PATVIRTINTA
Akcinės bendrovės „Via Lietuva“ generalinio direktoriaus
2025 m. d. įsakymu Nr.

# VALSTYBINĖS IR VIETINĖS REIKŠMĖS KELIŲ TURTO VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

## I SKYRIUS
## BENDROSIOS NUOSTATOS

1. Valstybinės ir vietinės reikšmės kelių turto valdymo informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Valstybinės ir vietinės reikšmės kelių turto valdymo informacinės sistemos (toliau – KTVIS) kibernetinio saugumo politiką, kurios tikslas – nustatyti ir įgyvendinti organizacines, administracines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti KTVIS 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 apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme.

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

3.1. Valstybinės ir vietinės reikšmės kelių turto valdymo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės;

3.2. Valstybinės ir vietinės reikšmės kelių turto valdymo informacinės sistemos naudotojų administravimo taisyklės;

3.3. Valstybinės ir vietinės reikšmės kelių turto valdymo informacinės sistemos veiklos tęstinumo valdymo planas.

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

5. KTVIS kibernetinio saugumo užtikrinimo tikslai - sudaryti sąlygas saugiai automatizuotomis priemonėmis tvarkyti KTVIS elektroninę informaciją, užtikrinti KTVIS elektroninės informacijos patikimumą, konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterinės, programinės ir ryšių įrangos funkcionavimą.

6. KTVIS elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

6.1. KTVIS elektroninei informacijai tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

6.2. KTVIS elektroninės informacijos tvarkymo kontrolė;

6.3. saugaus darbo su KTVIS elektronine informacija kontrolė;

6.4. fizinė KTVIS elektroninės informacijos tvarkymo priemonių (tarnybinių stočių, informacijos perdavimo įrangos, programinės įrangos) ir patalpų apsauga;

6.5. KTVIS veiklos tęstinumas.

7. Saugos nuostatais privalo vadovautis:

7.1. Via Lietuva darbuotojai, dirbantys pagal darbo sutartis (toliau – KTVIS vidiniai naudotojai), kibernetinio saugumo vadovas, KTVIS saugos įgaliotinis (toliau – saugos įgaliotinis), KTVIS administratorius, KTVIS duomenų valdymo įgaliotinis (toliau – duomenų valdymo įgaliotinis), kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai;

7.2. Via Lietuva Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka išrinkto juridinio asmens ar asmenų (asmenų grupės), kuriems Valstybės informacinių išteklių valdymo

įstatymo 39 straipsnyje nustatytomis sąlygomis ir tvarka perduotos KTVIS ir (ar) jos infrastuktūros priežiūros funkcijos (toliau – KTVIS paslaugos teikėjas (-ai), darbuotojai, informacinių sistemų veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantys ir (ar) tvarkantys KTVIS elektroninę informaciją (toliau – KTVIS paslaugos teikėjo (-ų) darbuotojai);

7.3. kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai.

8. KTVIS valdytoja, duomenų valdytoja yra Via Lietuva.

9. KTVIS pagrindinė tvarkytoja, duomenų tvarkytoja - Via Lietuva, KTVIS tvarkytoja - paslaugos teikėjas (-ai).

10. KTVIS valdytojo, duomenų valdytojo funkcijos ir atsakomybė:

10.1. atsako už KTVIS kibernetinio saugumo politikos ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

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

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

10.4. atsižvelgdamas į kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitą, prireikus tvirtina nustatytų trūkumų šalinimo planą;

10.5. priima sprendimą dėl KTVIS 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 KTVIS kibernetinio saugumo politikos dokumentuose nustatytiems reikalavimams vertinimo (toliau – KTVIS atitikties vertinimas) atlikimo;

10.6. prireikus tvirtina KTVIS atitikties vertinimo metu identifikuotų neatitikčių šalinimo planą;

10.7. pagal kompetenciją atsako už KTVIS kibernetinį saugumą;

10.8. nagrinėja pasiūlymus dėl KTVIS kibernetinio saugumo tobulinimo ir priima dėl jų sprendimus;

10.9. paskiria saugos įgaliotinį, duomenų valdymo įgaliotinį, KTVIS administratorių ir kibernetinio saugumo vadovą;

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

11. Via Lietuvos, kaip KTVIS tvarkytojos ir duomenų tvarkytojos funkcijos ir atsakomybės:

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

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

11.3. pagal kompetenciją atsako už KTVIS elektroninės informacijos tvarkymo teisėtumą, užtikrina KTVIS komponentų veikimą, organizuoja KTVIS plėtrą, pakeitimų įdiegimą;

11.4. rūpinasi KTVIS elektroninės informacijos saugumu, užtikrina tinkamą KTVIS administravimą ir nepertraukiamą KTVIS veiklą;

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

12. Paslaugos teikėjo, kaip KTVIS tvarkytojo, funkcijos ir atsakomybės:

12.1. atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir kibernetinio saugumo reikalavimų atitiktį KTVIS kibernetinio saugumo politikos dokumentams;

12.2. teikia KTVIS valdytojui, duomenų valdytojui pasiūlymus dėl KTVIS plėtros, saugos ir funkcionalumo;

12.3. KTVIS paslaugos teikėjo vadovas paskiria administratorių, kuris nurodomas Via Lietuva ir KTVIS paslaugų teikimo sutartyje;

12.4. pagal kompetenciją atsako už KTVIS elektroninės informacijos tvarkymo teisėtumą, saugumą;

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

13. Kibernetinio saugumo vadovo ir saugos įgaliotinio funkcijos:

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

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

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

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

13.5. 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;

13.6. organizuoja KTVIS vidinių naudotojų mokymus kibernetinio saugumo klausimais;

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

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

15. Kibernetinio saugumo vadovas gali vykdyti saugos įgaliotinio funkcijas.

16. Via Lietuvos, kaip KTVIS administratoriaus (Via Lietuva ir paslaugos teikėjo) funkcijos ir atsakomybė:

16.1. registruoja išorinius ir vidinius KTVIS naudotojus, tvarko jų duomenis, prieigos teises ir leidžiamus veiksmus KTVIS;

16.2. atsako už KTVIS 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 KTVIS ir užtikrinama joje tvarkomos elektroninės informacijos sauga ir kibernetinis saugumas bei KTVIS komponentų sąranka) administravimą, KTVIS komponentų sąrankos aprašymo dokumentacijos parengimą ir atnaujinimą;

16.3. nustato KTVIS pažeidžiamas vietas, parenka joms kibernetinio saugumo priemones, vykdo kibernetinio saugumo reikalavimų atitikties stebėseną;

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

16.5. reaguoja į KTVIS kibernetinius incidentus, registruoja KTVIS 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;

16.6. užtikrina įdiegtą KTVIS sąveiką su kitomis informacinėmis sistemomis ir registrais;

16.7. atsako už KTVIS elektroninės informacijos atsarginių kopijų darymą, tinkamumą ir saugojimą;

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

16.9. konsultuoja KTVIS naudotojus;

16.10. sunaikina asmens duomenis KTVIS duomenų bazėje, pasibaigus asmens duomenų saugojimo terminui;

16.11. teikia kibernetinio saugumo vadovui ir (ar) saugos įgaliotiniui informaciją apie kibernetinį saugumą užtikrinančių pagrindinių komponentų būklę, kibernetinio saugumo politikos pažeidimus, nustatytas KTVIS pažeidžiamas vietas, pasiūlymus dėl KTVIS palaikymo, priežiūros ir kibernetinio saugumo;

16.12. dalyvauja atkuriant KTVIS elektroninę informaciją iš atsarginių KTVIS elektroninės informacijos kopijų;

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

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

16.15. pagal kompetenciją atsako už techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugų administravimą;

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

17. Via Lietuva turi paskirti darbuotoją, kontroliuojantį KTVIS paslaugos teikėjo darbą (toliau – paslaugos teikėjo administratorius).

18. Tvarkant KTVIS elektroninę informaciją ir užtikrinant jos kibernetinę saugą vadovaujamasi šiais teisės aktais:

18.1. Valstybės informacinių išteklių valdymo įstatymu;

18.2. 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);

18.3. Kibernetinio saugumo įstatymu;

18.4. Aprašu;

18.5. 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);

18.6. 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;

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

## II SKYRIUS
## ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

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

20. Pagrindiniai rizikos veiksniai, galintys turėti įtakos KTVIS kibernetiniam saugumui:

20.1. 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);

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

20.3. 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. KTVIS rizikos vertinimas atliekamas vadovaujantis šiomis nuostatomis:

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

21.2. 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.

21.3. sutartiniais pagrindais gali būti samdomi tretieji asmenys.

22. KTVIS rizikos vertinimo metu atliekamos veiklos:

22.1. KTVIS sudarančių informacinių išteklių inventorizacija;

22.2. įtakos KTVIS veiklai vertinimas;

22.3. grėsmės ir pažeidimų analizė;

22.4. liekamosios rizikos vertinimas.

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

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

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

26. 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.

27. Kibernetinių atakų imitavimas turi būti atliekamas šiais etapais:

27.1. 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;

27.2. 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;

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

27.4. 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.

28. Siekdamas užtikrinti KTVIS kibernetinio saugumo politikos dokumentų nuostatų įgyvendinimo kontrolę ne rečiau kaip kartą per metus kibernetinio saugumo vadovas ar saugos įgaliotinis organizuoja KTVIS 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.

29. Atliekant KTVIS atitikties vertinimą:

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

29.2. inventorizuojama KTVIS techninė ir programinė įranga;

29.3. peržiūrima KTVIS administratoriui, KTVIS naudotojams suteiktų teisių atitiktis jų atliekamoms funkcijoms;

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

29.5. įvertinamas pasirengimas užtikrinti KTVIS veiklos tęstinumą įvykus kibernetiniam incidentui.

30. Atlikus KTVIS atitikties vertinimą, parengiama KTVIS 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.

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

32. Elektroninės informacijos saugos priemonėms parinkti taikomi šie principai:

32.1. parenkamos priemonės, kurios leidžia užtikrinti patalpų saugą;

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

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

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

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

33. Elektroninės informacijos saugos priemonės turi garantuoti:

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

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

33.3. elektroninės informacijos saugą nuo jos pažeidimo esant Saugos nuostatų 20 punkte nurodytiems rizikos veiksniams.

34. 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 KTVIS.

## III SKYRIUS
## ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

35. Nustatomi šie KTVIS naudojamos programinės įrangos reikalavimai:

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

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

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

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

35.5. 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.

35.6. Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai.

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

36.1. KTVIS turi būti naudojama antivirusinė programinė įranga, skirta KTVIS apsaugoti nuo kenksmingos programinės įrangos.

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

36.3. KTVIS 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.

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

36.5. KDV esančios programinės įrangos, skirtos KTVIS 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.

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

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

36.8. KTVIS operacinės sistemos ir naudojami programinės įrangos gamintojų rekomenduojami atnaujinimai turi būti įdiegiami nedelsiant.

37. Metodai ir priemonės, kurie taikomi užtikrinant prieigą prie KTVIS:

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

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

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

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

37.5. Prieigą prie KTVIS suteikia, apriboja ir panaikina KTVIS administratorius.

37.6. Teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam KTVIS naudotojui.

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

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

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

37.10. Prisijungimo prie kompiuterių tinklo laikas ir trukmė nėra ribojami, KTVIS pasiekiama visą parą.

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

38.1. KTVIS turi būti naudojama tik legali programinė įranga.

38.2. Draudžiama diegti ir naudoti bet kokią programinę įrangą, keisti sistemos, kompiuterio ar programinės įrangos sistemų nustatymus. Programinę įrangą, reikalingą KTVIS vidinio naudotojo funkcijoms atlikti, KDV diegia, atnaujina, kontroliuoja ir prižiūri KTVIS administratorius. Kiti asmenys (paslaugų teikėjų specialistai) gali diegti programinę įrangą tik KTVIS administratoriaus prižiūrimi.

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

38.4. Tarnybinėse stotyse ir KTVIS 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.

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

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

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

38.8. KTVIS tarnybinėse stotyse negali būti įdiegta programinė įranga, kuri yra nesusijusi su KTVIS veikla.

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

39.1. Stacionariuosiuose ir nešiojamuosiuose kompiuteriuose KTVIS įjungimo metu turi būti identifikuojamas KTVIS vidinis naudotojas.

39.2. Stacionarieji ir nešiojamieji KTVIS 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 KTVIS elektroninė informacija.

39.3. KTVIS vidiniai naudotojai, darbinėms funkcijoms atlikti naudojantys nešiojamuosius kompiuterius, išnešdami juos iš Via Lietuva patalpų, norėdami KTVIS elektroninę informaciją perduoti kompiuterių tinklais ne savo darbo vietoje, turi naudoti duomenų šifravimą, papildomą KTVIS 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 KTVIS duomenų bazės prisijungimas ribojamas. Nešiojamuosiuose kompiuteriuose ar išorinėse kompiuterinėse laikmenose esantys duomenys turi būti šifruojami. KTVIS vidiniai naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

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

40.1. 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.

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

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

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

40.5. Naudojamos turinio filtravimo sistemos.

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

40.7. KTVIS žurnaliniuose įrašuose (angl. *logs*) turi būti fiksuojami šie duomenys:

40.7.1. įvykio data ir tikslus laikas,

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

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

40.7.4. įvykio aprašymas.

40.8. 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.

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

40.10. 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.

41. 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.

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

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

42.2. Duomenų gavėjų prieigą prie KTVIS kontroliuoja kompiuterių tinklo užkarda.

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

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

43. IS išoriniai naudotojai naudojasi prieiga prie KTVIS per išorinį portalą. KTVIS išoriniams naudotojams prisijungimo laikas nėra ribojamas.

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

44.1. Turi būti sudaromi KTVIS elektroninės informacijos, kurių atsarginės kopijos daromos, sąrašai.

44.2. KTVIS veiklos tęstinumui užtikrinti KTVIS 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 KTVIS funkcionalumas ir veikla būtų atkurti per 8 valandas.

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

44.4. Atsarginėms kopijoms daryti turi būti naudojama speciali programinė įranga. Privalo būti visos saugomos elektroninės informacijos rezervinio kopijavimo funkcija. KTVIS 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.

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

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

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

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

44.9. 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.

45. Nustatomi duomenų naikinimo ir šalinimo reikalavimai:

45.1. 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.

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

45.3. 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

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

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

48. 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, KTVIS kibernetinio saugumo politikos dokumentais, standartų ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis kibernetinį saugumą, būti susipažinęs su esminiais KTVIS 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.

49. 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.

50. KTVIS 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.

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

52. KTVIS vidinių naudotojų ir KTVIS administratoriaus mokymai organizuojami ne rečiau kaip kartą per metus.

## V SKYRIUS
## INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

53. KTVIS vidinių naudotojų, KTVIS administratoriaus supažindinimą su KTVIS 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.

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

55. KTVIS vidinius naudotojus su KTVIS kibernetinio saugumo politikos dokumentais ir teisės aktais, reglamentuojančiais kibernetinį saugumą, kibernetinio saugumo vadovas ar saugos

įgaliotinis pasirašytinai supažindina prieš sukuriant KTVIS vidinio naudotojo prisijungimo duomenis.

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

## VI SKYRIUS
## BAIGIAMOSIOS NUOSTATOS

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

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

_____