NACIONALINIO BENDRŲJŲ FUNKCIJŲ CENTRO DIREKTORIUS

ĮSAKYMAS
DĖL INFORMACINĖS SISTEMOS „E. SĄSKAITA“ NUOSTATŲ IR INFORMACINĖS SISTEMOS „E.SĄSKAITA“ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2019 m. rugpjūčio 26 d. Nr. V-316
Vilnius

Vadovaudamasis Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“ ir Lietuvos Respublikos finansų ministro 2019 m. liepos 11 d. įsakymo Nr. 1K-215 „Dėl finansų ministro 2012 m. rugsėjo 6 d. įsakymo Nr. 1K-297 „Dėl Informacinės sistemos „E. sąskaita“ nuostatų patvirtinimo“ pakeitimo“ 2 punktu,

t v i r t i n u pridedamus:

1. Informacinės sistemos „E. sąskaita“ nuostatus.
2. Informacinės sistemos „E. sąskaita“ duomenų saugos nuostatus.

Direktorius Antanas Matusa

PATVIRTINTA
Nacionalinio bendrųjų funkcijų centro
direktoriaus 2019 m. rugpjūčio 26 d. įsakymu
Nr. V-316

INFORMACINĖS SISTEMOS „E. SĄSKAITA“ NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacinės sistemos „E. sąskaita“ nuostatai (toliau – Nuostatai) reglamentuoja valstybės informacinės sistemos „E. sąskaita“ (toliau – informacinė sistema) paskirtį, uždavinius, funkcijas ir tikslą, asmens duomenų tvarkymo informacinėje sistemoje tikslą, nustato informacinės sistemos valdytoją, tvarkytoją, jų teises ir pareigas, duomenų teikėjus, gavėjus, informacinės sistemos organizacinę, informacinę ir funkcinę struktūras, duomenų teikimo, naudojimo, finansavimo, modernizavimo ir likvidavimo tvarką, duomenų saugos reikalavimus.

2. Nuostatuose vartojamos sąvokos:

2.1. **Informacinės sistemos paslaugų gavėjas** (toliau – paslaugų gavėjas) – fizinis arba juridinis asmuo, turintis teisę jungtis prie informacinės sistemos ir pateikti, gauti elektronines sąskaitas už prekes, paslaugas ir darbus (toliau – e. sąskaitos), patikrinti jų duomenis ar apmokėjimo būseną ar kitą jam prieinamą informaciją.

2.2. Kitos Nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos pridėtinės vertės mokesčio įstatyme, Lietuvos Respublikos viešųjų pirkimų įstatyme, 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (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) (OL 2016 L 119, p. 1) (toliau – Reglamentas (ES) 2016/679), Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“ (toliau – Aprašas), 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“, vartojamas sąvokas.

3. Informacinės sistemos steigimo pagrindas – Nacionalinio bendrųjų funkcijų centro nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2018 m. vasario 7 d. nutarimu Nr. 125 „Dėl biudžetinės įstaigos Nacionalinio bendrųjų funkcijų centro įsteigimo ir jo nuostatų patvirtinimo“, 9.1.2, 9.1.8 ir 9.1.9 papunkčiai.

4. Informacinės sistemos veiklą reglamentuojantys teisės aktai:

4.1. Lietuvos Respublikos pridėtinės vertės mokesčio įstatymas;

4.2. Lietuvos Respublikos buhalterinės apskaitos įstatymas;

4.3. Lietuvos Respublikos viešųjų pirkimų įstatymas;

4.4. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

4.5. Lietuvos Respublikos teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatymas;

4.6. Lietuvos Respublikos kibernetinio saugumo įstatymas;

4.7. Aprašas;

4.8. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, Saugos dokumentų turinio gairių aprašas ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtinti 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“;

4.9. Lietuvos Respublikos Vyriausybės 2002 m. gegužės 29 d. nutarimas Nr. 780 „Dėl Mokesčiams apskaičiuoti naudojamų apskaitos dokumentų išrašymo ir pripažinimo taisyklių patvirtinimo“;

4.10. Elektroninių paslaugų kūrimo metodika, patvirtinta Lietuvos Respublikos susisiekimo ministro 2015 m. spalio 7 d. įsakymu Nr. 3-416(1.5E) „Dėl metodinių dokumentų patvirtinimo“;

4.11. 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“.

5. Asmens duomenys informacinėje sistemoje tvarkomi vadovaujantis Reglamentu (ES) 2016/679, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu.

6. Asmens duomenų tvarkymo informacinėje sistemoje tikslas – identifikuoti ir autentifikuoti paslaugų gavėjus, elektroniniu būdu tvarkyti informacinės sistemos duomenis, teikti informaciją duomenų gavėjams apie sąskaitas ir jų apmokėjimo būseną.

7. Informacinės sistemos tikslas – informacinių technologijų priemonėmis parengti, perkančiosioms organizacijoms pateikti ir išsaugoti su viešųjų pirkimų sutarčių vykdymu susijusias sąskaitas už įsigyjamas prekes, paslaugas ir darbus.

8. Informacinės sistemos uždaviniai:

8.1. automatizuotai kaupti duomenis, skirtus viešųjų pirkimų sutarčių vykdymo kontrolei ir skaidrumui didinti;

8.2. automatizuoti sąskaitų, kurios apmokamos iš valstybės biudžeto, apmokėjimo kontrolės procesus;

8.3. kompiuterizuoti perkančiųjų organizacijų veiklos ir valstybės pinigų srautų valdymą.

9. Pagrindinės informacinės sistemos funkcijos:

9.1. rengti, teikti, tvarkyti, priimti ir išsaugoti sąskaitas teisės aktų nustatytais terminais;

9.2. analizuoti sąskaitų duomenis, formuoti ataskaitas;

9.3. teikti sąskaitų duomenis informacinės sistemos duomenų gavėjams elektroniniu būdu;

9.4. teikti informaciją apie pateiktų sąskaitų apmokėjimo būseną paslaugų gavėjams;

9.5. teikti informaciją apie perkančiųjų organizacijų gautas sąskaitas, kurių pagrindu parengtos mokėjimo paraiškos, Lietuvos Respublikos finansų ministerijos Valstybės iždo departamentui;

9.6. rinkti, kaupti ir perduoti informaciją apie pirkimų sutarčių vykdymo rezultatus Viešųjų pirkimų tarnybai;

9.7. rinkti, kaupti ir perduoti informaciją apie teikiamas PVM sąskaitas duomenų gavėjams;

9.8. teikti informaciją apie pateiktų sąskaitų pagrindu parengtų mokėjimo paraiškų apmokėjimo būseną paslaugų gavėjams;

9.9. gauti iš Viešųjų pirkimų tarnybos sąskaitoms parengti reikalingą informaciją apie viešųjų pirkimų sutartis ir perkančiąsias organizacijas;

9.10. užtikrinti sąskaitų kilmės autentiškumą, turinio vientisumą ir įskaitomumą.

II SKYRIUS
INFORMACINĖS SISTEMOS ORGANIZACINĖ STRUKTŪRA

10. Informacinės sistemos valdytojas yra Nacionalinis bendrųjų funkcijų centras.

11. Informacinės sistemos valdytojas atlieka šias funkcijas:

11.1. kontroliuoja informacinės sistemos tvarkytojo darbą ir paveda jam vykdyti informacinės sistemos techninės ir programinės įrangos priežiūros funkcijas, vykdo jų stebėseną;

11.2. užtikrina informacinės sistemos funkcionavimo, techninės ir programinės įrangos priežiūros ir plėtros finansavimą;

11.3. tvirtina informacinės sistemos kūrimo ir plėtros planus, analizuoja pasiūlymus dėl informacinės sistemos veikimo, tobulinimo, priima sprendimus dėl informacinės sistemos tobulinimo ir modernizavimo, kontroliuoja jų vykdymą;

11.4. organizuoja duomenų saugos užtikrinimą;

11.5. organizacinėmis priemonėmis užtikrina informacinės sistemos prieinamumą, vientisumą, konfidencialumą;

11.6. organizuoja informacinės sistemos tobulinimo darbus ir jų finansavimą;

11.7. vadovauja informacinės sistemos tvarkytojui informacinės sistemos tvarkymo klausimais;

11.8. nagrinėja suinteresuotų asmenų siūlymus tobulinti informacinę sistemą ir priima dėl jų sprendimus;

11.9. nustato duomenų, kurie teikiami informacinės sistemos duomenų gavėjams, kategorijas;

11.10. vykdo kitas Nuostatuose, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir kituose teisės aktuose nurodytas informacinės sistemos valdytojo funkcijas.

12. Informacinės sistemos tvarkytojas yra valstybės įmonė Registrų centras (toliau – Registrų centras).

13. Informacinės sistemos tvarkytojas atlieka šias funkcijas:

13.1. užtikrina centralizuotą duomenų gavimą į informacinę sistemą ir informacinėje sistemoje kaupiamų duomenų teikimą duomenų gavėjams;

13.2. užtikrina informacinės sistemos funkcionavimą, techninės ir programinės įrangos priežiūrą;

13.3. teikia pasiūlymus informacinės sistemos valdytojui dėl informacinės sistemos tvarkymo ir tobulinimo;

13.4. tvarko informacinės sistemos duomenų archyvą ir užtikrina jo saugą;

13.5. tvarko paslaugų gavėjų duomenis;

13.6. sudaro sutartis su duomenų teikėjais ir gavėjais;

13.7. suderinęs su informacinės sistemos valdytoju nustato duomenų gavėjams teikiamų duomenų apimtis;

13.8. atsako, kad informacinės sistemos priemonėmis pateiktos sąskaitos ir duomenys, užtikrinantys sąskaitų kilmės autentiškumą, turinio vientisumą ir įskaitomumą, būtų saugomi vadovaujantis Lietuvos Respublikos teisės aktuose nustatyta dokumentų saugojimo tvarka;

13.9. vykdo kitas Nuostatuose, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir kituose teisės aktuose nurodytas informacinės sistemos tvarkytojo funkcijas.

14. Informacinės sistemos asmens duomenų valdytojas yra Nacionalinis bendrųjų funkcijų centras, o asmens duomenų tvarkytojas – Registrų centras.

15. Informacinės sistemos valdytojas ir tvarkytojas turi teisę su asmens duomenimis susijusią informaciją teisėtai gauti ir tvarkyti tokia apimtimi, kokia yra reikalinga informacinės sistemos tikslui įgyvendinti ir funkcijoms užtikrinti.

16. Informacinės sistemos duomenų teikėjai yra:

16.1. Viešųjų pirkimų tarnyba – teikia duomenis iš Centrinės viešųjų pirkimų informacinės sistemos;

16.2. Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos – teikia duomenis iš Mokesčių mokėtojų registro;

16.3. Lietuvos Respublikos ekonomikos ir inovacijų ministerija – teikia duomenis iš Valstybės informacinių išteklių sąveikumo platformos;

16.4. Lietuvos Respublikos teisingumo ministerija – teikia duomenis iš Lietuvos Respublikos juridinių asmenų registro ir Lietuvos Respublikos adresų registro;

16.5. Registrų centras – teikia duomenis iš autentifikavimo platformos (iPasas), Elektroninio dokumentų archyvo informacinės sistemos, Mokėjimų ir audito informacinės sistemos Sertifikatų centro;

16.6. Europos Komisija – teikia klasifikatorių duomenis iš PEPPOL (angl. *Pan-European Public Procurement Online*) tinklo;

16.7. Prie PEPPOL tinklo prisijungusių sistemų valdytojai – teikia e. sąskaitų duomenis.

17. Informacinės sistemos pirminių duomenų teikėjai yra tiekėjai (prekių tiekėjai, paslaugų teikėjai, rangovai), tiekiantys prekes, teikiantys paslaugas ar vykdantys darbus fiziniai asmenys, privatieji juridiniai ir viešieji juridiniai asmenys (toliau – tiekėjas). Tiekėjo darbuotojas, kuris yra paslaugų gavėjas, įveda Nuostatų 23 punkte išvardytus duomenis į informacinę sistemą.

18. Informacinės sistemos pirminių duomenų teikėju gali būti perkančioji organizacija, jeigu e. sąskaita pateikta ne informacinės sistemos priemonėmis.

19. Paslaugų gavėjų, kurie yra tiekėjo darbuotojai, teisės:

19.1. gauti informacinės sistemos teikiamas paslaugas;

19.2. gauti informaciją apie neteisingus jo pateiktų sąskaitų duomenis;

19.3. atsisakyti informacinės sistemos paslaugų.

20. Paslaugų gavėjų, kurie yra perkančiosios organizacijos darbuotojai, teisės:

20.1. gauti informacinės sistemos teikiamas paslaugas;

20.2. įgalioti perkančiosios organizacijos darbuotojus tvarkyti ir (ar) peržiūrėti perkančiajai organizacijai į informacinę sistemą pateiktus sąskaitų duomenis, pateikti, gauti ir peržiūrėti sąskaitas, keisti, naikinti šiuos įgaliojimus;

20.3. gauti informaciją apie neteisingus gautų sąskaitų duomenis;

20.4. atsisakyti informacinės sistemos paslaugų.

21. Paslaugų gavėjų pareigos:

21.1. tvarkyti (teikti, tikslinti, papildyti) informacinėje sistemoje esančius sąskaitų ir savo asmens duomenis;

21.2. gavus informaciją apie neteisingus sąskaitų duomenis, juos ištaisyti, patikslinti;

21.3. vykdyti kitas pareigas, nustatytas informacinės sistemos naudojimo sąlygų apraše.

III SKYRIUS
INFORMACINĖS SISTEMOS INFORMACINĖ STRUKTŪRA

22. Informacinės sistemos duomenų bazėje tvarkomi sąskaitų duomenys ir paslaugų gavėjų duomenys.

23. Informacinėje sistemoje tvarkomi šie e. sąskaitų duomenys:

23.1. Lietuvos Respublikos e. sąskaitos formatą atitinkančių e. sąskaitų duomenys:

23.1.1. e. sąskaitos išrašymo data;

23.1.2. e. sąskaitos serija ir numeris;

23.1.3. tiekėjo PVM mokėtojo kodas;

23.1.4. pirkėjo PVM mokėtojo kodas, kurį jis nurodė įsigydamas prekes, paslaugas ar darbus;

23.1.5. tiekėjo pavadinimas arba vardas, pavardė (jeigu tai fizinis asmuo) ir buveinė arba nuolatinė gyvenamoji vieta (jeigu tai fizinis asmuo);

23.1.6. pirkėjo pavadinimas arba vardas, pavardė (jeigu tai fizinis asmuo) ir buveinė arba nuolatinė gyvenamoji vieta (jeigu tai fizinis asmuo);

23.1.7. tiekiamų prekių arba teikiamų paslaugų pavadinimas ir jų kiekis;

23.1.8. prekių tiekimo, paslaugų teikimo ar darbų atlikimo data, jeigu ji nesutampa su sąskaitos išrašymo data;

23.1.9. avanso gavimo diena (jeigu sąskaita įforminamas avanso gavimas), kai ji nesutampa su sąskaitos išrašymo data;

23.1.10. tiekiamos prekės, teikiamos paslaugos ar atliekamų darbų vieneto kaina (be PVM), taip pat nuolaidos, neįtrauktos į vieneto kainą;

23.1.11. tiekiamų prekių, teikiamų paslaugų ar atliekamų darbų, apmokestinamų taikant vienodą tarifą, apmokestinamoji vertė;

23.1.12. PVM tarifas (tarifai);

23.1.13. PVM suma nacionaline valiuta;

23.1.14. kai įforminamas prekių ir (arba) paslaugų, kurios neapmokestinamos ar apmokestinamos taikant 0 procentų PVM tarifą, tiekimas (teikimas), – nuoroda į atitinkamą Lietuvos Respublikos pridėtinės vertės mokesčio įstatymo (toliau – PVM įstatymas) arba Direktyvos 2006/112/EB „Dėl pridėtinės vertės mokesčio bendros sistemos“ nuostatą arba bet kokia kita nuoroda, kad prekės (paslaugos) neapmokestinamos ar apmokestinamos taikant 0 procentų PVM tarifą;

23.1.15. fiskalinio agento PVM mokėtojo kodas, pavadinimas arba vardas, pavardė (jeigu tai fizinis asmuo) ir adresas – kai pagal PVM įstatymą prievolė apskaičiuoti PVM tenka užsienio apmokestinamojo asmens paskirtam fiskaliniam agentui;

23.1.16. nuoroda „Maržos apmokestinimo schema. Kelionių agentūros“ – kai taikoma speciali turizmo paslaugų apmokestinimo PVM schema, nurodyta PVM įstatymo XII skyriaus antrame skirsnyje, arba nuoroda „Maržos apmokestinimo schema. Naudotos prekės“ arba „Maržos apmokestinimo schema. Meno kūriniai“, arba „Maržos apmokestinimo schema. Kolekcionavimo objektai ir antikvariniai daiktai“ – kai taikoma speciali naudotų prekių, meno kūrinių, kolekcinių ir antikvarinių daiktų apmokestinimo PVM schema, nurodyta PVM įstatymo XII skyriaus trečiame skirsnyje;

23.1.17. nuoroda „Atvirkštinis apmokestinimas“ – kai įforminamas prekių, darbų ir (arba) paslaugų, už kurias prievolė apskaičiuoti (arba išskaityti) ir sumokėti PVM tenka pirkėjui (klientui), tiekimas (atlikimas, teikimas);

23.1.18. nuoroda „Pinigų apskaitos sistema“ – kai prievolė apskaičiuoti PVM atsiranda gavus atlygį už patiektas prekes, įvykdytus darbus ar suteiktas paslaugas;

23.1.19. nuoroda „Sąskaitų faktūrų išsirašymas“ – kai sąskaitą prekių tiekėjo ar paslaugų teikėjo vardu įformina pirkėjas;

23.1.20. nuoroda „Avansinė sąskaita“ – kai sąskaitą išrašo prekių tiekėjas ir (arba) paslaugų teikėjas, ir (arba) rangovas, t. y. avanso gavėjas, ir nurodo, kad PVM skaičiuojamas nuo avansinio mokesčio;

23.1.21. tikslinamos sąskaitos išrašymo data, serija, numeris ir kiti tikslinamų apskaitos dokumentų duomenys (laikotarpis, kuriuo buvo patiektos prekės, įvykdyti darbai ar suteiktos paslaugos ir kt.);

23.1.22. bendras kodas, jei tiekėjas yra užsienio įmonė;

23.1.23. viešojo pirkimo numeris;

23.1.24. viešojo pirkimo sutarties numeris arba viešojo pirkimo sutarties identifikatorius (jei yra);

23.1.25. nuoroda dėl pirkimo tipo;

23.1.26. tiekėjo juridinio asmens kodas (arba fizinio asmens kodas, jeigu tai fizinis asmuo), pirkimo objekto rūšis – darbai, prekė, paslauga – ir jį apibūdinančios kategorijos;

23.1.27. bendrojo viešųjų pirkimų žodyno pagrindinis kodas pirkimui apibūdinti;

23.1.28. sąskaitos tipas: PVM sąskaita faktūra, sąskaita faktūra (ne PVM), išankstinė sąskaita, kreditinė sąskaita faktūra, supaprastinta PVM sąskaita faktūra;

23.1.29. papildoma tiekėjo įvesta informacija (papildomos informacijos laukas);

23.1.30. tiekėjo pridėti sąskaitos priedai.

23.2. LST EN 16931 (EN 16931 – CEN/TC 434) standartą atitinkančių bei per PEPPOL eDelivery sistemą gaunamų e. sąskaitų duomenys:

23.2.1. sąskaitos faktūros (toliau – SF) numeris (angl. *Invoice number*);

23.2.2. SF data (angl. *Invoice issue date*);

23.2.3. SF tipo kodas (angl. *Invoice type code*);

23.2.4. SF valiutos kodas (angl. *Invoice currency code*);

23.2.5. PVM valiutos kodas (angl. *VAT accounting currency code*);

23.2.6. PVM priskaičiavimo data (angl. *Value added tax point date*);

23.2.7. PVM priskaičiavimo datos kodas (angl. *Value added tax point date code*);

23.2.8. mokėjimo data (angl. *Payment due date*);

23.2.9. pirkėjo nuoroda (angl. *Buyer reference*);

23.2.10. projekto nuoroda (angl. *Project reference*);

23.2.11. sutarties nuoroda (numeris, unikali nuoroda) (angl. *Contract reference*);

23.2.12. pirkėjo užsakymo nuoroda (angl. *Purchase order reference*);

23.2.13. pardavėjo užsakymo nuoroda (angl. *Sales order reference*);

23.2.14. perdavimo ir priėmimo akto nuoroda (angl. *Receiving advice reference*);

23.2.15. važtaraščio nuoroda (angl. *Despatch advice reference*);

23.2.16. kvietimo dalyvauti konkurse ar partijos nuoroda (angl. *Tender or lot reference*);

23.2.17. sąskaitos objekto / schemos identifikatorius (angl. *Invoiced object identifier / Scheme identifier*);

23.2.18. pirkėjo apskaitos nuoroda (angl. *Buyer accounting reference*);

23.2.19. mokėjimo sąlygos (angl. *Payment terms*);

23.2.20. SF pastabos (angl. *Invoice Note*):

23.2.20.1. pastabos temos kodas (angl. *Invoice note subject code*);

23.2.20.2. pastabos tekstas (angl. *Invoice Note*);

23.2.21. proceso duomenys (angl. *Process Control*):

23.2.21.1. veiklos proceso tipas (angl. *Business process type*);

23.2.21.2. specifikacijos identifikatorius (angl. *Specification identifier*);

23.2.22. tikslinamos sąskaitos informacija (angl. *Preceding Invoice reference*):

23.2.22.1. tikslinamos sąskaitos nuoroda (angl. *Preceding Invoice reference*);

23.2.22.2. tikslinamos SF data (angl. *Preceding Invoice issue date*);

23.2.23. pardavėjo duomenys:

23.2.23.1. pardavėjo pavadinimas (juridinio asmens pavadinimas arba vardas, pavardė, jeigu tai fizinis asmuo) (angl. *Seller name*);

23.2.23.2. pardavėjo prekės ženklas (angl. *Seller trading name*);

23.2.23.3. pardavėjo identifikacijos schemos nuoroda (angl. *Seller identifier Scheme identifier*);

23.2.23.4. pardavėjo registracijos identifikatoriaus schemos nuoroda (angl. *Seller legal registration identifier / Scheme identifier*);

23.2.23.5. pardavėjo PVM kodas (angl. *Seller VAT identifier*);

23.2.23.6. pardavėjo vietinis identifikavimas mokesčių tikslais arba nuoroda, leidžianti pardavėjui nurodyti savo registruotą mokesčių statusą (angl. *Seller tax registration identifier*);

23.2.23.7. papildoma pardavėjo teisinė informacija (angl. *Seller additional legal information*);

23.2.23.8. pardavėjo elektroninio adreso identifikavimo schema (angl. *Seller electronic address / Scheme identifier*);

23.2.23.9. pardavėjo adresas:

23.2.23.9.1. 1 pardavėjo adreso eilutė;

23.2.23.9.2. 2 pardavėjo adreso eilutė;

23.2.23.9.3. 3 pardavėjo adreso eilutė;

23.2.23.9.4. pardavėjo miestas;

23.2.23.9.5. pardavėjo pašto kodas;

23.2.23.9.6. šalies regionas;

23.2.23.9.7. pardavėjo šalies kodas;

23.2.23.10. pardavėjo kontaktiniai duomenys:

23.2.23.10.1. pardavėjo kontaktinis asmuo (vardas, pavardė, pareigos);

23.2.23.10.2. kontaktinio asmens telefono numeris;

23.2.23.10.3. kontaktinio asmens el. pašto adresas;

23.2.24. pirkėjo duomenys:

23.2.24.1. pirkėjo pavadinimas (juridinio asmens pavadinimas arba vardas, pavardė, jeigu tai fizinis asmuo) (angl. *Buyer name*);

23.2.24.2. pirkėjo prekės ženklas (angl. *Buyer trading name*);

23.2.24.3. pirkėjo identifikacijos schemos nuoroda (angl. *Buyer identifier Scheme identifier*);

23.2.24.4. pirkėjo registracijos identifikatoriaus schemos nuoroda (angl. *Buyer legal registration identifier / Scheme identifier*);

23.2.24.5. pirkėjo PVM kodas (angl. *Buyer VAT identifier*);

23.2.24.6. pirkėjo elektroninio adreso identifikavimo schema (angl. *Buyer electronic address / Scheme identifier*);

23.2.24.7. pirkėjo adresas:

23.2.24.7.1. 1 pirkėjo adreso eilutė;

23.2.24.7.2. 2 pirkėjo adreso eilutė;

23.2.24.7.3. 3 pirkėjo adreso eilutė;

23.2.24.7.4. pirkėjo miestas;

23.2.24.7.5. pirkėjo pašto kodas;

23.2.24.7.6. šalies regionas;

23.2.24.7.7. pirkėjo šalies kodas;

23.2.24.8. pirkėjo kontaktiniai duomenys:

23.2.24.8.1. pirkėjo kontaktinis asmuo (vardas, pavardė, pareigos);

23.2.24.8.2. kontaktinio asmens telefono numeris;

23.2.24.8.3. kontaktinio asmens el. pašto adresas;

23.2.25. mokėtojo duomenys:

23.2.25.1. mokėtojo arba mokėjimo gavėjo pavadinimas (juridinio asmens pavadinimas arba vardas, pavardė, jeigu tai fizinis asmuo) (angl. *Payee name*);

23.2.25.2. mokėtojo arba mokėjimo gavėjo identifikacijos schemos nuoroda (angl. *Payee identifier Scheme identifier*);

23.2.25.3. mokėtojo arba mokėjimo gavėjo registracijos identifikatoriaus schemos nuoroda (angl. *Payee legal registration identifier / Scheme identifier*);

23.2.26. pardavėjo fiskalinio agento duomenys (angl. *Seller tax representative party*):

23.2.26.1. pardavėjo fiskalinio agento pavadinimas (angl. *Seller tax representative name*);

23.2.26.2. pardavėjo fiskalinio agento PVM mokėtojo kodas (angl. *Seller tax representative VAT identifier*);

23.2.26.3. pardavėjo fiskalinio agento adresas (angl. *Seller tax representative postal address*):

23.2.26.3.1. 1 fiskalinio agento adreso eilutė;

23.2.26.3.2. 2 fiskalinio agento adreso eilutė;

23.2.26.3.3. 3 fiskalinio agento adreso eilutė;

23.2.26.3.4. fiskalinio agento miestas;

23.2.26.3.5. fiskalinio agento pašto kodas;

23.2.26.3.6. fiskalinio agento šalies regionas;

23.2.26.3.7. fiskalinio agento šalies kodas;

23.2.27. pristatymo duomenys:

23.2.27.1. pristatymo vietos pavadinimas (angl. *Deliver to party name*);

23.2.27.2. pristatymo vietos identifikatorius (angl. *Deliver to location identifier / Scheme identifier*);

23.2.27.3. pristatymo data (angl. *Actual delivery date*);

23.2.27.4. sąskaitos periodas (angl. *Invoicing period*):

23.2.27.4.1. sąskaitos periodo pradžia;

23.2.27.4.2. sąskaitos periodo pabaiga;

23.2.27.5. pristatymo adresas (angl. *Deliver to adress*):

23.2.27.5.1. 1 pristatymo adreso eilutė;

23.2.27.5.2. 2 pristatymo adreso eilutė;

23.2.27.5.3. 3 pristatymo adreso eilutė;
23.2.27.5.4. pristatymo miestas;
23.2.27.5.5. pristatymo pašto kodas;
23.2.27.5.6. pristatymo šalies regionas;
23.2.27.5.7. pristatymo šalies kodas;
23.2.28. mokėjimo nurodymai (angl. *Payment instructions*):
23.2.28.1. mokėjimo būdo kodas (angl. *Payment means type code*);
23.2.28.2. mokėjimo būdo aprašymas (angl. *Payment means text*);
23.2.28.3. kita mokėjimo informacija (angl. *Remittance information*);
23.2.28.4. mokėjimo pervedimai (angl. *Credit transfer*):
23.2.28.4.1. mokėjimo sąskaitos numeris (angl. *Payment account identifier*);
23.2.28.4.2. mokėjimo sąskaitos pavadinimas (angl. *Payment account name*);
23.2.28.4.3. mokėjimo paslaugos teikėjo identifikatorius (angl. *Payment service provider identifier*);
23.2.28.5. mokėjimo kortelės duomenys:
23.2.28.5.1. mokėjimo kortelės numeris;
23.2.28.5.2. mokėjimo kortelės savininkas;
23.2.28.6. tiesioginio debeto duomenys:
23.2.28.6.1. tiesioginio debeto identifikatorius (angl. *Mandate reference identifier*);
23.2.28.6.2. tiesioginio debeto identifikatorius (angl. *Bank assigned creditor identifier*);
23.2.28.6.3. pinigų nurašymo sąskaitos numeris (angl. *Debited account identifier*);
23.2.29. nuolaidų duomenys:
23.2.29.1. dokumento nuolaida (angl. *Document level allowance amount*);
23.2.29.2. dokumento nuolaidos bazė (angl. *Document level allowance base amount*);
23.2.29.3. dokumento nuolaidos procentas (angl. *Document level allowance percentage*);
23.2.29.4. dokumento nuolaidos PVM kategorija (identifikatorius / kodas) (angl. *Document level allowance VAT category code*);
23.2.29.5. dokumento nuolaidos PVM (angl. *Document level allowance VAT rate*);
23.2.29.6. dokumento nuolaidos priežastis (angl. *Document level allowance reason*);
23.2.29.7. dokumento nuolaidos priežasties kodas (angl. *Document level allowance reason code*);
23.2.30. papildomų mokesčių duomenys:
23.2.30.1. dokumento mokesčio suma be PVM (angl. *Document level charge amount*);
23.2.30.2. dokumento mokesčio bazė (angl. *Document level charge base amount*);
23.2.30.3. dokumento mokesčio procentas (angl. *Document level charge percentage*);
23.2.30.4. dokumento mokesčio PVM kategorija (identifikatorius / kodas) (angl. *Document level charge VAT category code*);
23.2.30.5. dokumento mokesčio PVM procentas (angl. *Document level charge VAT rate*);
23.2.30.6. mokesčio priežastis (angl. *Document level charge reason*);
23.2.30.7. mokesčio priežasties kodas (angl. *Document level charge reason code*);
23.2.31. dokumento sumos:
23.2.31.1. eilučių suma (angl. *Sum of Invoice line net amount*);
23.2.31.2. dokumento eilučių suma (angl. *Sum of allowances on document level*);
23.2.31.3. dokumento nuolaidos suma (angl. *Sum of charges on document level*);
23.2.31.4. sąskaitos suma be PVM (angl. *Invoice total amount without VAT*);

23.2.31.5. sąskaitos PVM suma (angl. *Invoice total VAT amount*);

23.2.31.6. sąskaitos PVM suma pardavėjo apskaitos valiuta (angl. *Invoice total VAT amount in accounting currency*);

23.2.31.7. sąskaitos suma su PVM (angl. *Invoice total amount with VAT*);

23.2.31.8. sumokėta suma (angl. *Paid amount*);

23.2.31.9. apvalinimo suma (angl. *Rounding amount*);

23.2.31.10. Nepaskirstyta suma, kurią prašoma sumokėti (angl. *Amount due for payment*);

23.2.32. PVM detalizavimas:

23.2.32.1. visų apmokestinamųjų sumų suma, kuriai taikomas konkretus PVM ir PVM procentas (angl. *VAT category, taxable amount*);

23.2.32.2. PVM suma konkrečiam PVM procentui (angl. *VAT category tax amount*);

23.2.32.3. PVM kategorija (angl. *VAT category code*);

23.2.32.4. PVM tarifas (angl. *VAT category rate*);

23.2.32.5. PVM neapmokestinimo priežastis (angl. *VAT exemption reason text*);

23.2.32.6. PVM neapmokestinimo priežasties kodas (angl. *VAT exemption reason code*);

23.2.33. sąskaitos priedų duomenys:

23.2.33.1. priedo identifikatorius (angl. *Supporting document reference*);

23.2.33.2. priedo apibūdinimas (angl. *Supporting document description*);

23.2.33.3. priedo saugojimo vieta (angl. *External document location*);

23.2.33.4. prisegtas priedas (angl. *Attached document / Attached document Mime code / Attached document Filename*);

23.2.34. sąskaitos eilučių duomenys:

23.2.34.1. sąskaitos eilutės identifikatorius (angl. *Invoice line identifier*);

23.2.34.2. eilutės pavadinimas (angl. *Invoice line note*);

23.2.34.3. eilutės identifikavimo schema (angl. *Invoice line object identifier / Scheme identifier*);

23.2.34.4. kiekis (angl. *Invoiced quantity*);

23.2.34.5. matavimo vienetas (angl. *Invoiced quantity unit of measure code*);

23.2.34.6. eilutės suma (angl. *Invoice line net amount*);

23.2.34.7. pirkimo užsakymo eilutės identifikatorius (angl. *Referenced purchase order line reference*);

23.2.34.8. pirkėjo apskaitos nuoroda (angl. *Invoice line Buyer accounting reference*);

23.2.34.9. eilutės periodas:

23.2.34.9.1. periodo pradžia (angl. *Invoice line period start date*);

23.2.34.9.2. periodo pabaiga (angl. *Invoice line period end date*);

23.2.34.10. eilutės nuolaidos duomenys:

23.2.34.10.1. nuolaidos suma be PVM (angl. *Invoice line allowance amount*);

23.2.34.10.2. nuolaidos bazė (angl. *Invoice line allowance base amount*);

23.2.34.10.3. nuolaidos procentas (angl. *Invoice line allowance percentage*);

23.2.34.10.4. nuolaidos priežastis (angl. *Invoice line allowance reason*);

23.2.34.10.5. nuolaidos priežasties kodas (angl. *Invoice line allowance reason code*);

23.2.34.11. eilutės papildomų mokesčių duomenys:

23.2.34.11.1. eilutės mokesčio suma be PVM (angl. *Invoice line charge amount*);

23.2.34.11.2. eilutės mokesčio bazė (angl. *Invoice line charge base amount*);

23.2.34.11.3. eilutės mokesčio procentas (angl. *Invoice line charge percentage*);

23.2.34.11.4. mokesčio priežastis (angl. *Invoice line charge reason*);

23.2.34.11.5. mokesčio priežasties kodas (angl. *Invoice line charge reason code*);

23.2.34.12. kainos detalizavimas:

23.2.34.12.1. kaina (angl. *Item net price*);

23.2.34.12.2. bendra nuolaida (angl. *Item price discount*);

23.2.34.12.3. vieneto kaina prieš bendros nuolaidos pritaikymą (angl. *Item gross price*);

23.2.34.12.4. prekių vienetų, kuriems taikoma kaina, skaičius (angl. *Item price base quantity*);

23.2.34.12.5. matavimo vienetas (angl. *Item price base quantity unit of measure code*);

23.2.34.13. eilutės PVM duomenys:

23.2.34.13.1. PVM kategorija (angl. *Invoiced item VAT category code*);

23.2.34.13.2. PVM procentas (angl. *Invoiced item VAT rate*);

23.2.34.14. prekės informacija:

23.2.34.15. prekės pavadinimas (angl. *Item name*);

23.2.34.16. prekės apibūdinimas (angl. *Item description*);

23.2.34.17. pardavėjo prekės kodas (angl. *Item Seller's identifier*);

23.2.34.18. pirkėjo prekės kodas (angl. *Item Buyer's identifier*);

23.2.34.19. prekės identifikavimo (katalogo) schema (angl. *Item standard identifier / Scheme identifier*);

23.2.34.20. prekės identifikavimo (katalogo) schema (angl. *Item classification identifier / Scheme identifier / Scheme version identifier*);

23.2.34.21. prekės šalies kodas (identifikatorius) (angl. *Item country of origin*);

23.2.34.22. papildomi prekės apibūdinimai:

23.2.34.22.1. papildomo prekės apibūdinimo pavadinimas (angl. *Item attribute name*);

23.2.34.22.2. papildomas prekės apibūdinimas (angl. *Item attribute value*).

24. Informacinėje sistemoje tvarkomi duomenys gaunami iš:

24.1. Centrinės viešųjų pirkimų informacinės sistemos:

24.1.1. registruotų perkančiųjų organizacijų duomenys:

24.1.1.1. juridinio asmens kodas;

24.1.1.2. juridinio asmens pavadinimas;

24.1.2. viešųjų pirkimų sutarčių duomenys:

24.1.2.1. viešojo pirkimo numeris;

24.1.2.2. viešojo pirkimo sutarties numeris arba identifikacinis numeris (jei yra);

24.1.2.3. perkančiosios organizacijos juridinio asmens kodas;

24.1.2.4. tiekėjo juridinio kodas;

24.1.2.5. bendrasis tiekėjo kodas;

24.1.2.6. viešojo pirkimo sutarties būsena;

24.1.2.7. tiekėjo šalies kodas;

24.1.2.8. sutarties sudarymo data;

24.2. Juridinių asmenų registro:

24.2.1. juridinio asmens kodas;

24.2.2. juridinio asmens pavadinimas;

24.2.3. juridinio asmens teisinė forma;

24.2.4. juridinio asmens buveinė (adresas);

24.3. Elektroninio dokumentų archyvo informacinės sistemos – elektroninių sąskaitų išsaugojimo elektroniniame archyve data;

24.4. Registrų centro Sertifikatų centro:

24.4.1. elektroninės sąskaitos laiko žymos identifikatorius;

24.4.2. laiko reikšmė, nustatoma pagal informacinės sistemos serverio laiką;

24.4.3. vienkrypčio šifravimo būdu sudaryta žymimų duomenų santrauka;

24.5. Mokesčių mokėtojų registro:

24.5.1. mokesčių mokėtojų duomenys:

24.5.1.1. PVM mokėtojo kodo prefiksas;

24.5.1.2. PVM mokėtojo kodo skaitmeninė dalis;

24.5.1.3. PVM mokėtojo pavadinimas;

24.5.1.4. PVM mokėtojo adresas;

24.5.1.5. įregistravimo PVM mokėtoju data;

24.5.1.6. išregistravimo iš PVM mokėtojų data (jei yra);

24.6. tiekėjų ir perkančiųjų organizacijų finansų valdymo ir apskaitos informacinių sistemų:

24.6.1. elektroninių sąskaitų duomenys pagal parengtą ir suderintą elektroninių sąskaitų duomenų modelį;

24.7. Valstybės informacinių išteklių sąveikumo platformos:

24.7.1. fizinio asmens vardas;

24.7.2. fizinio asmens pavardė;

24.7.3. fizinio asmens kodas;

24.8. Mokėjimų ir audito informacinės sistemos:

24.8.1. informacija apie laiku neapmokėtą sumą (pagal kiekvieną informacinės sistemos paskyrą);

24.9. autentifikavimo platformos (iPasas):

24.9.1. fizinio asmens vardas;

24.9.2. fizinio asmens pavardė;

24.9.3. fizinio asmens kodas;

24.9.4. požymis, nusakantis, kad fizinis asmuo yra užsienietis;

24.9.5. fizinio asmens šalis (taikoma užsienio šalių fiziniams asmenims);

24.9.6. fizinio asmens gimimo data (taikoma užsienio šalių fiziniams asmenims);

24.9.7. juridinio asmens kodas;

24.9.8. juridinio asmens pavadinimas;

24.9.9. požymis, nusakantis, ar tai užsienio šalies juridinis asmuo;

24.9.10. juridinio asmens šalis (taikoma užsienio šalių juridiniams asmenims);

25. Informacinėje sistemoje kaupiami paslaugų gavėjų duomenys (jeigu tai fizinis asmuo):

25.1. vardas (vardai);

25.2. pavardė (pavardės);

25.3. pareigos;

25.4. suteiktos prieigos teisės.

IV SKYRIUS
INFORMACINĖS SISTEMOS FUNKCINĖ STRUKTŪRA

26. Informacinės sistemos funkcinę struktūrą sudaro funkciniai komponentai:

26.1. bendras portalas, kurio funkcija – informacinės sistemos pagrindinio turinio saugojimas. Portale pateikiama bendra informacija: naujienos, teisinė informacija, dažniausiai užduodami klausimai ir atsakymai. Per šį portalą inicijuojamas prisijungimas prie paslaugų gavėjo posistemio arba prie administratorių posistemio;

26.2. paslaugų gavėjo posistemis, kurio funkcija – pagrindinių veiksmų su sąskaitomis atlikimas. Posistemis sudarytas iš penkių modulių:

26.2.1. sąskaitų įvedimo ir tvarkymo modulis, kurio funkcija – sąskaitų paruošimas, peržiūrėjimas ir pateikimas;

26.2.2. sąskaitų valdymo modulis, kurio funkcija – pateiktų sąskaitų tvirtinimas, grąžinimas jas tikslinti ar atmesti, kitų susijusių valdymo veiksmų atlikimas;

26.2.3. dokumentų formavimo modulis, kurio funkcija – PDF / A-3 formatą atitinkančių elektroninių dokumentų generavimas ir su jais susijusios laiko žymos suformavimo inicijavimas;

26.2.4. paskyrų tvarkymo modulis, kurio funkcija – paslaugų gavėjų paskyrų tvarkymas;

26.2.5. ES e. sąskaitų modulis, kuriame tvarkomi ES standartą atitinkančių e. sąskaitų duomenys;

26.3. administratorių posistemis, kurio funkcija – informacinės sistemos konfigūravimo bei valdymo veiksmų vykdymas. Posistemį sudaro 13 modulių:

26.3.1. klasifikatorių modulis, kurio funkcija – informacinėje sistemoje numatytų klasifikatorių tvarkymas;

26.3.2. sutarčių tvarkymo modulis, kurio funkcija – paslaugų gavėjų tvirtinamo informacinės sistemos naudojimo sąlygų aprašo tvarkymas ir pakeisto informacinės sistemos naudojimo sąlygų aprašo šablono įkėlimas;

26.3.3. parametrų tvarkymo modulis, kurio funkcija – informacinėje sistemoje numatytų parametrų tvarkymas;

26.3.4. klaidų ir įvykių modulis, kurio funkcija – informacinėje sistemoje įvykusių klaidų žurnalo peržiūrėjimas ir galimų sistemos įvykių sąrašo tvarkymas;

26.3.5. duomenų mainų valdymo modulis, kurio funkcija – naujų duomenų mainuose dalyvausiančių išorinių sistemų užregistravimas ir jų prisijungimo sertifikatų generavimo inicijavimas;

26.3.6. paskyrų tvarkymo modulis, kurio funkcija – visų informacinės sistemos paslaugų gavėjų paskyrų tvarkymas, naujų paskyrų kūrimas;

26.3.7. sesijų valdymo modulis, kurio funkcija – prie informacinės sistemos besijungiančių paslaugų gavėjų skaičiaus kontroliavimas ir informacijos apie paskutinį paslaugų gavėjo prisijungimą prie informacinės sistemos pateikimas;

26.3.8. asmens identifikavimo modulis, kurio funkcija – informacinės sistemos paslaugų gavėjų identifikavimas;

26.3.9. duomenų archyvavimo modulis, kurio funkcija – įvedamų bei tvarkomų duomenų automatinis archyvavimas;

26.3.10. ataskaitų modulis, kurio funkcija – informacinėje sistemoje numatytų ataskaitų formavimas;

26.3.11. paslaugos gavėjų veiksmų auditavimo modulis, kurio funkcija – užtikrinti, kad informacinės sistemos paslaugų gavėjų veiksmai būtų užregistruoti ir išsaugoti;

26.3.12. duomenų mainų modulis, kurio funkcija – duomenų mainų tiek su vidinėmis, tiek su išorinėmis informacinėmis sistemomis užtikrinimas;

26.3.13. informavimo modulis, kurio funkcija – informacinis žinučių formavimas ir pateikimas adresatams.

V SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ TEIKIMAS IR NAUDOJIMAS

27. Informacinės sistemos duomenų gavėjai yra:

27.1. Lietuvos Respublikos finansų ministerija;

27.2. Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos;

27.3. Viešųjų pirkimų tarnyba;

27.4. Prie PEPPOL tinklo prisijungusių šalių atsakingos institucijos;

27.5. Nacionalinis bendrųjų funkcijų centras.

28. Duomenys, įskaitant ir asmens duomenis, teikiami vykdant informacinės sistemos tvarkytojui pavestas funkcijas. Visi informacinės sistemos duomenys yra teikiami juridiniams ir fiziniams asmenims, jeigu Lietuvos Respublikos ar Europos Sąjungos teisės aktuose nenustatyta kitaip. Informacinės sistemos duomenys teikiami pagal informacinės sistemos tvarkytojo ir duomenų gavėjo sudarytą duomenų teikimo sutartį (daugkartinio teikimo atveju) arba duomenų gavėjo prašymą (vienkartinio teikimo atveju). Sutartyje turi būti nurodytas duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, sąlygos, tvarka ir teikiamų duomenų apimtis. Prašyme turi būti nurodytas duomenų naudojimo tikslas, teikimo bei gavimo teisinis pagrindas ir prašomų pateikti duomenų apimtis. Kai duomenys tvarkomi automatiniu būdu ir taikomos tinkamos duomenų saugumą užtikrinančios priemonės, teikiant duomenis pagal informacinės sistemos tvarkytojo ir duomenų gavėjo sudarytą duomenų teikimo sutartį prioritetas teikiamas automatiniam duomenų teikimo būdui, o teikiant duomenis pagal duomenų gavėjo prašymą – duomenų teikimui elektroninių ryšių priemonėmis.

29. Informacinėje sistemoje kaupiami duomenys teikiami tokio turinio ir formos, kokie yra tvarkomi informacinėje sistemoje. Kai teikiamų duomenų turinys ir forma neatitinka duomenų gavėjų poreikių, reikiamos priemonės rengiamos Lietuvos Respublikos Vyriausybės nustatyta tvarka.

30. Informacinės sistemos duomenų naudojimo sąlygos ir tvarka nustatyta informacinės sistemos naudojimosi sąlygų apraše, kuris yra viešai prieinamas informacinės sistemos tvarkytojo interneto svetainėje adresu www.registrucentras.lt ir informacinėje sistemoje. Laikoma, kad paslaugų gavėjas sutinka su informacinės sistemos naudojimosi sąlygomis, kai jis informacinėje sistemoje paspaudžia nuorodą (mygtuką) „Patvirtinti“, esančią naudojimosi sąlygų teksto apačioje.

31. Informacinės sistemos duomenys informacinės sistemos valdytojui, tvarkytojui ir duomenų gavėjams, nurodytiems Nuostatų 27 punkte, teikiami neatlygintinai. Už informacinės sistemos priemonėmis pateikiamas sąskaitas gali būti imamas atlygis, kurio dydį ir mokėjimo tvarką nustato informacinės sistemos valdytojas.

32. Duomenys 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 Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka.

33. Duomenų gavėjai, registrų tvarkytojai ar asmuo (fizinis arba juridinis), kurio duomenys įrašyti informacinėje sistemoje, gali pateikti informacinės sistemos tvarkytojui rašytinį prašymą ištaisyti klaidingus informacinės sistemos duomenis. Klaidingais laikomi informacinėje

sistemoje įrašyti duomenys, neatitinkantys informacinei sistemai pateiktų dokumentų. Informacinės sistemos tvarkytojas, gavęs prašymą ištaisyti klaidingus informacinės sistemos duomenis ir jame nurodytus faktus patvirtinančius dokumentus, turi per 5 darbo dienas ištaisyti informacinės sistemos duomenis ir apie tai raštu pranešti juridiniam arba fiziniam asmeniui, su kuriuo susiję ištaisyti duomenys, bei asmenims, kuriems klaidingi duomenys perduoti.

VI SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ SAUGA

34. Informacinės sistemos duomenų saugą reglamentuoja informacinės sistemos valdytojo patvirtinti informacinės sistemos duomenų saugos nuostatai ir kiti saugos politikos įgyvendinimo dokumentai, kurie rengiami, derinami ir tvirtinami vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ nuostatomis.

35. Už informacinės sistemos duomenų saugą pagal kompetenciją atsako informacinės sistemos valdytojas ir informacinės sistemos tvarkytojas.

36. Atsarginės duomenų kopijos daromos vadovaujantis Duomenų rezervinio kopijavimo ir laikmenų saugojimo tvarka, patvirtinta Registrų centro direktoriaus 2008 m. birželio 20 d. įsakymu Nr. v-148 „Dėl Nešiojamųjų įrenginių saugumo patvirtinimo tvarkos ir Duomenų rezervinio kopijavimo ir laikmenų saugojimo tvarkos patvirtinimo“ (2011 m. lapkričio 18 d. įsakymo Nr. v-221 redakcija).

37. Informacinės sistemos paslaugų gavėjai, tvarkantys informacinės sistemos duomenis, informaciją, dokumentus ir jų kopijas, yra įpareigoti saugoti duomenų ir informacijos paslaptį. Įpareigojimas saugoti paslaptį galioja ir nutraukus su duomenų, informacijos, dokumentų ir jų kopijų tvarkymu susijusią veiklą. Informacinės sistemos paslaugų gavėjai, kurie tvarko asmens duomenis, privalo saugoti asmens duomenų paslaptį. Ši pareiga galioja ir jiems pasitraukus iš valstybės tarnybos, perėjus dirbti į kitas pareigas, pasibaigus jų darbo ar sutartiniams santykiams.

38. Informacinėje sistemoje tvarkomų fizinių asmenų duomenų saugumas užtikrinamas laikantis Reglamente (ES) 2016/679 nustatytų reikalavimų.

39. Informacinės sistemos duomenys kaupiami ir sąskaitų duomenų bazėje saugomi, kol tvarkomi sąskaitų duomenys. Skaitmeniniame sąskaitų archyve duomenys saugomi 10 metų. Pasibaigus šiam terminui, duomenys sunaikinami Lietuvos vyriausiojo archyvaro nustatyta tvarka. Paslaugų gavėjų asmens duomenys informacinėje sistemoje ir archyve saugomi, kol saugomi tvarkomi (tvarkyti) jo sąskaitų duomenys arba kol paslaugų gavėjui kontrolės funkcijoms vykdyti reikalinga prieiga prie informacinės sistemos.

VII SKYRIUS
INFORMACINĖS SISTEMOS FINANSAVIMAS

40. Informacinė sistema finansuojama:

40.1. informacinės sistemos modernizavimas ir plėtra – iš Lietuvos Respublikos valstybės biudžeto ir Europos Sąjungos struktūrinių fondų lėšų;

40.2. informacinės sistemos priežiūra ir palaikymas – iš Lietuvos Respublikos valstybės biudžeto, Europos Sąjungos struktūrinių fondų ir kitų finansavimo šaltinių lėšų, taip pat ir / ar lėšų, gautų už naudojimąsi informacinės sistemos duomenimis.

VIII SKYRIUS
INFORMACINĖS SISTEMOS MODERNIZAVIMAS IR LIKVIDAVIMAS

41. Informacinė sistema modernizuojama ir likviduojama Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo ir Aprašo nustatyta tvarka.

42. Likviduojant informacinę sistemą, jos duomenys perduodami kitai informacinei sistemai arba sunaikinami, arba perduodami valstybės archyvui Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

43. Kiekvienas duomenų subjektas, kurio asmens duomenys tvarkomi informacinėje sistemoje, turi Reglamento (ES) 2016/679 15–18 straipsniuose nustatytas teises. Duomenų subjektų teisės įgyvendinamos vadovaujantis Duomenų subjektų teisių įgyvendinimo Nacionaliniame bendrųjų funkcijų centre tvarkos aprašu, patvirtintu Nacionalinio bendrųjų funkcijų centro direktoriaus 2018 m. rugpjūčio 29 d. įsakymu Nr. V-83 „Dėl duomenų subjektų teisių įgyvendinimo Nacionaliniame bendrųjų funkcijų centre tvarkos aprašo patvirtinimo“.

_____

PATVIRTINTA
Nacionalinio bendrųjų funkcijų centro
direktoriaus 2019 m. rugpjūčio 26 d.
įsakymu Nr. V-316

INFORMACINĖS SISTEMOS „E. SĄSKAITA“ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacinės sistemos „E. sąskaita“ (toliau – informacinė sistema) duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja informacinės sistemos elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką.

2. Saugos nuostatuose vartojamos sąvokos:

2.1. **Informacinės sistemos administratorius** (toliau – administratorius) – valstybės įmonės Registrų centro (toliau – Registrų centras) darbuotojas, dirbantis pagal darbo sutartį, arba Lietuvos Respublikos teisingumo ministerijos valstybės tarnautojas ar pagal darbo sutartį dirbantis darbuotojas, prižiūrintis informacinę sistemą ir (ar) jos infrastruktūrą, užtikrinantis jų veikimą, elektroninės informacijos saugą ir kibernetinį saugumą, ar kitas asmuo (asmenų grupė), kuriam (kuriai) Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos informacinės sistemos ir (ar) jos infrastruktūros priežiūros funkcijos.

2.2. **Informacinės sistemos elektroninė informacija** (toliau – elektroninė informacija) – duomenys, dokumentai ir informacija, tvarkomi Registrų centro tvarkomoje informacinėje sistemoje.

2.3. **Informacinės sistemos kibernetinio saugumo ir elektroninės informacijos saugos dokumentai** (toliau – saugos dokumentai) – Saugos nuostatai, Informacinės sistemos „E. sąskaita“ saugaus elektroninės informacijos tvarkymo taisyklės, Informacinės sistemos „E. sąskaita“ veiklos tęstinumo valdymo planas, Informacinės sistemos „E. sąskaita“ naudotojų administravimo taisyklės.

2.4. **Informacinės sistemos kibernetinio saugumo vadovas** (toliau – kibernetinio saugumo vadovas) – informacinės sistemos tvarkytojo paskirtas kompetentingas darbuotojas, atsakingas už informacinės sistemos kibernetinio saugumo organizavimą ir užtikrinimą. Kibernetinio saugumo vadovo funkcijas gali atlikti paskirtas Registrų centro padalinys.

2.5. **Informacinės sistemos komponentai** – kompiuteriai, operacinės sistemos, duomenų bazės ir jų valdymo sistemos, taikomųjų programų sistemos, užkardos, įsilaužimų aptikimo ir prevencijos sistemos, elektroninės informacijos perdavimo tinklai, duomenų saugyklos, serveriai ir kita techninė ir programinė įranga, reikalinga informacinei sistemai funkcionuoti ir joje tvarkomos elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti.

2.6. **Informacinės sistemos naudotojas** (toliau – naudotojas) – Registrų centro darbuotojas, dirbantis pagal darbo sutartį, arba Nacionalinio bendrųjų funkcijų centro pagal darbo sutartį dirbantis darbuotojas, arba kitas asmuo, informacinės sistemos veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją.

2.7. **Informacinės sistemos saugos įgaliotinis** (toliau – saugos įgaliotinis) – informacinės sistemos tvarkytojo paskirtas darbuotojas, dirbantis pagal darbo sutartį, koordinuojantis ir prižiūrintis elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimą informacinėje sistemoje.

2.8. **Vidinis informacinės sistemos naudotojas** (toliau – vidinis naudotojas) – Registrų centro darbuotojas, dirbantis pagal darbo sutartį, arba Nacionalinio bendrųjų funkcijų centro pagal darbo sutartį dirbantis darbuotojas, informacinės sistemos veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją.

2.9. Kitos Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių apraše, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių apraše (toliau – Klasifikavimo gairių aprašas), patvirtintuose 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“, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, ir kituose teisės aktuose bei Lietuvos ir tarptautiniuose „Informacijos technologija. Saugumo metodai“ grupės standartuose.

3. Saugos dokumentų taikymas ir naudojimas:

3.1. Saugos dokumentai taikomi:

3.1.1. Nacionaliniam bendrųjų funkcijų centrui (Geležinio Vilko g. 12, 03163 Vilnius) – informacinės sistemos valdytojui;

3.1.2. Registrų centrui (Lvovo g. 25-101, 09320 Vilnius) – informacinės sistemos tvarkytojui;

3.1.3. saugos įgaliotiniui, kibernetinio saugumo vadovui, administratoriams, naudotojams, informacinei sistemai funkcionuoti reikalingų paslaugų teikėjams;

3.2. Saugos nuostatai yra vieši ir skelbiami Lietuvos Respublikos teisės aktų registre. Informacinės sistemos „E. sąskaita“ saugaus elektroninės informacijos tvarkymo taisyklių, Informacinės sistemos „E. sąskaita“ veiklos tęstinumo valdymo plano, Informacinės sistemos „E. sąskaita“ naudotojų administravimo taisyklių naudojimas yra ribojamas – naudotojams, informacinei sistemai funkcionuoti reikalingų paslaugų teikėjams ir kitiems tretiesiems asmenims suteikiama teisė susipažinti tik su šių saugos dokumentų santrauka Saugos nuostatų V skyriuje „Naudotojų supažindinimo su saugos dokumentais principai“ nustatyta tvarka;

3.3. vadovaujantis būtinumo žinoti principu rengiama saugos dokumentų santrauka, už kurios parengimą atsakingas kibernetinio saugumo vadovas;

3.4. Informacinės sistemos „E. sąskaita“ saugaus elektroninės informacijos tvarkymo taisyklės, Informacinės sistemos „E. sąskaita“ veiklos tęstinumo valdymo planas, Informacinės sistemos „E. sąskaita“ naudotojų administravimo taisyklės turi būti saugiai platinami ir prieinami su jais turinčioms teisę susipažinti suinteresuotoms šalims visais elektroninės informacijos saugos ar kibernetinio saugumo incidentų ar avarijų atvejais.

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

4.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

4.2. informacinės sistemos veiklos tęstinumo užtikrinimas;

4.3. asmens duomenų apsauga;

4.4. naudotojų mokymas;

4.5. organizacinių, techninių, programinių, teisinių, informacijos sklaidos ir kitų priemonių, skirtų elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė.

5. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

5.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti informacinės sistemos elektroninę informaciją;

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

5.3. vykdyti elektroninės informacijos saugos ir kibernetinių incidentų prevenciją, reaguoti į elektroninės informacijos saugos ir kibernetinius incidentus ir juos operatyviai suvaldyti, atkuriant įprastinę informacinės sistemos veiklą.

6. Informacinės sistemos valdytojo funkcijos:

6.1. metodiškai vadovauti Registrų centrui, koordinuoti Registrų centro veiksmus užtikrinant informacinės sistemos funkcionavimą;

6.2. vertinti Registrų centro ir techninės bei programinės įrangos priežiūros paslaugas teikiančio paslaugų teikėjo, veikiančio Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka, paslaugas ir atlikti jo veiklos priežiūrą;

6.3. atlikti elektroninės informacijos tvarkymo ir elektroninės informacijos saugos bei kibernetinio saugumo reikalavimų laikymosi priežiūrą;

6.4. nagrinėti Registrų centro pasiūlymus dėl informacinės sistemos veiklos, elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo;

6.5. priimti sprendimus:

6.5.1. dėl informacinės sistemos veiklos, elektroninės informacijos saugos ir kibernetinio saugumo tobulinimo;

6.5.2. dėl informacinės sistemos techninių ir programinių priemonių, būtinų elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įsigijimo, diegimo ir modernizavimo;

6.5.3. dėl elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo;

6.6. planuoti veiksmingą ir spartų informacinės sistemos pokyčių valdymą;

6.7. pavesti informacinės sistemos tvarkytojui paskirti saugos įgaliotinį ir administratorius;

6.8. prireikus tvirtinti:

6.8.1. rizikos vertinimo ir rizikos valdymo priemonių planą;

6.8.2. grėsmių ir pažeidžiamumų, galinčių turėti įtakos ryšių ir informacinės sistemos kibernetiniam saugumui, rizikos vertinimo (toliau – ryšių ir informacinės sistemos rizikos vertinimas) ataskaitą;

6.8.3. informacinės sistemos informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

6.9. atlikti kitas Saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

7. Informacinės sistemos tvarkytojo funkcijos:

7.1. užtikrinti:

7.1.1. informacinės sistemos nepertraukiamą veiklą;

7.1.2. elektroninės informacijos saugą, kibernetinį saugumą ir saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais (automatiniu būdu);

7.1.3. informacinės sistemos sąveiką su susijusiais registrais ir susijusiomis informacinėmis sistemomis;

7.1.4. tinkamą informacinės sistemos valdytojo sprendimų ir rekomendacijų įgyvendinimą elektroninės informacijos saugos ir kibernetinio saugumo srityje;

7.2. teikti informacinės sistemos valdytojui pasiūlymus dėl elektroninės informacijos saugos ir kibernetinio saugumo gerinimo;

7.3. rengti ir įgyvendinti techninių ir programinių priemonių kūrimo ir plėtros planus, investicinius projektus;

7.4. skirti saugos įgaliotinį, kibernetinio saugumo vadovą ir administratorius;

7.5. ne rečiau kaip kartą per metus organizuoti saugos dokumentų peržiūrą;

7.6. organizuoti naudotojams mokomuosius ir pažintinius kursus elektroninės informacijos tvarkymo klausimais;

7.7. tvirtinti:

7.7.1. rizikos vertinimo ir rizikos valdymo priemonių planą;

7.7.2. ryšių ir informacinės sistemos rizikos vertinimo ataskaitą;

7.7.3. informacinės sistemos informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

7.8. atlikti kitas Saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

8. Už elektroninės informacijos saugą ir kibernetinį saugumą pagal kompetenciją atsako informacinės sistemos valdytojas ir tvarkytojas.

9. Informacinės sistemos valdytojas atsako už elektroninės informacijos saugos ir kibernetinio saugumo politikos formavimą, jos įgyvendinimo organizavimą bei priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

10. Informacinės sistemos tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi saugos dokumentuose nustatyta tvarka.

11. Saugos įgaliotinio funkcijos:

11.1. teikti informacinės sistemos tvarkytojo vadovui pasiūlymus dėl administratorių paskyrimo ir reikalavimų jiems nustatymo;

11.2. organizuoti informacinių technologijų saugos atitikties vertinimą pagal Informacinių technologijų saugos atitikties vertinimo metodiką, patvirtintą Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

11.3. teikti informacinės sistemos valdytojo vadovui pasiūlymus dėl saugos dokumentų priėmimo, keitimo;

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

11.5. teikti administratoriams ir naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimo;

11.6. organizuoti rizikos ir informacinių technologijų saugos atitikties vertinimą;

11.7. atlikti kitas Saugos nuostatuose, kituose teisės aktuose nustatytas ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše saugos įgaliotiniui priskirtas funkcijas.

12. Kibernetinio saugumo vadovas atlieka Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, ir kituose teisės aktuose nustatytas funkcijas. Kibernetinio saugumo vadovas ir saugos įgaliotinis gali būti tas pats asmuo.

13. Saugos įgaliotinis ir kibernetinio saugumo vadovas negali atlikti administratoriaus funkcijų.

14. Administratoriai yra šie:

14.1. koordinuojantysis administratorius – administratorius, kontroliuojantis administratorių veiklą, siekdamas užtikrinti tinkamą administratorių funkcijų vykdymą;

14.2. naudotojų administratorius – administratorius, atliekantis naudotojų teisių valdymo funkcijas (naudotojų duomenų administravimas, klasifikatorių tvarkymas, naudotojų veiksmų registracijos žurnalų įrašų analizė ir kt.);

14.3. informacinės sistemos komponentų administratorius – administratorius, atliekantis funkcijas, susijusias su informacinės sistemos komponentais ir jų sąranka. Informacinės sistemos komponentų administratoriai ir jų funkcijos:

14.3.1. kompiuterių tinklų administratorius:

14.3.1.1. užtikrina kompiuterių tinklų veikimą;

14.3.1.2. projektuoja kompiuterių tinklus;

14.3.1.3. diegia, konfigūruoja ir prižiūri kompiuterių tinklų aktyviąją įrangą;

14.3.1.4. užtikrina kompiuterių tinklų saugumą;

14.3.2. tarnybinių stočių administratorius:

14.3.2.1. užtikrina tarnybinių stočių veikimą;

14.3.2.2. konfigūruoja tarnybinių stočių tinklo prieigą;

14.3.2.3. kuria ir administruoja tarnybinių stočių naudotojų registracijos duomenis;

14.3.2.4. stebi ir analizuoja tarnybinių stočių veiklą;

14.3.2.5. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

14.3.2.6. diegia tarnybinių stočių programinės įrangos atnaujinimus;

14.3.2.7. užtikrina tarnybinių stočių saugą;

14.3.3. duomenų bazių administratorius:

14.3.3.1. užtikrina duomenų bazių veikimą;

14.3.3.2. tvarko duomenų bazių programinę įrangą;

14.3.3.3. kuria ir administruoja duomenų bazių naudotojų registracijos duomenis;

14.3.3.4. kuria ir atkuria atsargines elektroninės informacijos kopijas;

14.3.3.5. stebi duomenų bazes ir optimizuoja jų veikimą;

14.4. saugos administratorius – administratorius, atliekantis funkcijas, susijusias su informacinės sistemos pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena.

15. Administratoriai yra atsakingi už tinkamą saugos dokumentuose nustatytų funkcijų vykdymą.

16. Administratoriai privalo vykdyti visus saugos įgaliotinio ir kibernetinio saugumo vadovo nurodymus ir pavedimus dėl informacinės sistemos saugos ir kibernetinio saugumo užtikrinimo, pagal kompetenciją reaguoti į elektroninės informacijos saugos ir kibernetinio saugumo incidentus ir nuolat teikti saugos įgaliotiniui ir kibernetinio saugumo vadovui informaciją apie pagrindinių saugos užtikrinimo komponentų būklę.

17. Atlikdami informacinės sistemos sąrankos pakeitimus, informacinės sistemos komponentų administratoriai turi laikytis informacinės sistemos pokyčių valdymo tvarkos, nustatytos informacinės sistemos valdytojo tvirtinamose Informacinės sistemos „E. sąskaita“ saugaus elektroninės informacijos tvarkymo taisyklėse.

18. Informacinės sistemos komponentų administratoriai privalo reguliariai patikrinti (peržiūrėti) informacinės sistemos sąranką ir informacinės sistemos būsenos rodiklius – ne rečiau kaip kartą per metus ir (arba) po informacinės sistemos pokyčio.

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

19.1. Lietuvos Respublikos kibernetinio saugumo įstatymas;

19.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

19.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

19.4. 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) (OL 2016 L 119, p. 1);

19.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

19.6. Klasifikavimo gairių aprašas;

19.7. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai;

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

19.9. Lietuvos standartai LST EN ISO/IEC 27002:2017 ir LST EN ISO/IEC 27001:2017 bei kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys informacijos saugą;

19.10. kiti teisės aktai, reglamentuojantys elektroninės informacijos tvarkymą, elektroninės informacijos saugą, kibernetinį saugumą bei informacinės sistemos valdytojo ir tvarkytojų veiklą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

20. Informacinėje sistemoje tvarkoma elektroninė informacija priskiriama svarbios elektroninės informacijos kategorijai. Elektroninė informacija šiai kategorijai priskiriama vadovaujantis Klasifikavimo gairių aprašo 8.2 ir 8.3 papunkčiais.

21. Informacinė sistema pagal joje tvarkomos informacijos svarbą, vadovaujantis Klasifikavimo gairių aprašo 12.2 papunkčiu, priskiriama antrajai kategorijai.

22. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“ ir Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja informacinės sistemos rizikos vertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį informacinės sistemos rizikos vertinimą. Informacinės sistemos tvarkytojo rašytiniu pavedimu informacinės sistemos rizikos vertinimą gali atlikti pats saugos įgaliotinis. Kartu su informacinės sistemos rizikos vertinimu ir (arba) Saugos nuostatų 29 punkte nurodytu informacinių technologijų saugos atitikties vertinimu turi būti atliekamas grėsmių ir pažeidžiamų vietų, galinčių turėti įtakos informacinės sistemos kibernetiniam saugumui, vertinimas.

23. Informacinės sistemos rizikos vertinimo rezultatai išdėstomi rizikos vertinimo ataskaitoje, kuri pateikiama informacinės sistemos valdytojo vadovui ir informacinės sistemos tvarkytojo vadovui. Rizikos vertinimo ataskaita rengiama vertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai yra šie:

23.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingai pateikta elektroninė informacija, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais triktys, programinės įrangos klaidos ar netinkamas veikimas ir kita);

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

23.3. 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.

24. Atsižvelgdamas į rizikos vertinimo ataskaitą, informacinės sistemos valdytojas prireikus tvirtina rizikos vertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

25. Rizikos vertinimo ataskaitos, rizikos vertinimo ir rizikos valdymo priemonių plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo dienos pateikia į Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatuose, patvirtintuose Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

26. Vadovaujantis Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimais, kasmet, arba po esminių organizacinių ar sisteminių pokyčių, organizuojamas Grėsmių ir pažeidžiamumų, galinčių turėti įtakos ryšių ir informacinių sistemų kibernetiniam saugumui, rizikos vertinimas (toliau – ryšių ir informacinės sistemos rizikos vertinimas). Informacinės sistemos tvarkytojo rašytiniu pavedimu ryšių ir informacinės sistemos rizikos vertinimą gali atlikti pats saugos įgaliotinis. Ryšių ir informacinės sistemos rizikos vertinimo metu:

26.1. paskiriamas už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą atsakingas asmuo arba asmenys ir nustatomi jiems taikomi kvalifikaciniai reikalavimai;

26.2. nustatomi reikalavimai rizikos vertinimo procesui, rizikos išdėstymo pagal prioritetus kriterijai ir priimtinas rizikos lygis;

26.3. nustatomos grėsmės ir pažeidžiamumai, galintys turėti įtakos ryšių ir informacinės sistemos kibernetiniam saugumui, ir nustatomos galimos grėsmių ir pažeidžiamumų poveikio vykdomai veiklai sritys;

26.4. įvertinama ryšių ir informacinės sistemos pažeidimo grėsmių tikimybė ir pasekmės, nustatomas rizikos lygis, įvertinamos identifikuotų grėsmių tikimybės ir išdėstomos prioriteto tvarka pagal svarbą, kuri nustatoma atsižvelgiant į atliktą rizikos vertinimą;

26.5. atsižvelgiant į atliktą rizikos vertinimą, rengiami ir (ar) peržiūrimi patvirtinti teisės aktai, reglamentuojantys informacinės sistemos kibernetinio saugumo politiką ir jos įgyvendinimą.

27. Organizuojant ryšių ir informacinės sistemos rizikos vertinimą, rekomenduojama vadovautis Lietuvos ir tarptautiniais standartais ar metodikomis, reglamentuojančiais rizikos valdymą.

28. Ryšių ir informacinės sistemos rizikos vertinimas gali būti atliekamas kartu su informacinės sistemos rizikos vertinimu ar informacinės sistemos informacinių technologijų saugos atitikties vertinimu.

29. Siekiant užtikrinti saugos dokumentuose nustatytų elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų įgyvendinimo organizavimą ir kontrolę, turi būti organizuojami informacinės sistemos informacinių technologijų saugos atitikties vertinimai:

29.1. informacinės sistemos informacinių technologijų saugos atitikties vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip. Ne rečiau kaip kartą per trejus metus informacinės sistemos informacinių technologijų saugos atitikties vertinimą turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinės sistemos auditoriai;

29.2. informacinės sistemos atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatytiems organizaciniams

ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

30. Informacinės sistemos informacinių technologijų saugos atitikties vertinimo metu turi būti atliekamas kibernetinių atakų imitavimas ir vykdomos kibernetinių incidentų imitavimo pratybos. Imituojant kibernetines atakas, rekomenduojama vadovautis tarptautiniu mastu pripažintų organizacijų (pvz., EC-COUNCIL, ISACA, NIST ir kt.) rekomendacijomis ir gerąja praktika.

31. Kibernetinių atakų imitavimas atliekamas etapais:

31.1. planavimo etape parengiamas kibernetinių atakų imitavimo planas, kuriame nurodomi 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, baltosios dėžės ir (arba) pilkosios dėžės), galima neigiama įtaka veiklai, kibernetinių atakų imitavimo metodologija, programiniai ir (arba) techniniai įrankiai ir priemonės, nurodomi už plano vykdymą atsakingi asmenys ir jų kontaktai. Kibernetinių atakų imitavimo planas turi būti suderintas su informacinių sistemų tvarkytojo vadovu ir vykdomas tik gavus jo raštišką pritarimą;

31.2. žvalgybos ir aptikimo etape surenkama informacija apie tinklo perimetrą, tinklo mazgus, tinklo mazguose veikiančių serverių ir kitų tinklo įrenginių operacines sistemas ir programinę įrangą, paslaugas, pažeidžiamas vietas, konfigūracijas ir kitą sėkmingai kibernetinei atakai įvykdyti reikalingą informaciją. Šiame etape turi būti teikiamos tarpinės vykdomų veiklų ir jų rezultatų ataskaitos;

31.3. kibernetinių atakų imitavimo etape atliekami kibernetinių atakų imitavimo plane numatyti darbai. Šiame etape turi būti teikiamos tarpinės vykdomų veiklų ir jų rezultatų ataskaitos;

31.4. ataskaitos parengimo etape kibernetinių atakų imitavimo rezultatai turi būti išdėstomi informacinių technologijų saugos atitikties vertinimo ataskaitoje: darbų rezultatai turi būti detalizuojami ir palyginami su planuotais kibernetinių atakų imitavimo plane, kiekviena aptikta pažeidžiama vieta turi būti detalizuojama ir pateikiamos rekomendacijos pažeidžiamumui pašalinti. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos vertinimu. Jeigu nustatoma incidentų valdymo ir šalinimo ar organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinami veiklos tęstinumo planai.

32. Informacinės sistemos saugos atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka.

33. Atlikus informacinių technologijų saugos atitikties vertinimą, saugos įgaliotinis rengia ir informacinės sistemos tvarkytojo vadovui teikia informacinių technologijų saugos atitikties vertinimo ataskaitą. Atsižvelgdamas į informacinių technologijų saugos atitikties vertinimo ataskaitą, saugos įgaliotinis prireikus parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinės sistemos valdytojo vadovas.

34. Informacinių technologijų saugos atitikties vertinimo ataskaitos ir pastebėtų trūkumų šalinimo plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia į Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

35. Siekiant gerinti elektroninės informacijos saugos ir kibernetinio saugumo būklę, techninės, programinės, organizacinės ir kitos elektroninės informacijos saugos ir kibernetinio saugumo priemonės pasirenkamos atsižvelgiant į informacinės sistemos valdytojo turimus išteklius ir vadovaujantis šiais principais:

35.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

35.2. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei;

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

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

36. Informacinėje sistemoje naudojamų svetainių saugos valdymo reikalavimai:

36.1. svetainės turi atitikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimus, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimus;

36.2. svetainių užkardos turi būti sukonfigūruotos taip, kad prie svetainių turinio valdymo sistemų būtų galima jungtis tik iš vidinio informacinės sistemos tvarkytojo kompiuterių tinklo arba nustatytų IP adresų;

36.3. turi būti pakeisti numatytieji (angl. *default*) prisijungimo prie svetainių turinio valdymo sistemų ir administravimo skydų (angl. *panel*) slaptažodžiai ir nuorodos (angl. *default path*);

36.4. turi būti užtikrinama, kad prie svetainių turinio valdymo sistemų ir administravimo skydų būtų galima jungtis tik naudojantis šifruotuoju ryšiu;

36.5. informacinėje sistemoje naudojamų svetainių sauga turi būti vertinama informacinės sistemos rizikos įvertinimo, ryšių ir informacinės sistemos rizikos vertinimo ir (arba) informacinės sistemos informacinių technologijų saugos atitikties vertinimo, atliekamų Saugos nuostatų II skyriuje nustatyta tvarka, metu.

37. Programinės įrangos, skirtos informacinei sistemai apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

37.1. tarnybinėse stotyse ir vidinių naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo, stebėjimo realiuoju laiku priemonės;

37.2. informacinės sistemos komponentai be kenksmingos programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu rizikos vertinimo ar ryšių ir informacinės sistemos rizikos vertinimo metu yra patvirtinama, kad šių komponentų rizika yra priimtina;

37.3. kenksmingos programinės įrangos aptikimo priemonės turi atsinaujinti automatiškai ne rečiau kaip kartą per 24 valandas. Informacinės sistemos komponentų administratorius turi būti automatiškai informuojamas elektroniniu paštu apie tai, kurių informacinės sistemos posistemių, funkciškai savarankiškų sudedamųjų dalių, vidinių naudotojų kompiuterių ir kitų informacinės sistemos komponentų kenksmingos programinės

įrangos aptikimo priemonių atsinaujinimo laikas yra pradelstas, ir apie tai, kad kenksmingos programinės įrangos aptikimo priemonės funkcionuoja netinkamai arba yra išjungtos.

38. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

38.1. informacinės sistemos tarnybinėse stotyse ir vidinių naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga;

38.2. vidinių naudotojų kompiuteriuose naudojama programinė įranga turi būti įtraukta į suderintą su informacinės sistemos valdytoju leidžiamos naudoti programinės įrangos sąrašą, kurį turi parengti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti saugos įgaliotinis;

38.3. ne rečiau kaip kartą per mėnesį turi būti įvertinami tarnybinių stočių ir vidinių naudotojų kompiuterių operacinės sistemos kibernetiniam saugumui užtikrinti naudojamų priemonių ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai, klaidų pataisymai turi būti operatyviai išbandomi ir įdiegiami;

38.4. saugos administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius informacinės sistemos posistemiuose, funkciškai savarankiškose sudedamosiose dalyse, vidinių naudotojų kompiuteriuose. Apie įvertinimo rezultatus saugos administratorius turi informuoti saugos įgaliotinį ir kibernetinio saugumo vadovą;

38.5. programinė įranga turi būti prižiūrima ir atnaujinama laikantis gamintojo reikalavimų ir rekomendacijų;

38.6. programinės įrangos diegimą, konfigūravimą, priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai – informacinės sistemos komponentų administratoriai arba tokias paslaugas teikiantys paslaugų teikėjai;

38.7. programinė įranga turi būti testuojama naudojant atskirą testavimo aplinką, kurioje neturi būti naudojami realūs asmens duomenys, arba užtikrinamos kitos priemonės saugiam tokių duomenų naudojimui;

38.8. informacinės sistemos programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL intarpų įterpimas, įterptinių instrukcijų (XSS) atakų, internetinės paslaugos sutrikdymo (DoS) atakų, srautinių internetinės paslaugos sutrikdymo (DDoS) atakų ir kitų. Pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto interneto svetainėje www.owasp.org.

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

39.1. kompiuterių tinklai turi būti atskirti nuo viešųjų elektroninių ryšių tinklų (interneto) naudojant užkardas, automatinę įsilaužimų aptikimo ir prevencijos įrangą, apsaugos nuo internetinės paslaugos sutrikdymo atakų ir srautinių internetinės paslaugos sutrikdymo atakų įrangą;

39.2. kompiuterių tinklų perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešuosiuose ryšių tinkluose naršančių vidinių naudotojų kompiuterinę įrangą nuo kenksmingo kodo. Visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

39.3. apsaugai nuo elektroninės informacijos nutekinimo turi būti naudojama duomenų srautų analizės ir kontrolės įranga;

39.4. turi būti naudojamos turinio filtravimo sistemos;

39.5. turi būti naudojamos taikomųjų programų kontrolės sistemos.

40. Leidžiamos kompiuterių naudojimo ribos:

40.1. stacionariuosius kompiuterius leidžiama naudoti tik informacinės sistemos valdytojo ir informacinės sistemos tvarkytojo patalpose;

40.2. nešiojamiesiems kompiuteriams, išnešamiems iš informacinės sistemos valdytojo ar informacinės sistemos tvarkytojo patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimai ir pan.);

40.3. iš stacionariųjų ir nešiojamųjų kompiuterių ar elektroninės informacijos laikmenų, kurie perduodami remonto ar techninės priežiūros paslaugų teikėjui arba nurašomi, turi būti nebeatkuriamai pašalinta visa nevieša elektroninė informacija.

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

41.1. elektroninė informacija teikiama Informacinės sistemos „E. sąskaita“ nuostatuose nustatyta tvarka;

41.2. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą naudojamas šifravimas, virtualusis privatusis tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas. Elektroninės informacijos teikimui ir (ar) gavimui gali būti naudojamas saugus valstybinis duomenų perdavimo tinklas;

41.3. elektroninė informacija automatiniu būdu turi būti teikiama ir (ar) gaunama tik pagal Informacinės sistemos „E. sąskaita“ nuostatuose, elektroninės informacijos teikimo (keitimosi ja) sutartyse nustatytas specifikacijas ir sąlygas;

41.4. nuotolinis prisijungimas prie informacinės sistemos galimas:

41.4.1. naudojant transporto lygmens protokolus (TLS), reglamentuojančius abipusį tapatumo nustatymą tarp naudotojo ir serverio, kad būtų užtikrintas šifruotasis ryšys. Saugiam elektroninės informacijos perdavimui tarp serverio ir interneto naršyklės naudojamas TLS sertifikatas, patvirtinantis elektroninės informacijos šaltinio tapatumą ir šifruojantis tarp naudotojo ir serverio siunčiamą elektroninę informaciją. Informacinės sistemos interneto svetainėse TLS šifruota HTTP protokolo elektroninė informacija perduodama saugiu HTTPS protokolu;

41.4.2. naudojant virtualųjį privatųjį tinklą. Virtualiajame tinkle turi būti naudojamas IPsec protokolų rinkinys;

41.4.3. naudojant saugaus apvalkalo (angl. *Secure Shell*) protokolą ir nuotolinio darbalaukio protokolą. Šia galimybe gali būti pasinaudota tik informacinės sistemos administravimo tikslais;

41.5. šifro raktų ilgiai, šifro raktų generavimo algoritmai, šifro raktų apsikeitimo protokolai, sertifikato parašo šifravimo algoritmai bei kiti šifravimo algoritmai turi būti nustatomi atsižvelgiant į Lietuvos ir tarptautinių organizacijų bei standartų rekomendacijas, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimus, Techninius valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimus;

41.6. naudojamų šifravimo priemonių patikimumas turi būti vertinamas atliekant neeilinį arba kasmetinį informacinės sistemos rizikos vertinimą ar ryšių ir informacinės sistemos rizikos vertinimą. Šifravimo priemonės turi būti operatyviai keičiamos nustačius saugumo spragų šifravimo algoritmuose.

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

42.1. atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į priimtiną elektroninės informacijos praradimą ir priimtiną informacinės sistemos neveikimo laikotarpį;

42.2. atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokia apimtimi, kad informacinės sistemos veiklos sutrikimo, elektroninės informacijos saugos ar kibernetinio incidento arba elektroninės informacijos vientisumo praradimo atvejais informacinės sistemos neveikimo laikotarpis nebūtų ilgesnis, nei numatytas antros kategorijos informacinei sistemai, o elektroninės informacijos praradimas atitiktų priimtinumo kriterijus;

42.3. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai ir periodiškai ne rečiau kaip atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarkos, nustatytos informacinės sistemos saugaus elektroninės informacijos taisyklėse, nurodytais terminais;

42.4. elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių neteisėtai atkurti elektroninės informacijos;

42.5. atsarginių elektroninės informacijos kopijų laikmenos turi būti žymimos taip, kad jas būtų galima identifikuoti, ir saugomos nedegioje spintoje kitose patalpose, nei yra informacinės sistemos tarnybinės stotys ar įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate. Atsarginių elektroninės informacijos kopijų žymėjimo tvarka ir saugojimo terminai nustatyti Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarkos aprašyme;

42.6. atsarginių elektroninės informacijos kopijų darymas turi būti fiksuojamas;

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

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

43. Informacinės sistemos valdytojas ir (arba) informacinės sistemos tvarkytojas, pirkdamas paslaugas, darbus ar prekes, susijusias su informacine sistema, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimams.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

44. Naudotojų, administratorių, saugos įgaliotinio ir kibernetinio saugumo vadovo kvalifikacijos ir patirties reikalavimai:

44.1. naudotojų, administratorių, saugos įgaliotinio, kibernetinio saugumo vadovo kvalifikacija turi atitikti bendruosius ir specialiuosius reikalavimus, nustatytus jų pareiginiuose nuostatuose;

44.2. visi naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais,

reglamentuojančiais asmens duomenų ir elektroninės informacijos tvarkymą. Asmenys, tvarkantys asmens duomenis ir informaciją, privalo būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį ir jo laikytis. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą;

44.3. saugos įgaliotinis ir kibernetinio saugumo vadovas privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, tobulinti elektroninės informacijos saugos ir kibernetinio saugumo srities kvalifikaciją, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą ir kibernetinį saugumą. Informacinės sistemos tvarkytojas turi sudaryti sąlygas kelti saugos įgaliotinio ir kibernetinio saugumo vadovo kvalifikaciją;

44.4. saugos įgaliotiniu ir kibernetinio saugumo vadovu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinės sistemos saugumui, paskirtą 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, už savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai;

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

45. Saugos įgaliotinio, kibernetinio saugumo vadovo, naudotojų ir administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

45.1. saugos įgaliotiniui, kibernetinio saugumo vadovui, naudotojams ir administratoriams turi būti organizuojami mokymai elektroninės informacijos saugos ir kibernetinio saugumo klausimais;

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

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

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

45.5. naudotojų ir administratorių mokymus gali vykdyti saugos įgaliotinis ar kitas informacinės sistemos valdytojo ar informacinės sistemos tvarkytojo darbuotojas, išmanantis

elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, arba elektroninės informacijos saugos ir kibernetinio saugumo mokymų paslaugų teikėjas. Saugos įgaliotinio ir kibernetinio saugumo vadovo mokymus gali vykdyti tik aukštos kvalifikacijos elektroninės informacijos saugos ir kibernetinio saugumo mokymų paslaugų teikėjas;

45.6. naudotojų mokymai turi būti organizuojami periodiškai, ne rečiau kaip kartą per dvejus metus. Saugos įgaliotinio, kibernetinio saugumo vadovo ir administratorių mokymai turi būti organizuojami pagal poreikį. Už mokymų organizavimą atsakingas saugos įgaliotinis.

V SKYRIUS
NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

46. Naudotojų supažindinimą su saugos dokumentais ar jų santrauka, atsakomybe už saugos dokumentų nuostatų pažeidimus organizuoja saugos įgaliotinis.

47. Informacinės sistemos naudotojų supažindinimo su saugos dokumentais ar jų santrauka būdai turi būti pasirenkami atsižvelgiant į informacinės sistemos specifiką (pvz., informacinės sistemos ir jos naudotojų lokaciją, organizacinių ar techninių priemonių, leidžiančių identifikuoti su saugos dokumentais ar jų santrauka susipažinusį asmenį ir užtikrinančių supažindinimo procedūros įrodomąją (teisinę) galią, panaudojimo galimybes ir pan.). Naudotojai su saugos dokumentais ar jų santrauka turi būti supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą.

48. Pakartotinai su saugos dokumentais ar jų santrauka naudotojai supažindinami tik iš esmės pasikeitus informacinėms sistemoms arba elektroninės informacijos saugą ir kibernetinį saugumą reglamentuojantiems teisės aktams.

49. Tvarkyti elektroninę informaciją gali tik tie asmenys, kurie yra susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų.

50. Naudotojai atsako už informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą pagal savo kompetenciją. Naudotojai, administratoriai ir saugos įgaliotinis, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

51. Informacinės sistemos valdytojas saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Saugos dokumentai turi būti derinami su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką. Keičiami saugos dokumentai gali būti nederinami su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką, tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos ir kibernetinio saugumo politikos nekeičiantys pakeitimai arba pakeitimai, susiję su teisės technika.

52. Patvirtinęs Saugos nuostatus ar jų pakeitimus, informacinės sistemos valdytojas Registrų ir valstybės informacinių sistemų registro nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2012 m. spalio 16 d. nutarimu Nr. 1263 „Dėl Registrų sąrašo reorganizavimo į Registrų ir valstybės informacinių sistemų registrą ir Registrų ir valstybės informacinių

sistemų registro nuostatų patvirtinimo“, nustatyta tvarka pateikia šiam registrui reikiamus duomenis ar dokumentų kopijas.

53. Patvirtintų saugos dokumentų ir jų pakeitimų kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai krašto apsaugos ministro patvirtintų valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

54. Informacinės sistemos tvarkytojas saugos dokumentus turi persvarstyti (peržiūrėti) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos vertinimą, ryšių ir informacinės sistemos rizikos vertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems informacinės sistemos valdytojo ar tvarkytojo pokyčiams.

_____