PATVIRTINTA
Lietuvos Respublikos susisiekimo ministro
2021 m. d. įsakymu Nr.
(Lietuvos Respublikos susisiekimo ministro
2012 m. rugsėjo 17 d. įsakymą Nr. 3-609
redakcija)

VIEŠOJO TRANSPORTO KELIONIŲ DUOMENŲ INFORMACINĖS SISTEMOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Viešojo transporto kelionių duomenų informacinės sistemos nuostatai (toliau – Nuostatai) reglamentuoja Viešojo transporto kelionių duomenų informacinės sistemos (toliau – IS „Vintra“) steigimo teisinį pagrindą, tikslus, uždavinius, pagrindines funkcijas, organizacinę, informacinę ir funkcinę struktūras, duomenų teikimo ir naudojimo, duomenų ir informacijos pakartotinio panaudojimo sąlygas ir tvarką, duomenų saugą, finansavimo, modernizavimo ir likvidavimo tvarką.

2. IS „Vintra“ steigimo teisinis pagrindas – Lietuvos Respublikos transporto veiklos pagrindų įstatymo 13^1 straipsnio 3 dalis.

3. Kompiuterizuojamą veiklos sritį reglamentuojantys teisės aktai, kuriais vadovaujantis kuriama ir tvarkoma IS „Vintra“:

3.1. Nacionalinė susisiekimo plėtros 2014–2022 metų programa, patvirtinta Lietuvos Respublikos Vyriausybės 2013 m. gruodžio 18 d. nutarimu Nr. 1253 „Dėl Nacionalinės susisiekimo plėtros 2014–2022 metų programos patvirtinimo“;

3.2. 2010 m. liepos 7 d. Europos Parlamento ir Tarybos direktyva 2010/40/ES dėl kelių transporto ir jo sąsajų su kitų rūšių transportu srities intelektinių transporto sistemų diegimo sistemos.

3.3. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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) (toliau – Reglamentas (ES) 2016/679);

3.4. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

3.5. Lietuvos Respublikos kibernetinio saugumo įstatymas;

3.6. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas 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“;

3.7. Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimas Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“;

3.8. Nuostatai ir kiti teisės aktai, reglamentuojantys saugų elektroninės informacijos tvarkymą, saugojimą ir sunaikinimą.

4. Šiuose nuostatuose vartojamos sąvokos:

4.1. **IS „Vintra“ paslaugų gavėjas** – fizinis ar juridinis asmuo, kuris naudoja IS „Vintra“, siekdamas gauti kelionės viešuoju transportu maršruto paieškos ir planavimo elektroninę paslaugą.

4.2. **Maršruto punktas** – geografinis taškas maršruto trasoje, žymintis tuo maršrutu vykstančio viešojo transporto sustojimo arba tvarkaraščio vietą.

4.3. **Transporto priemonės reisas** (toliau – reisas) – viešojo transporto priemonės vykimas iš viešojo transporto maršrute numatyto pradinio taško į galutinį maršruto tašką per iš anksto nustatytus maršruto punktus nustatytu važiavimo laiku.

4.4. **Transporto priemonės maršrutas** (toliau – maršrutas) – iš anksto nustatytas viešojo transporto priemonės vykimo iš tam tikros vietos iki numatytos vietos kelias, kuris kerta maršruto punktus.

4.5. Kitos Nuostatuose vartojamos sąvokos apibrėžtos Reglamente (ES) 2016/679, Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatyme, 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“ ir kituose teisės aktuose.

5. IS „Vintra“ tikslas – informacinių technologijų priemonėmis centralizuotai kaupti maršrutų, maršrutų punktų ir reisų duomenis ir vykdyti maršrutų skirtingomis viešojo transporto rūšimis planavimą Lietuvos Respublikoje.

6. Asmens duomenų tvarkymo IS „Vintra“ tikslas – identifikuoti ir autentifikuoti IS „Vintra“ naudojančius asmenis ir administruoti prieigos teises, fiksuoti jų atliktus veiksmus IS „Vintra“, identifikuoti savivaldybės administracijos darbuotojus bei savivaldybės įgalioto asmens atstovus.

7. IS „Vintra“ uždaviniai:

7.1. teikti elektroninę maršrutų skirtingomis viešojo transporto rūšimis planavimo Lietuvos Respublikoje paslaugą;

7.2. automatizuoti maršrutų, maršrutų punktų, reisų, viešojo transporto kelionių duomenų, tvarkaraščių, tarifų ir kitos susijusios informacijos kaupimą.

8. Pagrindinės IS „Vintra“ funkcijos:

8.1. kaupti, apdoroti, sisteminti maršrutų skirtingomis viešojo transporto rūšimis duomenis ir kitą susijusią informaciją;

8.2. formuoti ir atvaizduoti maršrutų skirtingomis viešojo transporto rūšimis duomenis ir informaciją pagal užklausas ir palyginti su kelionės asmeniniu automobiliu Lietuvos Respublikoje duomenimis;

8.3. vykdyti maršrutų punktų paiešką ir atvaizduoti maršrutų punktus žemėlapyje.

II SKYRIUS
IS „VINTRA“ ORGANIZACINĖ STRUKTŪRA

9. IS „Vintra“ valdytoja ir asmens duomenų valdytoja yra Lietuvos Respublikos susisiekimo ministerija.

10. IS „Vintra“ tvarkytojos ir asmens duomenų tvarkytojos yra:

10.1. Lietuvos transporto saugos administracija;

10.2. VĮ Lietuvos automobilių kelių direkcija.

11. IS „Vintra“ valdytojas:

11.1. vykdo Reglamente (ES) 2016/679 nustatytas duomenų valdytojo teises ir pareigas, taip pat atlieka Valstybės informacinių išteklių valdymo įstatymo nustatytas funkcijas, turi šiame įstatyme nurodytas teises ir pareigas;

11.2. organizuoja ir valdo finansinius išteklius, skirtus IS „Vintra“ veikimui užtikrinti;

11.3. rengia ir tvirtina su IS „Vintra“ veikimu, valdymu, IS „Vintra“ duomenų teikimu ir tvarkymu susijusius teisės aktus ir kitus dokumentus;

11.4. tvirtina IS „Vintra“ saugos reikalavimus ir koordinuoja, kaip jų laikomasi;

11.5. analizuoja teisines, finansines, metodologines ir organizacines IS „Vintra“ tvarkymo problemas ir priima sprendimus, kurių reikia IS „Vintra“ tvarkymui užtikrinti;

11.6. teikia informaciją apie IS „Vintra“ veiklą teisės aktų nustatyta tvarka.

12. IS „Vintra“ tvarkytojai atlieka Valstybės informacinių išteklių valdymo įstatymo 34 straipsnio 5 ir 6 dalyse nustatytas funkcijas, turi šiame įstatyme nurodytas teises ir pareigas.

13. Asmens duomenų tvarkytojai vykdo Reglamente (ES) 2016/679 nustatytas duomenų tvarkytojo teises ir pareigas. VĮ Lietuvos automobilių kelių direkcija asmens duomenų valdytojo įgaliota įgyvendina duomenų subjektų teises, numatytas Reglamento (ES) 2016/679 III skyriuje. Detalios Reglamento (ES) 2016/679 28 straipsnio 3 dalyje nustatytos sąlygos nurodomos asmens duomenų tvarkymo sutartyje, sudarytoje tarp IS „Vintra“ valdytojo ir IS „Vintra“ tvarkytojų.

14. Lietuvos transporto saugos administracija be Nuostatų 12 ir 13 punktuose numatytų teisių ir pareigų turi šias teises ir pareigas:

14.1. tvarkyti tolimojo ir tarptautinio reguliariojo susisiekimo autobusais maršrutų duomenis;

14.2. bendradarbiauti su duomenų teikėjais dėl duomenų teikimo ir atnaujinimo;

14.3. formuoti ir teikti teisės aktų nustatyta tvarka su Lietuvos transporto saugos administracijos veikla susijusias ataskaitas, o su IS „Vintra“ veikimu susijusias ataskaitas ir atrinktus duomenis pagal kompetenciją teikti IS „Vintra“ valdytojui ir VĮ Lietuvos automobilių kelių direkcijai;

14.4. pagal kompetenciją tvarkyti IS „Vintra“ duomenis ir atsakyti už jų saugą.

15. VĮ Lietuvos automobilių kelių direkcija be Nuostatų 12 ir 13 punktuose numatytų teisių ir pareigų turi šias teises ir pareigas:

15.1. atlikti IS „Vintra“ veikimo, techninės ir programinės įrangos priežiūrą, tolimesnę plėtrą, planuoti atnaujinimus ir pajėgumus;

15.2. užtikrinti IS „Vintra“ veiklos tęstinumą ir veiklos atkūrimą, šalinti sutrikimus;

15.3. sudaryti duomenų teikimo sutartis;

15.4. sukurti automatinių duomenų mainų su duomenų teikėjais ir duomenų gavėjais sąsajas ir vykdyti jų priežiūrą;

15.5. registruoti IS „Vintra“ naudotojus sistemoje, tvarkyti jų duomenis, prieigos teises ir klasifikatorius, analizuoti IS „Vintra“ procesus ir IS „Vintra“ naudotojų veiksmus;

15.6. pagal kompetenciją rengti su IS „Vintra“ veikimu susijusias ataskaitas ir teikti jas IS „Vintra“ valdytojui ir Lietuvos transporto saugos administracijai;

15.7. organizuoti IS „Vintra“ naudotojų mokymus dirbti su IS „Vintra“;

15.8. gauti duomenis iš kitų informacinių sistemų, teikti informaciją registrams ir kitoms informacinėms sistemoms;

15.9. konsultuoti su IS „Vintra“ veikimu susijusiais klausimais;

15.10. pagal kompetenciją tvarkyti IS „Vintra“ duomenis ir atsakyti už jų saugą.

16. IS „Vintra“ duomenų teikėjai:

16.1. Lietuvos transporto saugos administracija (Kelių transporto veiklos valstybės informacinė sistema „Keltra“ (toliau – IS „Keltra“);

16.2. VĮ Lietuvos automobilių kelių direkcija (Valstybinės reikšmės kelių eismo informacinė sistema (toliau – EIS), Valstybinės reikšmės kelių informacinė sistema (toliau – LAKIS);

16.3. AB „Lietuvos geležinkeliai“;

16.4. VĮ Lietuvos oro uostai;

16.5. Vilniaus miesto savivaldybės administracija;

16.6. Kauno miesto savivaldybės administracija;

16.7. Alytaus miesto savivaldybės administracija;

16.8. Druskininkų savivaldybės administracija;

16.9. Klaipėdos miesto savivaldybės administracija;

16.10. kitos Lietuvos savivaldybių administracijos ir (ar) jų įsteigtos įmonės, tvirtinančios viešojo transporto maršrutus;

16.11. jūrų uostai;

16.12. kiti vežėjai.

17. Informacinę sistemą naudojantys asmenys yra IS „Vintra“ paslaugų gavėjai ir turi teisę:

17.1. gauti viešojo transporto kelionių duomenis (tvarkaraščius, tarifus ir kitą susijusią informaciją) ir elektroninę maršrutų skirtingomis viešojo transporto rūšimis planavimo Lietuvos Respublikoje paslaugą;

17.2. naudoti viešojo transporto kelionių duomenis, kiek tai leidžia šie nuostatai, Viešojo transporto kelionių duomenų informacinės sistemos duomenų saugos nuostatai ir kiti saugos politikos įgyvendinimo dokumentai.

III SKYRIUS
IS „VINTRA“ INFORMACINĖ STRUKTŪRA

18. Duomenų bazėje tvarkomi duomenys:

18.1. maršruto duomenys (maršruto numeris, transporto rūšis, maršruto tipas, maršruto zona, maršruto pavadinimas, maršruto galinių punktų duomenys, maršruto leidimo būsena ir numeris, maršruto galiojimo terminas, maršruto punktų ir jų eiliškumo duomenys, maršruto aprašomieji duomenys);

18.2. reiso duomenys (maršruto numeris, reiso numeris, vežėjo identifikatorius, transporto priemonės tipas, reiso paslaugų duomenys, reiso kryptis, reiso galiojimo datos, reiso dažnumas, reiso aprašomieji duomenys);

18.3. maršruto punkto duomenys (maršruto punkto identifikatorius, maršruto punkto pavadinimas, maršruto punkto erdviniai duomenys, gatvės ar kelio duomenys, savivaldybės duomenys, tarifų zonos duomenys, maršruto punkto interneto puslapio adresas, maršruto punkto priklausymo kitam maršruto punktui ar maršruto punktų grupei duomenys, maršruto punkto aprašomieji duomenys);

18.4. tvarkaraščio duomenys (atvykimo laikas, išvykimo laikas, keleivių galimų veiksmų duomenys);

18.5. kelionių dienų grupių duomenys (kelionių dienų grupės pavadinimas, grupės dienų datos, grupės savaitės dienos, dienų grupės galiojimo datos, grupės išimčių datos);

18.6. transporto priemonių geografinės padėties duomenys (maršruto numeris, reiso numeris, transporto priemonės identifikatorius, transporto priemonės geografinės koordinatės, greičio ir atstumų duomenys, transporto priemonės padėties maršruto atžvilgiu duomenys);

18.7. tarifų ir kainoraščių duomenys;

18.8. savivaldybių duomenys (savivaldybės administracijos kodas, savivaldybės administracijos pavadinimas, savivaldybės administracijos adresas, savivaldybės administracijos kontaktiniai duomenys (telefono numeris, elektroninio pašto adresas, interneto svetainė, kiti kontaktiniai duomenys (darbuotojo vardas (vardai), pavardė (pavardės), pareigos, telefono numeris)), savivaldybės įgalioto asmens atstovų duomenys (vardas (vardai), pavardė (pavardės), pareigos, telefono numeris);

18.9. vežėjų duomenys (vežėjo kodas, vežėjo pavadinimas, vežėjo adresas, vežėjo telefono numeris);

18.10. geležinkelių transporto infrastruktūros erdviniai ir kiti duomenys (geležinkelio kelių duomenys, sankryžų, susikirtimų ir jų priklausinių duomenys, maršruto punktų duomenys, stočių duomenys);

18.11. IS „Vintra“ naudotojų duomenys (vardas (vardai) ir pavardė (pavardės), pareigos, institucijos, kuriai atstovauja asmuo, pavadinimas, identifikatorius, slaptažodis).

19. Iš duomenų teikėjų gaunami duomenys:

19.1. iš IS „Keltra“ gaunami (ne kaupiami) duomenys:

19.1.1. informacija apie leidimo vežti maršrutu būseną, numerį ir leidimo galiojimo terminą;

19.1.2. vežėjų duomenys;

19.2. iš EIS gaunami (ne kaupiami) duomenys:

19.2.1. kelių ir gatvių erdviniai duomenys;

19.2.2. duomenys apie eismo apribojimus ir sutrikimus;

19.2.3. duomenys apie eismo sąlygas (eismo intensyvumą, vidutinį greitį kelio ruožuose, kelionės laiko skaičiavimo duomenys);

19.2.4. kelionės automobiliu Lietuvos Respublikoje maršrutų duomenys;

19.2.5. kiti su eismo informacija susiję duomenys;

19.3. iš LAKIS gaunami (ne kaupiami) duomenys:

19.3.1. kelių infrastruktūros aprašomieji ir erdviniai duomenys;

19.3.2. maršruto punktų duomenys.

20. Iš šių Nuostatų 16.3 papunktyje nurodyto duomenų teikėjo gaunami duomenys nurodyti šių Nuostatų 18.4, 18.5 ir 18.10 papunkčiuose.

21. Iš šių Nuostatų 16.4 ir 16.11 papunkčiuose nurodytų duomenų teikėjų gaunami duomenys nurodyti šių Nuostatų 18.4 ir 18.9 papunkčiuose.

22. Iš šių Nuostatų 16.5–16.10 papunkčiuose nurodytų duomenų teikėjų gaunami duomenys nurodyti šių Nuostatų 18.4–18.9 papunkčiuose.

23. Iš šių Nuostatų 16.12 papunktyje nurodyto duomenų teikėjo gaunami duomenys nurodyti šių Nuostatų 18.1, 18.2 ir 18.4–18.9 papunkčiuose.

IV SKYRIUS
IS „VINTRA“ FUNKCINĖ STRUKTŪRA

24. IS „Vintra“ funkcinę struktūrą sudaro šie komponentai:

24.1. maršruto viešinimo (elektroninių paslaugų) komponentas (interneto svetainė, nešiojamųjų įrenginių ir kitų viešinimo priemonių sąsajos), kurio funkcijos:

24.1.1. formuoti maršrutų paieškos ir peržiūros užklausas;

24.1.2. ieškoti ir atvaizduoti žemėlapyje informaciją pagal pateiktas užklausas;

24.1.3. formuoti kiekvieno maršruto, reisų ir tvarkaraščių sąrašus;

24.1.4. formuoti maršruto punktų atvaizdavimą žemėlapyje, artimiausio maršruto punkto paiešką pagal IS „Vintra“ paslaugų gavėjo nurodytą adresą;

24.1.5. atvaizduoti maršrutų, reisų ir tvarkaraščių ir realaus laiko transporto priemonių atvykimo grafikus konkrečiame maršruto punkte;

24.1.6. formuoti optimalaus (alternatyvaus) maršruto paiešką ir atvaizduoti žemėlapyje;

24.1.7. formuoti kelionės viešuoju transportu su kelionės asmeniniu automobiliu duomenų palyginimo ataskaitas;

24.1.8. formuoti ir teikti pranešimus apie reisų pakeitimus, atšaukimus ir kitas būsenas, susieti pranešimus su atitinkamais maršrutais ar reisais;

24.1.9. apskaičiuoti ir pateikti kelionės kainas;

24.2. maršruto duomenų tvarkymo komponentas, kurio funkcijos:

24.2.1. surinkti, sisteminti ir teikti informaciją apie maršruto punktus (su galimybe naudoti interaktyvius žemėlapius);

24.2.2. surinkti, sisteminti ir teikti informaciją apie vietinio (miesto ir priemiestinio) ir tolimojo reguliariojo susisiekimo reisų tvarkaraščius (bazinių ir konkrečių datų);

24.2.3. surinkti, sisteminti ir teikti informaciją apie tarptautinių maršrutų tvarkaraščius;

24.2.4. surinkti, sisteminti ir teikti informaciją, susijusią su maršrutais ir maršruto punktais, (paslaugų tipų, maršruto punktų grupių ir kitų atributų);

24.2.5. surinkti, sisteminti ir teikti informaciją apie tarifus ir kainoraščius;

24.3. valdymo komponentas, kurio funkcijos:

24.3.1. sisteminti ir taikyti IS „Vintra“ parametrus;

24.3.2. registruoti IS „Vintra“ naudotojus ir konfigūruoti jų teises;

24.3.3. formuoti ir teikti IS „Vintra“ naudotojų veiksmų registracijos audito žurnalus ir veiksmų ataskaitas;

24.3.4. formuoti naudotojų veiksmų ataskaitas;

24.3.5. identifikuoti IS „Vintra“ naudotojus;

24.3.6. taikyti duomenų analizės įrankius;

24.4. duomenų mainų komponentas, kurio funkcijos:

24.4.1. konfigūruoti IS „Vintra“ sąsajas su kitomis informacinėmis sistemomis;

24.4.2. importuoti ir eksportuoti duomenis.

V SKYRIUS
IS „VINTRA“ DUOMENŲ TEIKIMAS IR NAUDOJIMAS

25. IS „Vintra“ duomenys yra vieši, išskyrus asmens duomenis, ir teikiami institucijoms, kitiems juridiniams ir fiziniams asmenims, jeigu Lietuvos Respublikos įstatymai ir (ar) Europos Sąjungos teisės aktai nenustato kitaip.

26. IS „Vintra“ tvarkomi asmens duomenys teikiami Nuostatų 30 ir 31 punktuose nustatyta tvarka, laikantis Reglamento (ES) 2016/679.

27. IS „Vintra“ duomenys gali būti teikiami raštu, žodžiu ir (arba) elektroninių ryšių priemonėmis, taip pat automatiniu būdu, naudojant informacinių sistemų sąsajas.

28. IS „Vintra“ tvarkomi duomenys duomenų gavėjams teikiami tokio turinio ir formos, kurių nereikia papildomai apdoroti.

29. Jeigu Nuostatų nustatyta tvarka teikiamų duomenų turinys ir forma neatitinka duomenų gavėjų poreikių, IS „Vintra“ tvarkytojai pagal kompetenciją, esant galimybei, įvertinę laiko ir žmogiškųjų išteklių ir finansinius kaštus bei jų atsiperkamumą, sukuria reikalingas papildomas priemones.

30. IS „Vintra“ duomenys, įskaitant ir asmens duomenis, IS „Vintra“ duomenų gavėjams vienkartinio teikimo atveju teikiami pagal duomenų gavėjo prašymą, kuriame nurodomas IS „Vintra“ duomenų, įskaitant asmens duomenis, naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, prašomų pateikti IS „Vintra“ duomenų, įskaitant asmens duomenis, apimtis ir formatas, gavimo būdas. Vienkartinio teikimo atveju IS „Vintra“ duomenys teikiami ne vėliau nei per 7 (septynias) kalendorines dienas.

31. Daugkartinio teikimo atveju ir (ar) pakartotinio panaudojimo tikslais IS „Vintra“ duomenys, įskaitant asmens duomenis, teikiami pagal duomenų teikimo sutartį, kurioje turi būti nurodyta IS „Vintra“ duomenų, įskaitant asmens duomenis, naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka, teikiamų IS „Vintra“ duomenų, įskaitant asmens duomenis, apimtis, formatas, gavimo būdas ir teikimo terminai.

32. IS „Vintra“ duomenys teikiami neatlygintinai, jeigu dėl to neatsiranda nepagrįstai didelių išlaidų arba jeigu Lietuvos Respublikos įstatymai ar Europos Sąjungos teisės aktai nenustato kitaip.

33. Duomenų naudojimo sąlygos ir tvarka nustatytos Lietuvos Respublikos susisiekimo ministro 2014 m. gegužės 21 d. įsakymu Nr. 3-210-(E) „Dėl Viešojo transporto kelionių duomenų kaupimo tvarkos aprašo patvirtinimo“.

34. Sudaryti sutarčių dėl išimtinių teisių teikti IS „Vintra“ duomenis ir (arba) juos naudoti nenumatoma.

35. IS „Vintra“ duomenis, įskaitant asmens duomenis, duomenų gavėjas gali naudoti tik tokiam tikslui, tokios apimties ir tokiu būdu, kokie buvo nurodyti duomenų gavėjo prašyme arba duomenų teikimo sutartyje.

36. Fizinių asmenų asmens duomenys naudojami vadovaujantis Reglamentu (ES) 2016/679.

37. Asmens duomenys nėra skelbiami viešai.

38. IS „Vintra“ duomenys, įskaitant asmens duomenis, Europos Sąjungos valstybių narių ir (arba) Europos ekonominės erdvės valstybių, trečiųjų šalių fiziniams ir juridiniams asmenims, juridinio asmens statuso neturintiems subjektams, jų filialams ir atstovybėms teikiami Reglamento (ES) 2016/679, Valstybės informacinių išteklių valdymo įstatymo bei Nuostatų 30 ir 31 punktų nustatyta tvarka.

39. IS „Vintra“ duomenų gavėjas, IS „Vintra“ duomenų teikėjas, registro ar kitos valstybės informacinės sistemos tvarkytojas, kiti asmenys, pastebėję netikslumus, turi teisę reikalauti ištaisyti netikslius duomenis, ištrinti neteisingus duomenis, papildyti neišsamius duomenis arba apriboti IS

„Vintra“ duomenų tvarkymą. IS „Vintra“ duomenų gavėjas, IS „Vintra“ duomenų teikėjas, registro ar kitos valstybės informacinės sistemos tvarkytojas, kiti asmenys, pastebėję netikslumus, nedelsdami informuoja IS „Vintra“ duomenų tvarkytoją pagal kompetenciją apie pastebėtus netikslumus rašytiniu prašymu, pateiktu asmeniškai, paštu arba elektroniniu paštu. Gavusi reikalavimą dėl netikslių, neteisingų, neišsamių duomenų (toliau – netikslūs duomenys), IS „Vintra“ duomenų tvarkytojas pagal kompetenciją privalo nedelsdamas, bet ne vėliau kaip per 5 darbo dienas nuo reikalavimo ir jame nurodytus faktus patvirtinančių dokumentų gavimo, patikrinti IS „Vintra“ duomenų tikslumą ir, jei reikia, ištaisyti netikslius duomenis. Pranešimas apie netikslių duomenų ištaisymą arba apie motyvuotą atsisakymą tai padaryti nedelsiant (ne vėliau kaip per vieną darbo dieną) siunčiamas asmeniui, pranešusiam apie netikslius duomenis, tuo pačiu būdu, kuriuo buvo gautas reikalavimas. Ištaisiusi netikslius duomenis, IS „Vintra“ duomenų tvarkytojas pagal kompetenciją per vieną darbo dieną nuo jų ištaisymo apie tai praneša IS „Vintra“ duomenų gavėjams, kuriems perduoti netikslūs duomenys.

40. IS „Vintra“ duomenų teikimas ribojamas Valstybės informacinių išteklių valdymo įstatymo 27 straipsnio 7 dalyje numatytais atvejais.

41. Kai atsisakoma teikti IS „Vintra“ duomenis, asmeniui, pateikusiam prašymą juos gauti, raštu arba elektroninių ryšių priemonėmis pranešama apie priimtą motyvuotą sprendimą atsisakyti tenkinti jo prašymą ir suteikiama informacija apie tokio sprendimo apskundimo tvarką. Atsisakymas teikti IS „Vintra“ duomenis gali būti skundžiamas Lietuvos Respublikos teisės aktų nustatyta tvarka.

VI SKYRIUS
IS „VINTRA“ DUOMENŲ SAUGA

42. Tvarkant IS „Vintra“ duomenis, įskaitant asmens duomenis, turi būti įgyvendintos duomenų saugos organizacinės ir techninės priemonės, skirtos IS „Vintra“ duomenų, įskaitant asmens duomenų, konfidencialumui, vientisumui ir autentiškumui užtikrinti ir apsaugoti nuo netyčinio ar neteisėto IS „Vintra“ duomenų, įskaitant asmens duomenų, sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų. Minėtos priemonės turi užtikrinti tokio lygio saugumą, kuris atitiktų saugotinų IS „Vintra“ duomenų pobūdį, aprėptį, kontekstą ir tikslus, taip pat IS „Vintra“ duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus asmenų teisėms ir laisvėms ir jų tvarkymo riziką. IS „Vintra“ duomenų saugaus tvarkymo reikalavimų įgyvendinimas užtikrinamas vadovaujantis:

42.1. Reglamentu (ES) 2016/679;

42.2. Valstybės informacinių išteklių valdymo įstatymu;

42.3. Kibernetinio saugumo įstatymu;

42.4. 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“;

42.5. Lietuvos Respublikos krašto apsaugos ministro patvirtintais Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais;

42.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“;

42.7. Lietuvos standartais LST ISO/IEC 27001, ISO/IEC 27002 ir kitais Lietuvos ir tarptautiniais „Informacinės technologijos. Saugumo metodai“ grupės standartais, apibūdinančiais saugų informacinės sistemos duomenų tvarkymą;

42.8. IS „Vintra“ duomenų saugos nuostatais ir kitais IS „Vintra“ duomenų saugos politikos įgyvendinimo dokumentais, kurie rengiami, derinami ir tvirtinami Lietuvos Respublikos Vyriausybės nustatyta tvarka.

43. IS „Vintra“ valdytojas ir tvarkytojai pagal kompetenciją atsako už IS „Vintra“ duomenų, įskaitant asmens duomenų, ir elektroninės informacijos saugą. Pagal kompetenciją IS „Vintra“ tvarkytojai privalo įgyvendinti tinkamas organizacines ir technines priemones, tarp jų ir skirtas asmens duomenims apsaugoti nuo netyčinio ar neteisėto IS „Vintra“ duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų.

44. Asmenys, tvarkantys asmens duomenis, privalo saugoti asmens duomenų paslaptį, jeigu šie asmens duomenys neskirti skelbti viešai. Ši pareiga galioja jiems pasitraukus iš valstybės tarnybos, perėjus dirbti į kitas pareigas arba pasibaigus jų darbo, sutartiniams ar kitiems santykiams.

45. Duomenys, išskyrus asmens duomenis, saugomi IS „Vintra“ duomenų bazėje dvejus metus, po šio termino duomenys, išskyrus asmens duomenis, automatiniu būdu perkeliami į archyvą, kuriame saugomi nuolat. Gavus atnaujintus IS „Vintra“ naudojančių asmenų, savivaldybės administracijos darbuotojų bei savivaldybės įgalioto asmens atstovų asmens duomenis, IS „Vintra“ tvarkomi asmens duomenys nedelsiant sunaikinami.

VII SKYRIUS
IS „VINTRA“ FINANSAVIMAS

46. IS „Vintra“ kūrimas, diegimas ir priežiūra finansuojami Lietuvos Respublikos valstybės biudžeto lėšomis.

47. IS „Vintra“ tobulinimas ir plėtra finansuojami Lietuvos Respublikos valstybės biudžeto lėšomis.

VIII SKYRIUS
IS „VINTRA“ MODERNIZAVIMAS IR LIKVIDAVIMAS

48. IS „Vintra“ modernizuojama arba likviduojama Valstybės informacinių išteklių valdymo įstatymo ir Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, nustatyta tvarka.

49. Likviduojant IS „Vintra“, duomenys perduodami kitai valstybės informacinei sistemai, valstybės archyvui ar sunaikinami Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka arba sunaikinami.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

50. Detali duomenų subjekto teisių įgyvendinimo tvarka nustatyta Lietuvos Respublikos susisiekimo ministro patvirtintame Duomenų subjektų teisių įgyvendinimo tvarkant asmens duomenis Lietuvos Respublikos susisiekimo ministerijos valdomuose registruose ir valstybės informacinėse sistemose tvarkos apraše.

51. Duomenų teikėjai atsako už teikiamų duomenų, įskaitant asmens duomenų, tikslumą ir teisingumą.

52. Už šių nuostatų nesilaikymą IS „Vintra“ valdytojas, IS „Vintra“ tvarkytojai ir duomenų naudotojai atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

PATVIRTINTA
Lietuvos Respublikos susisiekimo ministro
2021 m. d. įsakymu Nr.
(Lietuvos Respublikos susisiekimo ministro
2012 m. rugsėjo 17 d. įsakymą Nr. 3-609
redakcija)

VIEŠOJO TRANSPORTO KELIONIŲ DUOMENŲ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Viešojo transporto kelionių duomenų informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Viešojo transporto kelionių duomenų informacinės sistemos (toliau – IS „Vintra“) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – saugos politika), kurių tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti IS „Vintra“ 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, 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 – Aprašas).

3. IS „Vintra“ saugos politiką nustato šie susisiekimo ministro patvirtinti teisės aktai (toliau – saugos politikos įgyvendinamieji dokumentai):

3.1. Viešojo transporto kelionių duomenų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės;

3.2. Viešojo transporto kelionių duomenų informacinės sistemos naudotojų administravimo taisyklės;

3.3. Viešojo transporto kelionių duomenų informacinės sistemos veiklos tęstinumo valdymo planas.

3.4. Saugos nuostatai kartu su saugos politikos įgyvendinamaisiais dokumentais sudaro saugos dokumentus.

4. IS „Vintra“ elektroninės informacijos saugos ir kibernetinio saugumo (toliau – IS „Vintra“ elektroninės informacijos sauga) užtikrinimo tikslai – sudaryti sąlygas saugiai automatizuotomis priemonėmis tvarkyti IS „Vintra“ elektroninę informaciją, užtikrinti IS „Vintra“ elektroninės informacijos patikimumą, konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterinės, programinės ir ryšių įrangos funkcionavimą.

5. IS „Vintra“ elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. IS „Vintra“ elektroninei informacijai tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

5.2. IS „Vintra“ elektroninės informacijos tvarkymo kontrolė;

5.3. saugaus darbo su IS „Vintra“ elektronine informacija kontrolė;

5.4. fizinė IS „Vintra“ elektroninės informacijos tvarkymo priemonių (tarnybinių stočių, informacijos perdavimo įrangos, programinės įrangos) ir patalpų apsauga;

5.5. IS „Vintra“ veiklos tęstinumas.

6. Saugos nuostatais privalo vadovautis IS „Vintra“ saugos įgaliotinis (toliau – saugos įgaliotinis), IS „Vintra“ administratorius (-iai) (toliau – administratorius), asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą (toliau – kibernetinio saugumo vadovas), IS „Vintra“ duomenų valdymo įgaliotinis, IS „Vintra“ naudotojai ir kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai.

7. IS „Vintra“ valdytoja yra Lietuvos Respublikos susisiekimo ministerija (Gedimino pr. 17, 01505 Vilnius).

8. IS „Vintra“ tvarkytojai yra:

8.1. VĮ Lietuvos automobilių kelių direkcija (toliau – Direkcija) (J. Basanavičiaus g. 36/2, LT-03109 Vilnius);

8.2. Lietuvos transporto saugos administracija (toliau – Administracija) (Švitrigailos g. 42, LT-03209 Vilnius).

9. IS „Vintra“ valdytojo funkcijos ir atsakomybė:

9.1. atsako už IS „Vintra“ saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

9.2. tvirtina IS „Vintra“ saugos dokumentus, prižiūri ir kontroliuoja, kad IS „Vintra“ būtų tvarkoma vadovaujantis šiais dokumentais, IS „Vintra“ nuostatais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą;

9.3. nagrinėja IS „Vintra“ tvarkytojų pasiūlymus dėl IS „Vintra“ elektroninės informacijos saugos tobulinimo ir priima dėl jų sprendimus;

9.4. atsižvelgdamas į rizikos įvertinimo ataskaitą, prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą;

9.5. priima sprendimą dėl IS „Vintra“ informacinių technologijų saugos atitikties vertinimo atlikimo;

9.6. prireikus tvirtina IS „Vintra“ informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

9.7. atsako už IS „Vintra“ pokyčių ir plėtros įgyvendinimą;

9.8. pagal kompetenciją atsako už IS „Vintra“ elektroninės informacijos saugą;

9.9. paveda IS „Vintra“ tvarkytojai – Direkcijai paskirti saugos įgaliotinį, IS „Vintra“ duomenų valdymo įgaliotinį, administratorių, kibernetinio saugumo vadovą;

9.10. vykdo kitas Saugos nuostatų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą, nustatytas funkcijas.

10. Direkcijos, kaip IS „Vintra“ tvarkytojos, funkcijos ir atsakomybė:

10.1. pagal kompetenciją atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir IS „Vintra“ saugos reikalavimų atitiktį Saugos nuostatams ir saugos politikos įgyvendinamiesiems dokumentams;

10.2. pagal kompetenciją teikia pasiūlymus IS „Vintra“ valdytojui ir Administracijai dėl IS „Vintra“ eksploatavimo ir tobulinimo darbų, saugos ir funkcionalumo;

10.3. IS „Vintra“ tvarkytojo vadovas įsakymu paskiria saugos įgaliotinį, IS „Vintra“ duomenų valdymo įgaliotinį, administratorių ir kibernetinio saugumo vadovą;

10.4. rengia IS „Vintra“ saugos dokumentus ir teikia juos tvirtinti IS „Vintra“ valdytojo vadovui;

10.5. užtikrina eksploataciją ir veikimo priežiūrą, įgyvendina pokyčius ir tolesnę plėtrą, prižiūri techninę ir programinę įrangą, planuoja atnaujinimus ir pajėgumus;

10.6. rūpinasi IS „Vintra“ duomenų saugumu, užtikrina tinkamą IS „Vintra“ administravimą ir nepertraukiamą IS „Vintra“ veiklą ir veiklos atkūrimą, šalina sutrikimus;

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

10.8. gauna duomenis iš kitų valstybės informacinių sistemų, teikia informaciją registrams ir kitoms valstybėms informacinėms sistemoms;

10.9. analizuoja IS „Vintra“ procesus ir IS „Vintra“ naudotojų veiksmus;

10.10. atlieka kitas IS „Vintra“ valdytojo pavestas, Saugos nuostatuose bei teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą, priskirtas funkcijas.

11. Administracijos, kaip IS „Vintra“ tvarkytojos, funkcijos:

11.1. pagal kompetenciją atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir IS „Vintra“ saugos reikalavimų atitiktį Saugos nuostatams ir saugos politikos įgyvendinamiesiems dokumentams;

11.2. pagal kompetenciją teikia IS „Vintra“ valdytojui ir Direkcijai pasiūlymus dėl IS „Vintra“ eksploatavimo ir tobulinimo darbų;

11.3. pagal kompetenciją registruoja IS „Vintra“ naudotojus sistemoje, tvarko jų duomenis, prieigos teises ir klasifikatorius, analizuoja IS „Vintra“ procesus ir IS „Vintra“ naudotojų veiksmus;

11.4. atlieka kitas IS „Vintra“ valdytojo pavestas, Saugos nuostatuose bei teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą, priskirtas funkcijas.

12. Saugos įgaliotinio funkcijos ir atsakomybė:

12.1. teikia pasiūlymus IS „Vintra“ tvarkytojo – Direkcijos vadovui dėl:

12.1.1. administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo;

12.1.2. IS „Vintra“ informacinių technologijų saugos atitikties vertinimo atlikimo Aprašo 43 punkte nurodytoje krašto apsaugos ministro tvirtinamoje Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka;

12.1.3. saugos dokumentų priėmimo, keitimo ar panaikinimo;

12.2. atsako už tinkamą IS „Vintra“ saugos reikalavimų ir funkcijų vykdymą;

12.3. ne rečiau kaip kartą per metus, jeigu kiti teisės aktai nenustato kitaip, organizuoja IS „Vintra“ rizikos įvertinimą, prireikus – neeilinį IS „Vintra“ rizikos įvertinimą ir IS „Vintra“ informacinių technologijų saugos atitikties vertinimą;

12.4. informuoja IS „Vintra“ tvarkytojo – Direkcijos vadovą apie IS „Vintra“ saugos problemas;

12.5. teikia administratoriui ir IS „Vintra“ naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

12.6. koordinuoja elektroninės informacijos saugos incidentų, įvykusių IS „Vintra“, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos sauga, išskyrus atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

12.7. užtikrina IS „Vintra“ saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

12.8. pasirašytinai supažindina administratorių ir IS „Vintra“ naudotojus su saugos dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, ir atsakomybe už šių dokumentų reikalavimų nesilaikymą;

12.9. periodiškai inicijuoja administratoriaus ir IS „Vintra“ naudotojų mokymus elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas (teminių seminarų rengimas, atmintinės priimtiems naujiems darbuotojams ir pan.);

12.10. atlieka kitas IS „Vintra“ tvarkytojo – Direkcijos vadovo pavestas užduotis, saugos dokumentuose ir kituose saugos reikalavimus nustatančiuose teisės aktuose jam priskirtas funkcijas.

13. Saugos įgaliotinis negali atlikti administratoriaus funkcijų.

14. Kibernetinio saugumo vadovas atlieka šias funkcijas:

14.1. koordinuoja kibernetinių incidentų tyrimą, bendradarbiauja su kompetentingomis institucijomis, tiriančiomis kibernetinius incidentus;

14.2. atlieka kitas Saugos nuostatuose, saugos politikos įgyvendinamuosiuose dokumentuose nurodytas ir kituose teisės aktuose, reglamentuojančiuose kibernetinio saugumą, jam priskirtas funkcijas.

15. Saugos įgaliotinis ir kibernetinio saugumo vadovas gali būti tas pats asmuo.

16. Administratoriaus funkcijos ir atsakomybė:

16.1. atlieka IS „Vintra“ naudotojams priskirtų funkcijų ir suteiktų teisių atitikties vertinimą, administruoja šias teises;

16.2. rengia ir tikrina IS „Vintra“ sudarančių komponentų sąranką, teikia saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;

16.3. vykdo IS „Vintra“ sudarančių dalių (kompiuterių, operacinės sistemos, duomenų bazių valdymo sistemos, taikomųjų programų sistemos, ugniasienės, įsilaužimo aptikimo sistemos, duomenų perdavimo tinklų ir kt.) priežiūrą, kontroliuoja ir atsako už IS „Vintra“ ir ją sudarančių komponentų nepertraukiamą veikimą;

16.4. nuolat peržiūri ir atnaujina IS „Vintra“ sąrankos aprašus ir rodo esamą IS „Vintra“ sąrankos būklę;

16.5. pagal kompetenciją reaguoja į elektroninės informacijos saugos ir kibernetinius incidentus (toliau – saugos incidentai), registruoja juos ir informuoja saugos įgaliotinį apie nustatytus saugos politikos pažeidimus, teikia pasiūlymus dėl minėtų incidentų šalinimo, taip pat informuoja saugos įgaliotinį apie nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

16.6. nustato IS „Vintra“ pažeidžiamas vietas ir informuoja apie jas saugos įgaliotinį;

16.7. užtikrina, kad būtų laikomasi saugos dokumentų ir kitų teisės aktų reikalavimų;

16.8. vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su IS „Vintra“ duomenų saugos užtikrinimu;

16.9. įregistruoja ir išregistruoja IS „Vintra“ naudotojus, atsako už prieigos prie IS „Vintra“ teisių nustatymą;

16.10. įdiegia programinės įrangos atnaujinimus, nustato automatinio atnaujinimo procedūras;

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

16.12. tikrina pranešimus apie serverių operacinių sistemų ir duomenų bazių valdymo sistemų klaidas ir imasi būtinų priemonių, kad būtų išvengta galimų gedimų;

16.13. jeigu administruojamas nutolęs serveris ir nustatomas sutrikimas, kurio negalima pašalinti nuotolinėmis priemonėmis, susisiekia su asmenimis, įgaliotais atlikti techninę priežiūrą nutolusioje vietovėje, ir prižiūri sutrikimų šalinimo eigą;

16.14. užtikrina visų prisijungimo vardų, slaptažodžių apsaugą;

16.15. teikia IS „Vintra“ tvarkytojo – Direkcijos vadovui ir saugos įgaliotiniui pasiūlymus dėl IS „Vintra“ kūrimo, funkcionalumo užtikrinimo, priežiūros ir duomenų saugos klausimų;

16.16. daro atsargines IS „Vintra“ elektroninės informacijos kopijas;

16.17. atsako už IS „Vintra“ elektroninės informacijos atsarginių kopijų darymą, tinkamumą ir saugojimą;

16.18. dalyvauja atkuriant IS „Vintra“ elektroninę informaciją iš elektroninės informacijos atsarginių kopijų;

16.19. perkelia IS „Vintra“ elektroninę informaciją į IS „Vintra“ duomenų bazės archyvą ir tvarko elektroninės informacijos perkėlimo įrašų žurnalą;

16.20. tvarko IS „Vintra“ eksploatacijos žurnalą;

16.21. dalyvauja svarstant teikimus dėl IS „Vintra“ pokyčių projektavimo, konstravimo ir diegimo, dalyvauja aptariant IS „Vintra“ plėtrą ir vykdant IS „Vintra“ plėtros specifikavimo, projektavimo, konstravimo ir diegimo etapų darbus;

16.22. organizuoja IS „Vintra“ konfigūravimą, įskaitant saugų IS „Vintra“ įjungimą ir išjungimą;

16.23. atlieka kitas IS „Vintra“ tvarkytojo – Direkcijos vadovo pavestas užduotis ir kitas Saugos nuostatuose ir kituose saugos dokumentuose administratoriui priskirtas funkcijas.

17. Teisės aktų, kuriais vadovaujamasi tvarkant IS „Vintra“ elektroninę informaciją ir užtikrinant jų saugumą, sąrašas:

17.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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) (toliau – Reglamentas (ES) 2016/679);

17.2. Valstybės informacinių išteklių valdymo įstatymas;

17.3. Kibernetinio saugumo įstatymas;

17.4. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas 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“;

17.5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo aprašas);

17.6. Lietuvos Respublikos krašto apsaugos ministro tvirtinami Techniniai informacinių sistemų elektroninės informacijos saugos reikalavimai;

17.7. Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001, Lietuvos ir tarptautiniai „Informacinės technologijos. Saugumo metodai“ grupės standartai, nustatantys saugų informacinės sistemos duomenų tvarkymą;

17.8. IS „Vintra“ nuostatai;

17.9. Saugos nuostatai;

17.10. saugos politikos įgyvendinamieji dokumentai.

II SKYRIUS
IS „VINTRA“ ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

18. IS „Vintra“ tvarkoma elektroninė informacija priskiriama svarbios elektroninės informacijos kategorijai vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Gairių aprašas), 8 punktu.

19. IS „Vintra“ pagal joje tvarkomos informacijos svarbą priskiriama antrajai kategorijai, vadovaujantis Gairių aprašo 12.2 papunkčiu.

20. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacinės technologijos. Saugumo metodai“ grupės standartus, gerosios praktikos pavyzdžiais (COBIT ar kitais), kasmet arba po esminių organizacinių ar sisteminių pokyčių organizuoja IS „Vintra“ rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą. IS „Vintra“ rizikos įvertinimas atliekamas pagal kokybinį rizikos vertinimo metodą. Kartu su pagrindiniu IS „Vintra“ rizikos įvertinimu organizuojamas ir atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos IS „Vintra“ kibernetiniam saugumui, vertinimas pagal Kibernetinio saugumo aprašą. Rizikos įvertinimui atlikti sutartiniais pagrindais gali būti samdomi tretieji asmenys. IS „Vintra“ tvarkytojo – Direkcijos rašytiniu pavedimu IS „Vintra“ rizikos įvertinimą gali atlikti pats saugos įgaliotinis.

21. IS „Vintra“ rizikos įvertinimo rezultatai pateikiami rizikos įvertinimo ataskaitoje ir ji pateikiama IS „Vintra“ tvarkytojų vadovams. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. IS „Vintra“ rizikos įvertinimo ataskaitą rengia arba, jei vertinimą atlieka trečioji šalis, dalyvauja rengiant saugos įgaliotinis. Svarbiausi rizikos veiksniai:

21.1. 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 ir kita);

21.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis IS „Vintra“ elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

21.3. 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.

22. Rizikos įvertinimo metu atliekamos veiklos:

22.1. IS „Vintra“ sudarančių informacinių išteklių inventorizacija;

22.2. įtakos IS „Vintra“ veiklai vertinimas;

22.3. grėsmės ir pažeidimų analizė;

22.4. liekamosios rizikos vertinimas.

23. 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. Kibernetinių atakų imitavimas turi būti atliekamas šiais etapais:

23.1. 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.

23.2. 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.

23.3. Kibernetinių atakų imitavimo etapas. Atliekami pažeidžiamumų nustatymo plane numatyti testai.

23.4. 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 ir pateikiamos rekomendacijos jam pašalinti. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos įvertinimu. Jeigu nustatoma incidentų valdymo ir šalinimo, taip pat organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinami veiklos tęstinumo planai.

24. Atsižvelgdamas į rizikos įvertinimo ataskaitą, IS „Vintra“ valdytojas prireikus tvirtina IS „Vintra“ rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis IS „Vintra“ rizikos valdymo priemonėms įgyvendinti.

25. Atsižvelgiant į kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitą, rengiamas nustatytų trūkumų šalinimo planas, kuriame atsižvelgiant į kibernetinių atakų imitavimo metu nustatytus trūkumus, IS „Vintra“ valdytojo vadovui teikiami pasiūlymai dėl kibernetinį saugumą reglamentuojančių teisės aktų ar kitų IS „Vintra“ valdytojo vadovo patvirtintų dokumentų pakeitimo, kibernetinio saugumo būklės gerinimo ir papildomų kibernetinio saugumo priemonių įsigijimo. Nustatytų trūkumų šalinimo planą tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato IS „Vintra“ valdytojo vadovas.

26. Pagrindiniai IS „Vintra“ elektroninės informacijos saugos priemonių parinkimo principai yra šie:

26.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

26.2. informacijos saugos priemonės diegimo kaina turi atitikti saugomos informacijos vertę;

26.3. esant galimybei, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

27. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas, kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitos ir nustatytų trūkumų šalinimo plano kopijas IS „Vintra“ valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

28. Siekdamas užtikrinti Saugos nuostatų ir kituose saugos politikos įgyvendinamuosiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, saugos įgaliotinis ne rečiau kaip kartą per metus (jeigu teisės aktai nenustato kitaip) atlieka IS „Vintra“ informacinių technologijų saugos atitikties vertinimą, vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“.

29. Atliekant IS „Vintra“ informacinių technologijų saugos atitikties vertinimą:

29.1. įvertinama esamos IS „Vintra“ elektroninės informacijos saugos situacijos atitiktis IS „Vintra“ saugos dokumentams ir kitiems elektroninės informacijos saugą reglamentuojantiems teisės aktams;

29.2. inventorizuojama IS „Vintra“ techninė ir programinė įranga;

29.3. peržiūrima administratoriui ir IS „Vintra“ naudotojams suteiktų teisių atitiktis jų atliekamoms funkcijoms;

29.4. duomenų saugos požiūriu patikrinama IS „Vintra“ techninė ir programinė įranga: visos tarnybinės stotys ir ne mažiau kaip 10 procentų atsitiktinai parinktų IS „Vintra“ naudotojų darbo vietų;

29.5. įvertinamas pasirengimas užtikrinti IS „Vintra“ veiklos tęstinumą įvykus saugos incidentui.

30. Atlikus IS „Vintra“ informacinių technologijų saugos atitikties vertinimą, parengiama informacinių technologijų saugos atitikties vertinimo ataskaita ir pateikiama IS „Vintra“ tvarkytojų vadovams, taip pat prireikus parengiamas pastebėtų trūkumų šalinimo planas. IS „Vintra“ valdytojo vadovas patvirtina šį planą, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus.

31. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas IS „Vintra“ valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

32. Prireikus saugos įgaliotinis gali organizuoti neeilinį IS „Vintra“ informacinių technologijų saugos atitikties vertinimą.

33. Neeilinis IS „Vintra“ informacinių technologijų saugos atitikties vertinimas atliekamas:

33.1. įvykus IS „Vintra“ techninės ar programinės įrangos pokyčiams, kurie gali turėti įtakos IS „Vintra“ veikimui;

33.2. paaiškėjus naujoms tendencijoms informacinių technologijų saugos srityje, dėl kurių kiltų grėsmė IS „Vintra“ techninei, programinei įrangai ar IS „Vintra“ tvarkomai elektroninei informacijai;

33.3. po saugos incidento, kurio metu buvo sutrikdyta IS „Vintra“ veikla, sugadinta ar prarasta IS „Vintra“ elektroninė informacija.

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 IS „Vintra“.

35. IS „Vintra“ pokyčius gali inicijuoti saugos įgaliotinis ar administratorius, o įgyvendina administratorius.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

36. Nustatomi šie IS „Vintra“ naudojamos programinės įrangos reikalavimai:

36.1. IS „Vintra“ naudojama programinė įranga turi atitikti programinės įrangos saugos gerąją praktiką, kuriant programinę įrangą taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras, standartus.

36.2. Specifiniai saugos reikalavimai turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.

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

36.4. Programinės įrangos kūrimo, testavimo ir verifikacijos etapai turi vykti atsižvelgiant į pagrindinius saugos reikalavimus.

36.5. 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.

36.6. Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai.

37. Metodai ir priemonės, kurie taikomi užtikrinant prieigą prie IS „Vintra“:

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

37.2. IS „Vintra“ priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą administratoriaus klasifikatorių, kuriuo naudojantis nebūtų galima atlikti IS „Vintra“ naudotojo funkcijų.

37.3. IS „Vintra“ naudotojas turi būti IS „Vintra“ unikaliai identifikuojamas – IS „Vintra“ naudotojas turi patvirtinti savo tapatybę slaptažodžiu, IS „Vintra“ naudotojui suteiktas pirminis slaptažodis turi būti pakeistas pirmo prisijungimo metu.

37.4. IS „Vintra“ turi registruoti paskutinį IS „Vintra“ elektroninės informacijos pakeitimą atlikusį IS „Vintra“ naudotoją ir pakeitimo laiką.

37.5. Prieigą prie IS „Vintra“ suteikia, apriboja ir panaikina administratorius.

37.6. Teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam darbuotojui.

37.7. Patalpose, kuriose yra IS „Vintra“ duomenų centras, turi būti įrengti ir prie pastato signalizacijos ir apsaugos tarnybų prijungti gaisro ir įsilaužimo davikliai.

37.8. Duomenų centro patalpose turi būti įrengta stebėjimo sistema su įrašymo funkcija.

37.9. IS „Vintra“ turi būti prieinama ne mažiau kaip 96 proc. paros laiko.

38. Programinės įrangos, skirtos IS „Vintra“ ir kompiuterizuotoms darbo vietoms (toliau – KDV) apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos:

38.1. IS „Vintra“ turi būti naudojama antivirusinė programinė įranga, skirta IS „Vintra“ apsaugoti nuo kenksmingos programinės įrangos.

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

38.3. IS „Vintra“ 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.

38.4. IS „Vintra“ programinė įranga turi būti apsaugota nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS)*, dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP*) interneto svetainėje www.owasp.org;

38.5. Atsiradus požymių, kad KDV yra kenksmingų programų, turi būti patikrinami visi KDV standieji diskai, naudojama programinė įranga, skirta IS „Vintra“ ir KDV apsaugoti nuo kenksmingos programinės įrangos.

38.6. KDV esančios programinės įrangos, skirtos IS „Vintra“ 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.

38.7. Programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

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

38.9. Turi būti operatyviai ne vėliau kaip per 5 (penkias) darbo dienas nuo programinės įrangos paketo išleidimo dienos įdiegiamos IS „Vintra“ operacinės sistemos ir naudojami programinės įrangos gamintojų rekomenduojami atnaujinimai.

38.10. IS „Vintra“ turi būti naudojama tik licencijuota programinė įranga.

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

39.1. IS „Vintra“ naudojama tik legali programinė įranga.

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

39.3. Diegti ir naudoti programinę įrangą, nesusijusią su IS „Vintra“ valdytojo ar tvarkytojų veikla ar IS „Vintra“ naudotojo atliekamomis funkcijomis (žaidimų, bylų siuntimo, internetinių pokalbių programas ir kt.), draudžiama.

39.4. Programinė įranga yra nuolat atnaujinama laikantis gamintojo reikalavimų.

39.5. IS „Vintra“ tarnybinėse stotyse negali būti įdiegta programinė įranga, kuri yra nesusijusi su IS „Vintra“ veikla.

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

39.7. Už programinės įrangos tinkamą naudojimą pagal kompetenciją atsako tarnybinių stočių ir kompiuterizuotų darbo vietų administratoriai.

40. Leistinos kompiuterių (ypač nešiojamų) naudojimo ribos ir metodai, kuriais užtikrinamas saugus IS „Vintra“ duomenų teikimas ir (ar) gavimas:

40.1. IS „Vintra“ naudotojai naudojasi prieiga prie IS „Vintra“ per išorinį portalą; prisijungimo laikas nėra ribojamas.

40.2. Prie IS „Vintra“ prisijungiama nuotoliniu būdu naudojant interneto naršyklę (*https* protokolą).

40.3. IS „Vintra“ naudotojui teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma, kai IS „Vintra“ naudotojas atostogauja, vykdomas IS „Vintra“ naudotojo veiklos tyrimas ir pan. Pasibaigus tarnybos (darbo), sutartiniams ar kitiems santykiams, IS „Vintra“ naudotojo teisė naudotis IS „Vintra“ turi būti panaikinta.

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

40.5. IS „Vintra“ naudotojui 15 min. neatliekant jokių veiksmų, IS „Vintra“ turi užsirakinti, kad toliau naudotis IS „Vintra“ būtų galima tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus.

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

41.1. Turi būti naudojama programinė įranga, leidžianti atlikti IS „Vintra“ naudojamų kompiuterių tinklų stebėseną ir užtikrinanti šių tinklų saugos prevencines priemones.

41.2. Techninis nuotolinio prisijungimo sprendimas turi užtikrinti ne žemesnį nei vidiniam prisijungimui naudojamą saugumo lygį, t. y. turi būti naudojamos Saugos nuostatuose minimos priemonės ir duomenų šifravimas naudojantis virtualiu privačiu tinklu (angl. *virtual private network* – VPN).

41.3. IS „Vintra“ naudotojams, kuriems atliekant tiesiogines pareigas būtina prisijungti iš nutolusios darbo vietos, gali būti suteikiama nuotolinio prisijungimo prie IS „Vintra“ galimybė.

41.4. Kompiuterinis tinklas, prie kurio prijungtos IS „Vintra“ tarnybinės stotys ir IS „Vintra“ naudotojų kompiuteriai, nuo viešojo interneto turi būti atskirtas ugniasienėmis ir įsilaužimų aptikimo ir prevencijos įranga, už kurios administravimą ir priežiūrą atsakingas administratorius.

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

41.6. Naudojamos turinio filtravimo sistemos.

42. Kompiuterių (įskaitant nešiojamuosius) naudojimo reikalavimai:

42.1. Stacionarūs ir nešiojamieji IS „Vintra“ naudotojų kompiuteriai turi būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai. Iš kompiuterių, kurie perduodami remontui ar techninei priežiūrai, turi būti pašalinta visa riboto naudojimo IS „Vintra“ elektroninė informacija.

42.2. Visiems IS „Vintra“ naudotojų kompiuteriams turi būti naudojamos papildomos saugos priemonės, kuriomis patvirtinama kompiuterio naudotojo tapatybė.

42.3. IS „Vintra“ naudotojai, darbinėms funkcijoms atlikti naudojantys nešiojamuosius kompiuterius, išnešdami juos iš IS „Vintra“ tvarkytojų patalpų, norėdami IS „Vintra“ duomenis perduoti kompiuterių tinklais ne savo darbo vietoje, turi IS „Vintra“ duomenis perduoti saugiu šifruotu duomenų perdavimo kanalu *(VPN)*, turi naudoti papildomą naudotojo tapatybės patvirtinimą, rakinimo įrenginį. Nešiojamojo kompiuterio pagrindinė įvesties ir išvesties sistema (BIOS) turi būti apsaugota slaptažodžiu ir nurodytas kietasis diskas kaip pirminis paleidimo įrenginys. Iš išorės prie IS „Vintra“ duomenų bazės prisijungimas ribojamas. Nešiojamuosiuose kompiuteriuose ar išorinėse kompiuterinėse laikmenose esantys duomenys turi būti šifruojami. IS „Vintra“ naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

43. Užtikrinant saugų elektroninės informacijos teikimą kitoms valstybės institucijoms ir (ar) gavimą iš jų, naudojamas šifruotas virtualus privatus tinklas (*VPN*) arba Saugus valstybinis duomenų perdavimo tinklas (toliau – SVDPT). Elektronine informacija keičiamasi per saugųjį HTTP (angl. *Hypertext Transfer Protocol Secure*) duomenų perdavimo protokolą (HTTPS) 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.

44. Metodai, kuriais gali būti užtikrinamas saugus IS „Vintra“ elektroninės informacijos teikimas ir (ar) gavimas:

44.1. IS „Vintra“ elektroninė informacija perduodama automatiniu būdu (naudojant TCP/IP protokolą) realiuoju laiku arba asinchroniniu režimu pagal IS „Vintra“ duomenų teikimo ir gavimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka.

44.2. Už IS „Vintra“ elektroninės informacijos teikimo ir gavimo sutartyse nurodomų saugos reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas saugos įgaliotinis.

44.3. IS „Vintra“ elektroninei informacijai perduoti naudojamas SVDPT arba kitas šifruotas perdavimo kanalas, užtikrinantis saugų elektroninės informacijos perdavimą.

44.4. Už saugų IS „Vintra“ kompiuterių tinklų veikimą pagal kompetenciją atsako IS „Vintra“ tvarkytojų kompiuterių tinklų administratoriai.

44.5. Duomenų gavėjų prieigą prie IS „Vintra“ kontroliuoja kompiuterių tinklo užkarda.

45. Pagrindiniai atsarginių IS „Vintra“ elektroninės informacijos kopijų (toliau – atsarginės duomenų kopijos) darymo ir atkūrimo reikalavimai:

45.1. Turi būti sudaromi IS „Vintra“ duomenų, kurių kopijos daromos, sąrašai.

45.2. Atsarginėms duomenų kopijoms daryti turi būti naudojama speciali programinė įranga.

45.3. Atsarginės duomenų kopijos turi būti daromos automatiškai kartą per parą.

45.4. Duomenys į duomenų archyvą perkeliami automatiškai, pasibaigus duomenų saugojimo IS „Vintra“ laikui.

45.5. 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.

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

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

45.8. Atsarginės duomenų kopijos turi būti laikomos atskiroje (nuo pagrindinių duomenų) patalpoje ir saugomos užrakintoje nedegioje spintoje. Už atsarginių duomenų kopijų darymą bei atkūrimą, archyvų kūrimą atsakingas administratorius.

45.9. Atkūrimo iš atsarginių duomenų kopijų funkcija privalo būti išbandoma ne rečiau kaip kartą per metus. Testavimo eiga ir rezultatai įforminami kopijų darymo žurnale. Duomenų atkūrimo bandymą organizuoja saugos įgaliotinis.

45.10. Atsarginės duomenų kopijos ir archyvai turi būti daromi ir duomenys iš atsarginių duomenų kopijų atkuriami vadovaujantis Direkcijos patvirtinta tvarka.

46. Nustatomi duomenų naikinimo ir šalinimo reikalavimai:

46.1. 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.

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

46.3. 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

47. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus ir metodus, rizikų valdymą, kartą per metus tobulinti kvalifikaciją elektroninės informacijos saugos srityje ir savo darbe vadovautis Reglamentu (ES) 2016/679, saugos dokumentais, Aprašu, Informacinių technologijų saugos atitikties vertinimo metodika ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais elektroninės informacijos saugą, taip pat būti susipažinęs su esminiais IS „Vintra“ elektroninės informacijos saugos reikalavimais. Saugos įgaliotinis privalo sugebėti prižiūrėti, kaip įgyvendinama saugos politika.

48. Kibernetinio saugumo vadovas privalo išmanyti kibernetinio saugumo užtikrinimo principus, tobulinti kvalifikaciją kibernetinio saugumo srityje ir savo darbe vadovautis Saugos nuostatais ir saugos politikos įgyvendinamaisiais dokumentais, Lietuvos Respublikos ir Europos Sąjungos teisės aktais, standartais, reglamentuojančiais kibernetinį saugumą.

49. Saugos įgaliotiniu ir kibernetinio saugumo vadovu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą galiojančią administracinę nuobaudą už neteisėtą asmens duomenų

tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

50. Administratorius privalo išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugumą, būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą bei saugą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų bei saugos incidentų diagnostiką ir šalinimą.

51. Visi IS „Vintra“ naudotojai privalo turėti darbo kompiuteriu įgūdžių.

52. IS „Vintra“ naudotojai privalo rūpintis tvarkomų duomenų saugumu. Visi IS „Vintra“ naudotojai turi būti pasirašytinai susipažinę su Reglamentu (ES) 2016/679, Saugos nuostatais ir saugos politikos įgyvendinamaisiais dokumentais. Tvarkyti IS „Vintra“ elektroninę informaciją gali tik IS „Vintra“ naudotojai, pasirašę pasižadėjimą saugoti asmens duomenų paslaptį ir susipažinę su atsakomybe už Reglamento (ES) 2016/679, saugos dokumentų nuostatų pažeidimus. Ši pareiga galioja ir pasitraukus iš valstybės tarnybos, perėjus dirbti į kitas pareigas arba pasibaigus darbo, sutartiniams ar kitiems santykiams.

53. IS „Vintra“ naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias IS „Vintra“ saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti saugos įgaliotiniui, o jam nesant – administratoriui. Jeigu saugos įgaliotinis nebuvo informuotas apie šiame punkte nurodytus pažeidimus, administratorius informuoja saugos įgaliotinį apie šiuos pažeidimus.

54. IS „Vintra“ naudotojų mokymai organizuojami taip, kaip numatyta Saugos nuostatų 12.9 papunktyje, ne rečiau kaip kartą per metus.

V SKYRIUS
IS „VINTRA“ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

55. Už IS „Vintra“ naudotojų ir administratoriaus supažindinimą su saugos dokumentais ir atsakomybe, kylančia dėl jų pažeidimo, atsakingas saugos įgaliotinis.

56. IS „Vintra“ naudotojus su saugos dokumentais ir teisės aktais, reglamentuojančiais IS „Vintra“ elektroninės informacijos saugą, saugos įgaliotinis pasirašytinai supažindina prieš sukuriant IS „Vintra“ naudotojo prisijungimo duomenis.

57. Administratorių su Saugos nuostatais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą, supažindina saugos įgaliotinis per 10 darbo dienų nuo administratoriaus paskyrimo, o su saugos politikos įgyvendinamaisiais dokumentais – per 10 darbo dienų nuo šių dokumentų patvirtinimo.

58. Administratorius, IS „Vintra“ naudotojai turi būti nuolat informuojami apie saugos problemas (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.).

59. Pakartotinai su saugos dokumentais ir teisės aktais, reglamentuojančiais IS „Vintra“ elektroninės informacijos saugą, saugos įgaliotinis pasirašytinai supažindina IS „Vintra“ naudotojus ir administratorių kitą darbo dieną po saugos dokumentų ir teisės aktų, reglamentuojančių IS „Vintra“ elektroninės informacijos saugą, priėmimo (išdėstymo nauja redakcija), pakeitimo ar pripažinimo netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

60. Saugos įgaliotinis organizuoja saugos dokumentų peržiūrą ne rečiau kaip kartą per metus ir prireikus atnaujina. Saugos dokumentai taip pat turi būti peržiūrimi ir prireikus atnaujinami

atlikus rizikos vertinimą ar informacinių technologijų saugos atitikties vertinimą, pasikeitus saugos politiką reglamentuojantiems teisės aktams, įvykus esminiams organizaciniams, technologiniams ar kitiems IS „Vintra“ pokyčiams, po įvykusio kibernetinio incidento.

61. Saugos įgaliotinis, administratorius, kibernetinio saugumo vadovas, IS „Vintra“ naudotojai ir kiti subjektai, kuriems taikomi Saugos nuostatų reikalavimai, pažeidę saugos dokumentų ir kitų teisės aktų, reglamentuojančių saugų elektroninės informacijos tvarkymą, reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2021 m. d. raštu Nr.