LIETUVOS RESPUBLIKOS FINANSŲ MINISTRAS

ĮSAKYMAS DĖL FINANSŲ MINISTRO 2012 M. RUGSĖJO 6 D. ĮSAKYMO NR. 1K-297 „DĖL INFORMACINĖS SISTEMOS „E. SĄSKAITA“ NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2016 m. gegužės 4 d. Nr. 1K-166
Vilnius

P a k e i č i u Lietuvos Respublikos finansų ministro 2012 m. rugsėjo 6 d. įsakymą Nr. 1K-297 „Dėl Informacinės sistemos „E. sąskaita“ nuostatų patvirtinimo“:

1. Pakeičiu preambulę ir ją išdėstau taip:

„Vadovaudamasis Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, 11 punktu ir 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 19 ir 26 punktais:“.

2. Pakeičiu 3 punktą ir jį išdėstau taip:

„3. P a v e d u informacinės sistemos „E. sąskaita“ tvarkytojui:

3.1. paskirti informacinės sistemos „E. sąskaita“ saugos įgaliotinį ir administratorius;

3.2. iki 2016 m. gegužės 15 d. parengti ir pateikti Lietuvos Respublikos finansų ministerijai informacinės sistemos „E. sąskaita“ duomenų saugos politikos įgyvendinimo dokumentus:

3.2.1. Informacinės sistemos „E. sąskaita“ saugaus elektroninės informacijos tvarkymo taisyklių projektą;

3.2.2. Informacinės sistemos „E. sąskaita“ veiklos tęstinumo valdymo plano projektą;

3.2.3. Informacinės sistemos „E. sąskaita“ naudotojų administravimo taisyklių projektą.“

3. Pakeičiu nurodytuoju įsakymu patvirtintus Informacinės sistemos „E. sąskaita“ duomenų saugos nuostatus ir juos išdėstau nauja redakcija (pridedama).

Finansų ministras Rimantas Šadžius

PATVIRTINTA
Lietuvos Respublikos finansų ministro
2012 m. rugsėjo 6 d. įsakymu Nr. 1K-297
(Lietuvos Respublikos finansų ministro
2016 m. gegužės 4 d. įsakymo Nr. 1K-166
redakcija)

INFORMACINĖS SISTEMOS „E. SĄSKAITA“ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacinės sistemos „E. sąskaita“ duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja informacinės sistemos „E. sąskaita“ duomenų (toliau – Informacinė sistema) duomenų saugos politiką, nustato organizacines, technines, programines, teisines ir kitas priemones, užtikrinančias saugų Informacinės sistemos duomenų tvarkymą.

2. Saugos nuostatų tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti Informacinės sistemos duomenis, užtikrinti elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei tinklo įrangos veikimą. Informacinės sistemos duomenų saugai užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo, atsakomybės, elektroninės informacijos saugos suvokimo kėlimo ir saugos priemonių projektavimo bei diegimo principus.

3. Saugos nuostatuose vartojamos sąvokos:

3.1. **Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentai** – Lietuvos Respublikos finansų ministro patvirtinti dokumentai: Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės, Informacinės sistemos veiklos tęstinumo valdymo planas, Informacinės sistemos naudotojų administravimo taisyklės.

3.2. Kitos šiuose Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme (toliau – Valstybės informacinių išteklių įstatymas), 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Saugos reikalavimų aprašas), vartojamas sąvokas.

4. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Informacinės sistemos duomenų saugai užtikrinti, įgyvendinimas ir kontrolė;

4.2. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

4.3. Informacinės sistemos veiklos tęstinumo užtikrinimas;

4.4. asmens duomenų apsauga;

4.5. Informacinės sistemos naudotojų mokymas.

5. Informacinės sistemos valdytojo ir tvarkytojo pavadinimai ir adresai:

5.1. Informacinės sistemos valdytojas – Lietuvos Respublikos finansų ministerija, buveinės adresas Lukiškių g. 2, LT-01104 Vilnius;

5.2. Informacinės sistemos tvarkytojas – valstybės įmonė Registrų centras (toliau – Registrų centras), buveinės adresas Vinco Kudirkos g. 18-3, 03105 Vilnius.

6. Informacinės sistemos valdytojo funkcijos ir atsakomybė:

6.1. tvirtina Informacinės sistemos duomenų saugos politiką reglamentuojančius teisės aktus;

6.2. kontroliuoja, kaip laikomasi Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentų ir kitų teisės aktų, reglamentuojančių Informacinės sistemos duomenų tvarkymo teisėtumą ir saugos valdymą;

6.3. priima sprendimus dėl Informacinės sistemos techninių ir programinių priemonių, būtinų Informacinės sistemos duomenų saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

6.4. prižiūri, kaip laikomasi Informacinės sistemos duomenų ir elektroninės informacijos saugos reikalavimų;

6.5. nagrinėja Informacinės sistemos tvarkytojo pasiūlymus dėl Informacinės sistemos saugos tobulinimo ir priima dėl jų sprendimus;

6.6. priima sprendimą atlikti Informacinės sistemos informacinių technologijų saugos reikalavimų atitikties vertinimą;

6.7. vykdo kitas Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentuose ir kituose teisės aktuose, reglamentuojančiuose Informacinės sistemos duomenų tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas;

6.8. atsako už Informacinės sistemos duomenų tvarkymo, teikimo ir (ar) gavimo teisėtumą ir saugą.

7. Informacinės sistemos tvarkytojo funkcijos:

7.1. teikia pasiūlymus Informacinės sistemos valdytojui, kaip tobulinti Informacinės sistemos saugą;

7.2. vykdo Informacinės sistemos valdytojo priimtus teisės aktus ir įgyvendina rekomendacijas;

7.3. užtikrina nepertraukiamą Informacinės sistemos veikimą ir elektroninės informacijos saugą, taip pat saugų elektroninės informacijos perdavimą kompiuterių tinklais (automatiniu būdu);

7.4. užtikrina Informacinės sistemos sąveiką su kitomis informacinėmis sistemomis ir registrais;

7.5. skiria Informacinės sistemos saugos įgaliotinį ir Informacinės sistemos administratorių.

8. Informacinės sistemos tvarkytojo vadovas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentuose nustatyta tvarka.

9. Saugos įgaliotinio funkcijos ir atsakomybė:

9.1. rengia duomenų saugos politikos įgyvendinimo dokumentų projektus;

9.2. teikia Informacinės sistemos valdytojo vadovui pasiūlymus dėl:

9.2.1. duomenų saugos politikos įgyvendinimo dokumentų priėmimo, keitimo ar panaikinimo;

9.2.2. informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

9.3. teikia Registrų centro vadovui pasiūlymus dėl Informacinės sistemos administratoriaus paskyrimo ir reikalavimų jam nustatymo;

9.4. koordinuoja elektroninės informacijos saugos incidentų tyrimą, išskyrus atvejus, kai šią funkciją atlieka informacijos saugos darbo grupė;

9.5. kasmet organizuoja kasmetinius ir prireikus neeilinius Informacinės sistemos rizikos vertinimus;

9.6. teikia Informacinės sistemos administratoriui privalomus vykdyti nurodymus ir pavedimus, susijusius su Informacinės sistemos saugos politikos įgyvendinimu;

9.7. supažindina Informacinės sistemos naudotojus ir Informacinės sistemos administratorių su Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, bei atsakomybe už šiuose dokumentuose nustatytų reikalavimų nesilaikymą;

9.8. periodiškai inicijuoja Informacinės sistemos naudotojų supažindinimą su informacijos sauga, siųsdamas priminimus ir konsultuodamas elektroniniu paštu ar per Registrų centro intraneto svetainę;

9.9. atsako už Informacinės sistemos duomenų saugos politikos įgyvendinimo organizavimą;

9.10. atsako už Informacinės sistemos saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

9.11. vykdo kitas Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentuose ir kituose teisės aktuose, reglamentuojančiuose Informacinės sistemos duomenų tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas.

10. Informacinės sistemos priežiūrą atlieka administratoriai: kompiuterių tinklo administratorius, tarnybinių stočių administratorius, duomenų bazių administratorius ir naudotojų administratorius. Pagal einamas pareigas ir prieigos prie Informacinės sistemos lygį:

10.1. Kompiuterių tinklo administratorius atlieka šias funkcijas:

10.1.1. užtikrina kompiuterių tinklo veikimą;

10.1.2. projektuoja kompiuterių tinklą;

10.1.3. diegia, konfigūruoja ir prižiūri kompiuterių tinklo aktyviąją įrangą;

10.1.4. užtikrina kompiuterių tinklo saugumą.

10.2. Tarnybinių stočių administratorius atlieka šias funkcijas:

10.2.1. užtikrina tarnybinių stočių veikimą;

10.2.2. konfigūruoja tarnybinių stočių tinklo prieigą;

10.2.3. kuria ir administruoja tarnybinių stočių naudotojų registracijos į tarnybines stotis duomenis;

10.2.4. stebi ir analizuoja tarnybinių stočių veiklą;

10.2.5. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

10.2.6. atnaujina tarnybinių stočių programinę įrangą;

10.2.7. užtikrina tarnybinių stočių saugą.

10.3. Duomenų bazių administratorius atlieka šias funkcijas:

10.3.1. užtikrina duomenų bazių veikimą;

10.3.2. tvarko duomenų bazių programinę įrangą;

10.3.3. konfigūruoja duomenų bazių kompiuterių tinklo aplinką;

10.3.4. kuria ir administruoja duomenų bazių naudotojų registracijos į duomenų bazes duomenis;

10.3.5. kuria ir atkuria atsargines elektroninės informacijos kopijas;

10.3.6. stebi duomenų bazes ir optimizuoja jų veikimą.

10.4. Naudotojų administratorius atlieka šias funkcijas:

10.4.1. administruoja Informacinės sistemos naudotojų duomenis;

10.4.2. tvarko Informacinės sistemos naudotojų klasifikatorius;

10.4.3. analizuoja Informacinės sistemos naudotojų veiksmų registracijos žurnalų įrašus.

11. Administratoriai, vykdydami Informacinės sistemos priežiūrą, yra atsakingi už tinkamą Saugos nuostatuose nustatytų funkcijų vykdymą.

12. Informacinės sistemos duomenys tvarkomi ir jų sauga užtikrinama vadovaujantis:

12.1. Valstybės informacinių išteklių valdymo įstatymu;

12.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau – Asmens duomenų teisinės apsaugos įstatymas);

12.3. Lietuvos Respublikos kibernetinės saugos įstatymu;

12.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

12.5. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – IS klasifikavimo gairių aprašas);

12.6. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 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“;

12.7. Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“ (toliau – Bendrieji reikalavimai duomenų saugumo priemonėms);

12.8. Lietuvos standartais LST ISO/IEC 27001:2013 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2014 „Informacijos technologija. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“;

12.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

12.10. kitais teisės aktais, kuriais reglamentuojamas elektroninės informacijos tvarkymo teisėtumas, Informacinės sistemos valdytojo ir tvarkytojo veikla ir elektroninės informacijos saugos valdymas.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Informacinėje sistemoje tvarkoma elektroninė informacija, vadovaujantis IS klasifikavimo gairių aprašo 4.2.4, 4.5.5 ir 4.2.7 papunkčiais, priskiriama svarbios elektroninės informacijos kategorijai.

14. Informacinė sistema, atsižvelgiant į joje apdorojamos elektroninės informacijos svarbą, priskiriama antrajai kategorijai, vadovaujantis IS klasifikavimo gairių aprašo 5.2 papunkčiu.

15. Informacinėje sistemoje tvarkomi asmens duomenys automatiniu būdu priskiriami antrajam saugumo lygiui, vadovaujantis Bendrųjų reikalavimų duomenų saugumo priemonėms 7.2 papunkčiu.

16. Informacinės sistemos saugos įgaliotinis, vadovaudamasis Lietuvos Respublikos vidaus reikalų ministerijos išleistu metodiniu leidiniu „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, kasmet organizuoja Informacinės sistemos rizikos vertinimą, o prireikus ir neeilinį šios rizikos vertinimą.

17. Informacinės sistemos rizikos įvertinimo rezultatai įforminami Informacinės sistemos rizikos įvertinimo ataskaita. Informacinės sistemos rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos Informacinės sistemos informacijos saugai. Informacinės sistemos rizikos įvertinimo ataskaita pateikiama Informacinės sistemos valdytojo vadovui.

18. Svarbiausi Informacinės sistemos rizikos veiksniai yra šie:

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

18.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Informacine sistema siekiant gauti jos duomenų, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

18.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

19. Atsižvelgdamas į Informacinės sistemos rizikos įvertinimo ataskaitą, Informacinės sistemos valdytojas prireikus tvirtina Informacinės sistemos rizikos įvertinimo ir rizikos valdymo

priemonių planą, kuriame numatomas techninių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

20. Informacinės sistemos saugos įgaliotinis ne rečiau kaip vieną kartą per dvejus metus organizuoja Informacinės sistemos informacinių technologijų saugos atitikties vertinimą, kurio metu:

20.1. įvertinama, ar Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentai atitinka realią informacijos saugos situaciją;

20.2. inventorizuojama Informacinės sistemos techninė ir programinė įranga;

20.3. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų Informacinės sistemos naudotojų kompiuterinių darbo vietų, visose tarnybinėse stotyse įdiegtos programos ir jų sąranga;

20.4. įvertinama Informacinės sistemos naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;

20.5. įvertinamas pasirengimas užtikrinti Informacinės sistemos veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui.

21. Atlikus Informacinės sistemos informacinių technologijų saugos atitikties vertinimą, Informacinės sistemos saugos įgaliotinis rengia ir Informacinės sistemos valdytojui teikia Informacinės sistemos informacinių technologijų saugos atitikties vertinimo ataskaitą.

22. Atsižvelgdamas į Informacinės sistemos informacinių technologijų saugos atitikties vertinimo ataskaitą, Informacinės sistemos saugos įgaliotinis prireikus parengia pastebėtų trūkumų šalinimo planą. Šį planą tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Informacinės sistemos valdytojo vadovas.

23. Patvirtintų Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentų ir jų pakeitimų kopijas Informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo dienos pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ (toliau – Valstybės informacinių išteklių atitikties stebėsenos sistemos nuostatai), nustatyta tvarka.

24. Techninės, programinės ir organizacinės Informacinės sistemos elektroninės informacijos saugos priemonės pasirenkamos atsižvelgiant į Informacinės sistemos valdytojo turimus išteklius, vadovaujantis šiais priemonių parinkimo principais:

24.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

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

24.3. kur galima, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

25. Informacinės sistemos rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano, saugos atitikties vertinimo ataskaitos ir pastebėtų trūkumų šalinimo plano kopijas Informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo dienos pateikia Valstybės informacinių išteklių atitikties stebėsenos sistemos nuostatų nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

26. 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:

26.1. tarnybinėse stotyse ir kompiuterinėse darbo vietose, kuriose naudojama „Microsoft Windows“ operacinė sistema, privalo būti įdiegta centralizuotai valdoma, apsaugai nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos ir kt.) naudojama programinė įranga;

26.2. elektroninio pašto tarnybinės stotys turi būti apsaugotos nuo brukalų ir nepageidaujamo turinio elektroninių laiškų;

26.3. kompiuterinėse darbo vietose turi būti įdiegtos priemonės, leidžiančios riboti USB ir kito tipo laikmenų naudojimą;

26.4. apsaugai naudojama programinė įranga privalo atsinaujinti ne rečiau kaip kartą per 24 valandas;

26.5. apsaugai naudojama programinė įranga privalo automatiškai elektroniniu paštu informuoti atsakingus Informacinės sistemos naudotojus apie kompiuterines darbo vietas ir tarnybines stotis, kuriose apsaugos sistema netinkamai veikia, yra išjungta arba neatsinaujino per 24 valandas;

26.6. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

27. Informacinės sistemos programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

27.1. naudojama tik legali programinė įranga;

27.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

27.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka tik tarnybinių stočių administratorius.

28. Informacinės sistemos kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių ir kt.) pagrindinės naudojimo nuostatos:

28.1. kompiuterių tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

28.2. visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

28.3. naudojamos turinio filtravimo sistemos;

28.4. naudojamos aplikacijų kontrolės sistemos.

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

29.1. nuotolinis prisijungimas prie Informacinės sistemos galimas:

29.1.1. iš virtualiųjų darbo vietų naudojant „PCoIP“ protokolą. Nutolusiame kompiuteryje įdiegiama speciali programinė įranga „Vmware view client“ ir jungiamasi per specializuotą tarnybinę stotį (securitysrv.kada.lt) naudojant HTTPS protokolą;

29.1.2. naudojantis „IPSec“ protokolų rinkiniu ir jungiantis kaip „IPSec“ programiniam klientui;

29.1.3. naudojant šifruotą komandinės eilutės protokolą SSH. Šia galimybe gali būti pasinaudota tik Informacinės sistemos administravimo tikslais;

29.2. prieiga prie Informacinės sistemos yra ribojama ugniasienėmis;

29.3. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą į Informacinę sistemą iš kitų valstybės institucijų, naudojami saugūs ryšio kanalai. Informacijai perduoti gali būti naudojamas Saugus valstybinis duomenų perdavimo tinklas;

29.4. teikti ir (ar) gauti elektroninę informaciją į Informacinę sistemą automatiniu būdu galima tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas – naudojami saugūs ryšio kanalai (VPN).

30. Nešiojamieji kompiuteriai, kuriuose saugomi su Informacine sistema susiję duomenys, naudojami tik Registrų centro patalpose. Jie, kaip ir stacionarūs kompiuteriai, turi būti apsaugoti prisijungimo vardu ir slaptažodžiu.

31. Pagrindiniai atsarginių Informacinės sistemos elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

31.1. atsarginės elektroninės informacijos kopijos (toliau – kopijos) daromos automatiškai kiekvieną dieną;

31.2. elektroninė informacija kopijose turi būti užšifruota;

31.3. laikmena, kurioje yra kopija, pažymima specialia ženklinimo etikete, kurioje nurodoma kopijavimo data, kopiją padariusio asmens duomenys (pareigos, vardas, pavardė), duomenų katalogai;

31.4. kiekvienos savaitės (mėnesio, metų) paskutinės kopijos ženklinimo etiketėje papildomai nurodoma, kad tai yra savaitinė (mėnesinė, metinė) kopija;

31.5. kopijas turi teisę daryti tik duomenų bazių administratorius, kurio pareigybės aprašyme nurodyta ši funkcija;

31.6. laikmenos, kuriose yra kopijos, saugomos Registrų centro patalpose, atskirai nuo tarnybinių stočių. Už jų atidavimą saugoti atsako administratorius, vykdantis dokumentų kopijavimo funkciją;

31.7. atsarginės metinės kopijos saugomos 10 metų nuo jų sukūrimo dienos. Atsarginės mėnesinės kopijos saugomos 1 metus nuo jų sukūrimo dienos. Atsarginės savaitinės kopijos saugomos 1 mėnesį nuo jų sukūrimo dienos;

31.8. atkurti elektroninę informaciją iš kopijų turi teisę tik duomenų bazių administratorius;

IV SKYRIUS
REIKALAVIMAI PERSONALUI

32. Informacinės sistemos saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentų, standartų ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, būti susipažinęs su esminiais Informacinės sistemos duomenų saugos reikalavimais, turėti saugos politikai įgyvendinti reikiamą kvalifikaciją.

33. Informacinės sistemos saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat 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, savavališką prisijungimą arba

elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jo paskyrimo praėję mažiau kaip vieni metai.

34. Informacinės sistemos administratoriai privalo išmanyti informacijos saugos principus, mokėti užtikrinti jų saugą, administruoti ir prižiūrėti duomenų bazes, turi būti susipažinę su Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentais, darbo saugos taisyklėmis. Informacinės sistemos administratoriai privalo sugebėti užtikrinti nepertraukiamą techninės ir programinės įrangos veikimą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų diagnostiką ir šalinimą, išmanyti elektroninės informacijos saugos užtikrinimo principus.

35. Informacinės sistemos naudotojai privalo turėti pagrindinius darbo su kompiuteriu įgūdžius, mokėti tvarkyti duomenis, turi būti susipažinę su Asmens duomenų teisinės apsaugos įstatymu, Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentais ir kitais teisės aktais, reglamentuojančiais Informacinės sistemos duomenų saugos politiką; pasirašę pasižadėjimą saugoti asmens duomenų paslaptį; nuolat kelti savo kvalifikaciją kvalifikacijos kėlimo kursuose, saugaus darbo su duomenimis seminaruose ir mokymuose; gilinti kompiuterines žinias ir siekti Europos kompiuterio vartotojo pažymėjimo (ECDL).

36. Informacinės sistemos saugos įgaliotinis periodiškai, bet ne rečiau kaip kartą per dvejus metus, Informacinės sistemos naudotojams organizuoja mokymus elektroninės informacijos saugos klausimais, įvairiais būdais primena apie saugumo problemas (pvz., pranešimai elektroniniu paštu, naujų darbuotojų instruktavimas ir pan.).

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

37. Naudoti Informacinės sistemos duomenis gali tik tie asmenys, kurie yra susipažinę su Saugos nuostatais, Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, ir raštu sutikę laikytis šių teisės aktų reikalavimų.

38. Už Informacinės sistemos naudotojų supažindinimą su Saugos nuostatais, Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentais ir kitais teisės aktais bei atsakomybe už šiuose dokumentuose nustatytų reikalavimų nesilaikymą yra atsakingas Informacinės sistemos saugos įgaliotinis.

39. Saugos nuostatai ir Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentai skelbiami Informacinės sistemos naudotojams pasiekiamoje interneto svetainėje.

40. Pakartotinai su Saugos nuostatais ir Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentais supažindinama elektroniniu paštu, pasikeitus šiems dokumentams.

41. Informacinės sistemos naudotojai, Informacinės sistemos administratoriai ir Informacinės sistemos saugos įgaliotinis, pažeidę Saugos nuostatų, Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentų ir saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

_____