patvirtinta, kol nėra pasiektas reikiamas saugumo lygis.

33.6. Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai.

34. Programinės įrangos, skirtos EIS ir KDV apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos:

34.1. EIS turi būti naudojama antivirusinė programinė įranga, skirta EIS apsaugoti nuo kenksmingos programinės įrangos.

34.2. Antivirusinė programinė įranga turi būti atnaujinama automatiškai ne rečiau kaip kartą per parą.

34.3. EIS vidinių naudotojų kompiuteriuose naudojama įranga, skirta KDV apsaugoti nuo kenksmingos programinės įrangos, turi apsaugoti ir elektroninio pašto programinę įrangą nuo nepageidaujamo pašto ar kenksmingų programų patekimo į KDV.

34.4. Atsiradus požymių, kad KDV yra kenksmingų programų, turi būti patikrinami visi KDV standieji diskai, naudojama programinė įranga, skirta EIS ir KDV apsaugoti nuo kenksmingos programinės įrangos.

34.5. KDV esančios programinės įrangos, skirtos EIS ir KDV apsaugoti nuo kenksmingos programinės įrangos, nustatymai turi būti parinkti pagal rekomenduojamus tokios programinės įrangos gamintojų reikalavimus arba pagal vidinio kompiuterių tinklo administratoriaus rekomendacijas.

34.6. Programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu. Draudžiama EIS techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius.

34.7. Apsaugos sistema privalo automatiškai informuoti EIS administratorių apie KDV ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 24 valandas.

34.8. EIS operacinės sistemos ir naudojami programinės įrangos gamintojų rekomenduojami atnaujinimai turi būti įdiegiami nedelsiant.

35. Metodai ir priemonės, kurie taikomi užtikrinant prieigą prie EIS:

35.1. EIS naudotojai privalo turėti galimybę naudotis tik tokiomis teisėmis ir tais duomenimis, kurie jiems numatyti nustačius prieigos prie EIS teises, įgyvendinant principą „būtina žinoti“.

35.2. EIS naudotojams suteikiamos teisės naudotis tomis EIS funkcijomis, kurios negali pakenkti EIS veikimui ir duomenims (viešai teikiamų duomenų analizės ir peržiūros funkcijos).

35.3. EIS priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus klasifikatorių, kuriuo naudojantis nebūtų galima atlikti EIS naudotojo funkcijų.

35.4. EIS naudotojas turi būti EIS unikaliai identifikuojamas – EIS naudotojas turi patvirtinti savo tapatybę slaptažodžiu, EIS naudotojui suteiktas pirminis slaptažodis turi būti pakeistas pirmo prisijungimo metu. Slaptažodžiai sudaromi, keičiami ir jų galiojimo trukmė nustatoma vadovaujantis EIS naudotojų administravimo taisyklėmis.

35.5. Prieigą prie EIS suteikia, apriboja ir panaikina EIS administratorius.

35.6. Teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam EIS naudotojui.

35.7. Siekiant užtikrinti, kad naudotojo teisė dirbti su konkrečia EIS posisteme būtų kontroliuojama, naudotojų paskyros turi būti peržiūrimos ne rečiau, kaip kas 3 (tris) mėnesius, EIS vidiniam naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai EIS vidinis naudotojas atostogauja, vykdomas EIS vidinio naudotojo veiklos tyrimas ir pan. Teisė dirbti su EIS turi būti sustabdoma, kai EIS naudotojas nesinaudoja sistema ilgiau kaip 3 (tris) mėnesius, o administratorių – ne ilgiau kaip 2 (du) mėn. Pasibaigus darbo santykiams, EIS naudotojo teisė naudotis EIS turi būti panaikinta nedelsiant.

35.8. Baigus darbą, turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo EIS, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą.

35.9. EIS naudotojui 15 min. neatliekant jokių veiksmų, EIS turi užsirakinti, kad toliau naudotis EIS būtų galima tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus.

35.10. Prisijungimo prie kompiuterių tinklo laikas ir trukmė nėra ribojami, EIS pasiekiama visą parą.

36. Programinės įrangos, įdiegtos KDV ir tarnybinėse stotyse, naudojimo nuostatos ir reikalavimai:

36.1. EIS turi būti naudojama tik legali programinė įranga.

36.2. EIS KDV administratorius turi nustatyti, kad EIS naudotojai neturėtų teisių diegti ir naudoti pašalinės programinės įrangos, keisti sistemos, kompiuterio ar programinės įrangos sistemų nustatymų. Programinę įrangą, reikalingą EIS vidinio naudotojo funkcijoms atlikti, KDV diegia, atnaujina, kontroliuoja ir prižiūri EIS administratorius. Kiti asmenys (paslaugų teikėjų specialistai) gali diegti programinę įrangą tik EIS administratoriaus prižiūrimi.

36.3. Diegti ir naudoti programinę įrangą, nesusijusią su Via Lietuva veikla ar EIS vidinio naudotojo atliekamomis funkcijomis (žaidimų, bylų siuntimo, internetinių pokalbių programas ir kt.), draudžiama.

36.4. Tarnybinėse stotyse ir EIS vidinių naudotojų kompiuterizuotose darbo vietose privalo būti naudojama programinė įranga, kuri apsaugo nuo kenksmingos programinės įrangos ir kuri turi būti atnaujinama ne rečiau kaip kartą per parą.

36.5. KDV, programinė įranga, jos sertifikatai ir licencijos kasmet turi būti inventorizuojami.

36.6. Turi būti naudojama programinė įranga, leidžianti atlikti EIS naudojamų kompiuterių tinklų stebėseną ir užtikrinančią šių tinklų kibernetinį saugumą.

36.7. Programinė įranga turi būti nuolat atnaujinama laikantis gamintojo reikalavimų.

36.8. EIS tarnybinėse stotyse negali būti įdiegta programinė įranga, kuri yra nesusijusi su EIS veikla.

37. Turi būti suformuotos leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos ir metodai, užtikrinantys saugų EIS duomenų teikimą ir (ar) gavimą:

37.1. Stacionariuosiuose ir nešiojamuosiuose kompiuteriuose EIS įjungimo metu turi būti identifikuojamas EIS vidinis naudotojas.

37.2. Stacionarieji ir nešiojamieji EIS vidinių naudotojų kompiuteriai privalo būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai. Iš kompiuterių, kurie perduodami remontui ar techninei priežiūrai, turi būti pašalinta visa neskelbtina EIS elektroninė informacija.

37.3. EIS vidiniai naudotojai, darbinėms funkcijoms atlikti naudojantys nešiojamuosius kompiuterius, išnešdami juos iš Via Lietuva patalpų, norėdami EIS elektroninę informaciją perduoti kompiuterių tinklais ne savo darbo vietoje, turi naudoti duomenų šifravimą, papildomą EIS naudotojo tapatybės patvirtinimą, rakinimo įrenginį. Nešiojamojo kompiuterio pagrindinės įvesties ir išvesties sistema (BIOS) turi būti apsaugota slaptažodžiu ir nurodytas standusis diskas kaip pirminis paleidimo įrenginys. Iš išorės prie EIS duomenų bazės prisijungimas ribojamas. Nešiojamuosiuose kompiuteriuose ar išorinėse kompiuterinėse laikmenose esantys duomenys turi būti šifruojami. EIS vidiniai naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

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

38.1. Techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose minimos priemonės, duomenų perdavimas šifruotu virtualaus privataus tinklo (angl. virtual private network – VPN) duomenų perdavimo kanalu arba naudojant saugų HTTPS (angl. Hypertext Transfer Protocol Secure) duomenų perdavimo protokolą. Jei sistema palaiko, rekomenduojama įjungti dviejų veiksnių tapatumo patvirtinimo priemonę.

38.2. EIS vidiniams naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie EIS galimybė.

38.3. Kompiuterinis tinklas, prie kurio prijungtos EIS tarnybinės stotys ir EIS vidinių naudotojų kompiuteriai, nuo viešojo interneto turi būti atskirtas ugniasienėmis ir įsilaužimų aptikimo ir prevencijos įranga, už kurios administravimą ir priežiūrą atsakingas EIS administratorius.

38.4. Visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos.

38.5. Naudojamos turinio filtravimo sistemos.

38.6. Naudojama programinė įranga, leidžianti atlikti EIS naudojamų kompiuterių tinklų monitoringą ir užtikrinanti šių tinklų kibernetinio saugumo prevencines priemones.

38.7. EIS žurnaliniuose įrašuose (angl. logs) turi būti fiksuojami šie duomenys:

38.7.1. įvykio data ir tikslus laikas,

38.7.2. įvykio rūšis (informacija, klaida, saugumo pranešimas, sisteminis pranešimas, perspėjimas (angl. *warning*)),

38.7.3. naudotojo, administratoriaus ir (arba) tinklų ir informacinės sistemos įrenginio, susijusio su įvykiu, identifikavimo duomenys,

38.7.4. įvykio aprašymas.

38.8. Fiksuojami žurnaliniai įrašai turi būti saugomi specializuotoje tam pritaikytoje techninėje ar programinėje įrangoje ne trumpiau kaip 90 kalendorinių dienų. Draudžiama žurnalinius įrašus trinti, keisti, kol nesibaigęs žurnalinių įrašų saugojimo terminas.

38.9. Naudojimasis žurnaliniais įrašais turi būti kontroliuojamas ir fiksuojamas, t.y. žurnaliniai įrašai turi būti pasiekiami tik įgaliotiems asmenims ir kibernetinio saugumo vadovui (peržiūros teisėmis).

38.10. Žurnalinių įrašų duomenys turi būti analizuojami įgalioto asmens ne rečiau kaip kartą per mėnesį ir apie analizės rezultatų nuokrypius informuojamas kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

39. Užtikrinant saugų elektroninės informacijos teikimą kitoms valstybės institucijoms ir (ar) gavimą iš jų, naudojamas šifruotas VPN arba Saugusis valstybinis duomenų perdavimo tinklas (toliau – SVDPT). Elektronine informacija keičiamasi per saugųjį HTTPS (angl. *Hypertext Transfer Protocol Secure*) duomenų perdavimo protokolą, žiniatinklio paslaugų metodu (XML formatu) arba

duomenų bazių užklausomis. Duomenys teikiami ir (ar) gaunami automatizuotomis priemonėmis tik pagal duomenų teikimo sutartyje nustatytas specifikacijas, duomenų perdavimo sąlygas ir tvarką.

40. Metodai, kuriais gali būti užtikrinamas saugus EIS elektroninės informacijos teikimas ir (ar) gavimas:

40.1. Iš duomenų gavėjų elektroninė informacija gaunama pagal teikimo sutartyse numatytas elektroninės informacijos perdavimo technologijas, jų šifravimo mechanizmus, specifikacijas ir kitas sąlygas.

40.2. Duomenų gavėjų prieigą prie EIS kontroliuoja kompiuterių tinklo užkarda.

40.3. Už EIS elektroninės informacijos teikimo ir gavimo sutartyse nurodomų kibernetinio saugumo reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

40.4. EIS elektroninei informacijai perduoti naudojamas SVDPT arba kitas šifruotas perdavimo kanalas, užtikrinantis saugų elektroninės informacijos perdavimą.

41. EIS išoriniai naudotojai naudojasi prieiga prie EIS per išorinį portalą. EIS išoriniams naudotojams prisijungimo laikas nėra ribojamas.

42. Pagrindiniai atsarginių EIS elektroninės informacijos kopijų (toliau – atsarginės kopijos) darymo ir atkūrimo reikalavimai:

42.1. Turi būti sudaromi EIS elektroninės informacijos, kurių atsarginės kopijos daromos, sąrašai.

42.2. EIS veiklos tęstinumui užtikrinti EIS duomenys yra periodiškai, bet ne rečiau kaip kas 24 valandas kopijuojami į rezervinių kopijų laikmenas ir laikmenos saugomos taip, kad, įvykus kibernetinio saugumo incidentui, visiškas EIS funkcionalumas ir veikla būtų atkurti per 8 valandas.

42.3. Detalus atsarginių kopijų ir archyvų darymas ir duomenų iš jų atkūrimas nustatomi Via Lietuva patvirtinta tvarka.

42.4. Atsarginėms kopijoms daryti turi būti naudojama speciali programinė įranga. Privalo būti visos saugomos elektroninės informacijos rezervinio kopijavimo funkcija. EIS administratorius privalo turėti galimybę inicijuoti elektroninės informacijos atkūrimo iš rezervinės kopijos procedūrą pasirinktinai iš turimų rezervinių kopijų sąrašo. Atkūrus elektroninę informaciją privalo būti užtikrintas ir išlaikytas elektroninės informacijos vientisumas ir integralumas.

42.5. EIS elektroninė informacija EIS naudotojams turi būti prieinama ne mažiau kaip 99,30 procento sistemos veikimo laiko per mėnesį.

42.6. Elektroninė informacija atsarginėse kopijose turi būti šifruota (šifravimo raktai turi būti saugomi atskirai nuo atsarginių kopijų).

42.7. Atsarginės kopijos yra daromos ir saugomos taip, kad jos nebūtų prieinamos tretiesiems asmenims, kurie neturi teisės su jomis dirbti.

42.8. Atsarginės kopijos turi būti laikomos atskirai nuo tarnybinių stočių. Už atsarginių kopijų darymą ir atkūrimą atsakingas EIS administratorius.

42.9. Atkūrimo iš atsarginių kopijų funkcija privalo būti išbandoma ne rečiau kaip kartą per metus. Testavimo eiga ir rezultatai įforminami kopijų darymo žurnale. Duomenų atkūrimo bandymą organizuoja kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.

43. Nustatomi duomenų naikinimo ir šalinimo reikalavimai:

43.1. Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinta visa joje esanti elektroninė informacija, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jeigu to padaryti neįmanoma (pvz., DVD laikmenos), duomenų laikmenos turi būti fiziškai sunaikinamos be galimybės atkurti duomenis.

43.2. Prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai.

43.3. Jeigu saugiems duomenų naikinimo ir šalinimo duomenų laikmenose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti sudaryta atitinkama paslaugų sutartis.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

44. Tvarkyti EIS duomenis gali asmenys, susipažinę su Reglamentu (ES) 2016/679, EIS nuostatais, EIS kibernetinio saugumo politikos dokumentais, informacinių sistemų kibernetinio saugumo politiką reglamentuojančiais teisės aktais.

45. EIS vidiniai naudotojai turi būti įgiję darbo kompiuteriu įgūdžių, mokėti tvarkyti EIS duomenis EIS nuostatuose nurodyta tvarka, išmanyti informacinių sistemų kibernetinio saugumo politiką reglamentuojančius teisės aktus. Tvarkyti EIS elektroninę informaciją gali tik EIS vidiniai naudotojai, pasirašę pasižadėjimą saugoti asmens duomenų paslaptį. Ši pareiga galioja perėjus dirbti į kitas pareigas arba pasibaigus darbo, sutartiniams ar kitiems santykiams.

46. Kibernetinio saugumo vadovas ir saugos įgaliotinis privalo išmanyti šiuolaikinių informacinių technologijų panaudojimo ypatumus, žinoti elektroninės informacijos saugumo užtikrinimo principus bei metodus, savo darbe vadovautis Kibernetinio saugumo įstatymu, Aprašu, Informacinių technologijų saugumo atitikties vertinimo metodika, EIS kibernetinio saugumo politikos dokumentais, standartų ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis kibernetinį saugumą, būti susipažinęs su esminiais EIS duomenų apsaugos reikalavimais. Kibernetinio saugumo vadovas ir saugos įgaliotinis privalo sugebėti prižiūrėti, kaip įgyvendinama kibernetinio saugumo politika. Kibernetinio saugumo vadovas ir saugos įgaliotinis kiekvienais metais privalo tobulinti kvalifikaciją kibernetinio saugumo srityje.

47. Saugos įgaliotiniu ir kibernetinio saugumo vadovu negali būti skiriamas asmuo, neatitinkantis Lietuvos Respublikos valstybės tarnybos įstatyme valstybės tarnautojams nustatytus nepriekaištingos reputacijos reikalavimus, taip pat turintis administracines nuobaudas už teisės aktų pažeidimus tinklų ir informacinių sistemų ir asmens duomenų tvarkymo ir privatumo apsaugos srityse, nuo kurios paskyrimo praėję mažiau kaip vieni metai.

48. EIS administratorius privalo gerai išmanyti kompiuterizuotos veiklos procesus, elektroninės informacijos apsaugos užtikrinimo metodus ir principus, žinoti tarnybinių stočių veikimo principus, būti susipažinęs su naudojamų duomenų bazių organizavimo principais, gebėti jas administruoti, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų bei kibernetinio saugumo incidentų diagnostiką ir šalinimą.

49. EIS vidiniai naudotojai, pastebėję EIS kibernetinio saugumo politikos pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias EIS saugumo užtikrinimo priemones, privalo nedelsdami apie tai pranešti kibernetinio saugumo vadovui, saugos įgaliotiniui, EIS administratoriui. Jeigu kibernetinio saugumo vadovas, saugos įgaliotinis nebuvo informuotas apie šiame punkte nurodytus pažeidimus, EIS administratorius informuoja kibernetinio saugumo vadovą ir saugos įgaliotinį apie šiuos pažeidimus.

50. EIS vidinių naudotojų ir EIS administratoriaus mokymai organizuojami ne rečiau kaip kartą per metus.

V SKYRIUS
EIS VIDINIŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

51. EIS vidinių naudotojų, EIS administratoriaus supažindinimą su EIS kibernetinio saugumo politikos dokumentais ar kitais kibernetinį saugumą reglamentuojančiais teisės aktais atlieka kibernetinio saugumo vadovas ar saugos įgaliotinis pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodymą.

52. EIS administratorių su EIS kibernetinio saugumo politikos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai supažindina kibernetinio saugumo vadovas ar saugos įgaliotinis per 10 darbo dienų nuo EIS administratoriaus paskyrimo.

53. EIS vidinius naudotojus su EIS kibernetinio saugumo politikos dokumentais ir teisės aktais, reglamentuojančiais kibernetinį saugumą, kibernetinio saugumo vadovas ar saugos įgaliotinis pasirašytinai supažindina prieš sukuriant EIS vidinio naudotojo prisijungimo duomenis.

54. Pakartotinai su EIS kibernetinio saugumo politikos dokumentais ir teisės aktais, reglamentuojančiais kibernetinį saugumą, kibernetinio saugumo vadovas ar saugos įgaliotinis pasirašytinai supažindina EIS vidinius naudotojus ir EIS administratorių kitą darbo dieną po EIS kibernetinio saugumo politikos dokumentų ir teisės aktų, reglamentuojančių kibernetinį saugumą, priėmimo, pakeitimo ar pripažinimo netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

55. Kibernetinio saugumo vadovas ar saugos įgaliotinis organizuoja EIS kibernetinio saugumo politikos dokumentų persvarstymą ne rečiau kaip kartą per metus. EIS kibernetinio saugumo politikos dokumentai turi būti persvarstomi atlikus rizikos analizę ar EIS atitikties vertinimą, pasikeitus kibernetinio saugumo politiką reglamentuojantiems teisės aktams, įvykus esminiams organizaciniams, technologiniams ar kitiems EIS pokyčiams, po įvykusio didelio kibernetinio incidento.

56. Kibernetinio saugumo vadovas, saugos įgaliotinis, Via Lietuva, EIS administratorius, EIS naudotojai ir kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai, pažeidę EIS kibernetinio saugumo politikos dokumentų ir kitų teisės aktų, reglamentuojančių kibernetinį saugumą, reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____