SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2021 m. birželio 10 d. raštu Nr. (4.1.E)6K-479

PATVIRTINTA
Lietuvos administracinių ginčų komisijos pirmininko 2021 m. birželio 17 d. įsakymu
Nr. 1VE-31

LIETUVOS ADMINISTRACINIŲ GINČŲ KOMISIJOS INFORMACINĖS SISTEMOS SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos administracinių ginčų komisijos (toliau – Komisija) Informacinės sistemos saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Komisijos informacinės sistemos (toliau – Informacinė sistema) elektroninės informacijos saugos ir kibernetinio saugumo politiką, nustato organizacines, technines, programines, teisines ir kitas priemones, užtikrinančias saugų Informacinės sistemos duomenų tvarkymą ir kibernetinį saugumą.

2. Saugos nuostatai parengti vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu, 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, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

3. Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarime 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“, Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, Lietuvos „Informacijos technologija. Saugumo metodai“ grupės standartuose ir kituose teisės aktuose, reglamentuojančiuose duomenų saugą.

4. Komisijos informacinėje sistemoje tvarkomos elektroninės informacijos saugos tikslas – saugiai tvarkyti Komisijos informacinėje sistemoje kaupiamus duomenis, užtikrinti jų konfidencialumą, vientisumą ir prieinamumą.

5. Informacijos saugumo užtikrinimo prioritetinės kryptys:

5.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.2. Informacinės sistemos veiklos tęstinumo užtikrinimas;

5.3. asmens duomenų apsauga;

5.4. Informacinės sistemos naudotojų mokymas elektroninės informacijos saugos ir kibernetinio saugumo klausimais.

6. Elektroninės informacijos saugumo užtikrinimo tikslai:

6.1. sudaryti sąlygas automatiniu būdu saugiai tvarkyti elektroninę informaciją;

6.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo ar neteisėto jos tvarkymo.

7. Saugos nuostatai taikomi Komisijos informacinės sistemos valdytojui ir tvarkytojui Lietuvos administracinių ginčų komisijai (juridinio asmens kodas 188735253, adresas: Vilniaus g. 27, Vilnius) ir Komisijos teritoriniams skyriams: Kauno (Laisvės al. 36, Kaunas), Klaipėdos (H. Manto g. 37, Klaipėda), Panevėžio (Respublikos g. 62, Panevėžys) ir Šiaulių (Dvaro g. 81, Šiauliai) apygardos skyriams.

8. Komisija, kaip Informacinės sistemos valdytoja ir tvarkytoja, atlieka šias funkcijas:

8.1. tvirtina saugos politikos įgyvendinimo dokumentus Bendrųjų elektroninės informacijos saugos reikalavimų apraše nustatyta tvarka ir terminais, t. y. per 6 mėnesius nuo Komisijos Saugos nuostatų įsigaliojimo dienos;

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

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

8.4. atlieka Informacinės sistemos duomenų, elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų laikymosi priežiūrą;

8.5. priima sprendimus dėl Informacinės sistemos saugos užtikrinimo;

8.6. priima sprendimą atlikti Informacinės sistemos informacinių technologijų saugos reikalavimų atitikties vertinimą ir tvirtina saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

8.7. prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą;

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

8.9 atsako už Informacinės sistemos duomenų tvarkymo, teikimo ir (ar) gavimo teisėtumą ir saugą;

8.10 skiria saugos įgaliotinį ir Informacinės sistemos administratorius;

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

8.12. užtikrina kibernetinių incidentų, įvykusių Informacinėje sistemoje, valdymą ir tyrimą;

8.13. pateikia paskirto saugos įgaliotinio kontaktinę informaciją Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos;

8.14 užtikrina Informacinės sistemos sąveiką su kitomis informacinėmis sistemomis ir registrais;

8.15. užtikrina Informacinės sistemos atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams;

8.16. ne rečiau kaip kartą per 3 (tris) metus organizuoti saugos dokumentų persvarstymą;

8.17. organizuoja naudotojams mokomuosius ir pažintinius kursus elektroninės informacijos tvarkymo klausimais.

8.18. Komisija atsako už saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą ir už Informacinės sistemos administracinių, techninių ir organizacinių saugos ir kibernetinio saugumo priemonių įgyvendinimą,

užtikrinimą ir jų laikymąsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

9. Saugos įgaliotinis atlieka šias funkcijas:

9.1. rengia Informacinės sistemos saugos dokumentų projektus;

9.2. teikia Komisijos pirmininkui pasiūlymus dėl:

9.2.1. Informacinės sistemos saugos dokumentų priėmimo, keitimo ar panaikinimo;

9.2.2. Informacinės sistemos informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

9.2.3. Informacinės sistemos administratorių skyrimo ir reikalavimų jiems nustatymo;

9.2.4. organizacinių ir techninių priemonių, skirtų Informacinės sistemos kibernetinio saugumo užtikrinimui ir kontrolei, diegimo;

9.2.5. Informacinės sistemos kibernetinio saugumo reikalavimų atitikties vertinimo atlikimo;

9.3. koordinuoja elektroninės informacijos saugos incidentų tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

9.4. organizuoja kasmetinius ir prireikus neeilinius Informacinės sistemos rizikos vertinimus;

9.5. teikia administratoriams privalomus vykdyti nurodymus ir pavedimus dėl saugos politikos įgyvendinimo ir kibernetinio saugumo reikalavimų įgyvendinimo;

9.6. organizuoja Informacinės sistemos naudotojų supažindinimą su saugos politikos įgyvendinimo dokumentais ir teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą ir atsakomybę už šiuose dokumentuose nustatytų reikalavimų nesilaikymą;

9.7. periodiškai inicijuoja darbuotojų mokymą duomenų saugos klausimais, juos supažindina su informacijos saugos reikalavimais;

9.8. atsako už saugos politikos įgyvendinimo organizavimą;

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

9.10. atsako už kibernetinio saugumo reikalavimų atitiktį Lietuvos Respublikos teisės aktams;

9.11. vykdo Informacinės sistemos kibernetinio saugumo stebėseną, kontrolę ir užtikrinimą;

9.12. vykdo Informacinės sistemos kibernetinio saugumo būklės analizę, kylančių grėsmių, rizikų ir pažeidžiamų vietų vertinimą;

9.13. praneša Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos apie kibernetinį incidentą;

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

10. Saugos įgaliotinis negali atlikti administratoriaus funkcijų.

11. Saugos įgaliotinis, atlikdamas savo funkcijas, turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems Informacinės sistemos valdytojo ir tvarkytojo darbuotojams, jeigu tai būtina saugos politikai įgyvendinti.

12. Administratoriai skiriami keliems posistemiams, funkciškai savarankiškoms sudedamosioms dalims ar tam tikroms administratoriaus funkcijoms atlikti.

13. Administratoriai skirstomi į šias grupes:

13.1. Komisijos Informacinės sistemos administratorius, kuris atlieka funkcijas, susijusias su sistemos komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazių valdymo sistemomis, taikomųjų programų sistemomis, užkardomis, įsilaužimų aptikimo sistemomis, elektroninės informacijos perdavimu tinklais, bylų serveriais ir kitais komponentais) ir jų sąranka;

13.2. Veiklos administratoriai, kurie atlieka funkcijas, susijusias su Komisijos naudojamų taikomųjų programų administravimu.

14. Informacinės sistemos valdytojo vadovo sprendimu administratorių funkcijos gali būti sugretintos.

15. Administratoriai privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus dėl Informacinės sistemos saugos užtikrinimo, pagal kompetenciją reaguoti į elektroninės informacijos saugos incidentus ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

16. Atlikdamas Informacinės sistemos sąrankos pakeitimus, Informacinės sistemos administratorius turi laikytis valdytojo Informacinės sistemos pokyčių valdymo tvarkos, nustatytos valdytojo tvirtinamose Komisijos Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

17. Informacinės sistemos administratorius privalo patikrinti (peržiūrėti) Informacinės sistemos sąranką ir Informacinės sistemos būsenos rodiklius reguliariai, ne rečiau kaip kartą per metus ir (arba) po Informacinės sistemos pokyčio.

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

18.1. 2016 m. balandžio 26 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB;

18.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

18.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

18.4. Lietuvos Respublikos kibernetinio saugumo įstatymu;

18.5. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

18.6. 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

18.7. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ 1.3 punktu;

18.8. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymą Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“

18.9. pagrindiniais saugos reikalavimais, nustatytais Lietuvos standartuose LST ISO/IEC 27001:2017 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ ir LST ISO/IEC 27002:2017 „Informacijos technologija. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“;

18.10. kitais teisės aktais, kuriais reglamentuojamas elektroninės informacijos, kibernetinio saugumo tvarkymas ir saugos valdymas, Informacinės sistemos valdytojo ir tvarkytojo veikla.

19. Saugos nuostatai privalomi visiems Informacinės sistemos naudotojams, Informacinės sistemos administratoriams, saugos įgaliotiniui.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

20. Informacinėje sistemoje tvarkoma elektroninė informacija priskiriama mažiausios svarbos elektroninės informacijos kategorijai, kadangi, įvertinus informacijos konfidencialumo, vientisumo ir (ar) prieinamumo galimo praradimo neigiamą poveikį, nepatenka į 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“ patvirtinto Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo 6.1–6.3 papunkčiuose nustatytas kategorijas.

21. Atsižvelgiant į Informacinės sistemos tvarkomos elektroninės informacijos svarbos kategoriją ir vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 12.4 papunkčiu, Informacinė sistema priskiriama ketvirtajai informacinės sistemos kategorijai, nes tvarkoma mažiausios svarbos informacija.

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

23. Informacinės sistemos rizikos vertinimo rezultatai pateikiami rizikos vertinimo ataskaitoje, kuri rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Informacinės sistemos rizikos vertinimo ataskaita pateikiama Informacinės sistemos valdytojo vadovui.

24. Svarbiausi rizikos veiksniai yra šie:

24.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, netyčinis duomenų ištrynimas, klaidingas duomenų suvedimas ir teikimas, fizinės informacijos technologijų triktys, duomenų perdavimo tinklais triktys, programinės įrangos klaidos, netinkamas veikimas ir kita);

24.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais trikdžiai, saugumo pažeidimai, vagystės ir kita);

24.3. atsitiktinės subjektyvios aplinkybės (darbuotojų praradimas, gaisrai, vandens poveikis, elektros instaliacijos gedimas ir kita);

24.4. 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.

25. Atsižvelgdamas į rizikos vertinimo ataskaitą, Informacinės sistemos valdytojo vadovas prireikus tvirtina rizikos vertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

26. Saugos įgaliotinis ne rečiau kaip vieną kartą per metus organizuoja informacinių technologijų saugos atitikties vertinimą, kurį atliekant:

26.1. įvertinama, ar Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentai parengti atsižvelgiant į realią informacijos saugos situaciją;

26.2. inventorizuojama Informacinės sistemos techninė ir programinė įranga;

26.3. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų Informacinės sistemos tvarkytojo naudotojų kompiuterinių darbo vietų;

26.4. patikrinamos visose tarnybinėse stotyse įdiegtos programos ir jų sąranga;

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

26.6. įvertinamas pasirengimas užtikrinti Informacinės sistemos veiklos tęstinumą įvykus elektroninės informacijos saugos, kibernetinio saugumo incidentui.

27. Atlikus informacinių technologijų saugos atitikties vertinimą Informacinės sistemos valdytojui pateikiama vertinimo ataskaita.

28. 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.

29. Kartu su Informacinės sistemos rizikos vertinimu ir (arba) informacinių technologijų saugos atitikties vertinimu, saugos įgaliotinis organizuoja ir grėsmių ir pažeidžiamumų, galinčių turėti įtaką Informacinės sistemos elektroninės informacijos saugai ir kibernetiniam saugumui, vertinimą.

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

30.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

30.2. informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;

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

31. Patvirtintų Saugos nuostatų, saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas saugos įgaliotinis ne vėliau kaip per penkias darbo dienas nuo jų patvirtinimo dienos pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

32. Rizikos vertinimo ataskaitos, rizikos vertinimo ir rizikos valdymo priemonių plano, saugos atitikties vertinimo ataskaitos ir pastebėtų trūkumų šalinimo plano kopijas saugos įgaliotinis ne vėliau kaip per penkias darbo dienas nuo minėtų dokumentų priėmimo dienos pateikia Stebėsenos sistemos nuostatuose nustatyta tvarka.

33. Kibernetinių incidentų, įvykusių Informacinėje sistemoje, valdymas ir tyrimas užtikrinamas vadovaujantis Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

34. Programinės įrangos, skirtos Informacinei sistemai nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.) apsaugoti, naudojimo nuostatos ir atnaujinimo reikalavimai:

34.1. Informacinės sistemos tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti įdiegta centralizuotai valdoma programinė įranga, skirta Informacinei sistemai nuo kenksmingos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.) programinės įrangos apsaugoti, kuri turi atsinaujinti automatiniu būdu ne rečiau kaip kartą per 24 valandas;

34.2. Informacinės sistemos apsaugai naudojama programinė įranga turi būti nustatyta taip, kad Informacinės sistemos administratorius būtų automatiškai elektroniniu paštu informuojamas

apie kompiuterizuotas darbo vietas ir tarnybines stotis, kuriose apsaugos sistema veikia netinkamai, yra išjungta arba neatsinaujino per 24 valandas arba aptiko kenksmingą programinę įrangą;

34.3. Informacinės sistemos apsaugai naudojama programinė įranga turi turėti apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų.

35. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo nuostatos:

35.1. turi būti naudojama tik Informacinės sistemos funkcijoms vykdyti būtina programinė įranga;

35.2. programinės įrangos diegimą, šalinimą ir konfigūravimą gali atlikti tik administratoriai;

35.3. turi būti naudojama tik legali programinė įranga;

35.4. programinė įranga turi būti atnaujinama laikantis gamintojo reikalavimų.

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

36.1. elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant užkardas, kurių saugos įvykių žurnalai turi būti reguliariai, ne rečiau kaip kartą per savaitę, analizuojami;

36.2. Informacinės sistemos tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių Informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

36.3. turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų Informacinės sistemos įeinantį ir išeinantį duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų;

36.4. įsilaužimo aptikimo konfigūracijos ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo Informacinės sistemos techninės įrangos (kartu nurodant atitinkamas datas (įgyvendinimo, atnaujinimo ir panašiai), atsakingus asmenis, taikymo periodus ir panašiai);

36.5. Informacinės sistemos tarnybinėse stotyse, kompiuteriuose turi būti įjungtos vietinės ugniasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su Informacinės sistemos funkcionalumu ir administravimu ir darbuotojų funkcijomis, susijusį duomenų srautą.

37. Leidžiamos kompiuterių naudojimo ribos:

37.1. Informacinės sistemos naudotojų kompiuteriai privalo būti naudojami tik tiesioginėms pareigoms atlikti ir turi būti apsaugoti prisijungimo vardu ir slaptažodžiu;

37.2. Informacinės sistemos naudotojai, naudojantys nešiojamuosius kompiuterius ar kitus mobilius įrenginius ir teikiantys ar gaunantys elektroninę informaciją (vykdydami savo tarnybines funkcijas) per viešuosius kompiuterių tinklus (internetą), turi naudoti papildomas saugos priemones (elektroninės informacijos šifravimas, papildomas tapatybės patvirtinimas, prisijungimo ribojimai, rakinimo įrenginių naudojimas);

37.3. Iš stacionarių ir nešiojamųjų kompiuterių, kurie perduodami taisymui priežiūros paslaugų teikėjui, turi būti išimtos informacijos laikmenos. Jei sugenda pati laikmena ar įranga nurašoma, laikmenos turi būti neatstatomai sunaikintos;

37.4. stacionarius kompiuterius ne valdytojo ir tvarkytojo patalpose leidžiama naudoti tik su valdytojo vadovo sutikimu.

37.5. Informacinės sistemos naudotojai gali jungti prie kompiuterio ir naudoti išorinius įrenginius ir laikmenas tik savo darbo funkcijoms vykdyti;

37.6. iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi Informacinės sistemos duomenys ir Informacinės sistemos informacija;

37.7. Informacinės sistemos duomenų naudotojai privalo naudotis visomis saugumo priemonėmis, kad kompiuteris ir duomenų laikmenos būtų apsaugoti nuo vagystės arba pažeidimo.

38. Metodai, kuriais užtikrinamas saugus elektroninės informacijos teikimas ir (ar) gavimas:

38.1. elektroninė informacija iš Informacinės sistemos gaunama tik pagal duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

38.2. prieigos prie elektroninės informacijos teises gali suteikti tik administratoriai. Informacinės sistemos naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės, vadovaujantis principu „būtina žinoti“;

38.3. Informacinėje sistemoje jos naudotojui turi būti leista atlikti tik tuos veiksmus, kuriuos atlikti jam yra suteiktos teisės;

38.4. Informacinėje sistemoje kiekvienas jos naudotojas turi būti unikaliai autentifikuojamas (Informacinės sistemos naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kita identifikavimo ir autentifikavimo priemone) ir autorizuojamas;

38.5. Informacinėje sistemoje turi būti saugoma informacija apie naudotojų ir administratorių veiksmus;

38.6. pasibaigus Informacinės sistemos naudotojo darbo sutarčiai (ar nutrūkus tarnybiniams santykiams), teisė naudotis elektronine informacija turi būti panaikinta. Informacinės sistemos naudotojui prieiga prie Informacinės sistemos turi būti ribojama ar sustabdoma, kai vyksta Informacinės sistemos naudotojo veiklos tyrimas arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos;

38.7. viešuoju tinklu perduodamos elektroninės informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualųjį privatųjį tinklą (angl. *virtual private network*), skirtines linijas, saugų valstybinį duomenų perdavimo tinklą ar kitas priemones.

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

39.1. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai, kiekvieną parą nakties metu;

39.2 atsarginės kopijos turi būti šifruojamos arba naudojamos kitos priemonės atsarginių kopijų konfidencialumui užtikrinti;

39.3. periodiškai (ne rečiau kaip 1 kartą per metus) atliekami elektroninės informacijos atkūrimo iš Informacinės sistemos duomenų atsarginių kopijų bandymai.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

40. Informacinės sistemos naudotojų, administratorių, saugos įgaliotinio kvalifikacija turi atitikti bendruosius ir specialiuosius reikalavimus, nustatytus jų pareiginiuose nuostatuose ir šiuose nuostatuose.

41. Visi Informacinės sistemos naudotojai privalo turėti darbo kompiuteriu, taikomosiomis programomis įgūdžių.

42. Visi naudotojai privalo rūpintis Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugumu.

43. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentais, standartais ir kitais duomenų tvarkymą reglamentuojančiais Lietuvos Respublikos ir Europos Sąjungos teisės aktais bei būti susipažinęs su esminiais Informacinės sistemos duomenų saugos reikalavimais saugos politikai įgyvendinti.

44. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą, susijusį su elektroninių duomenų ir Informacinės sistemos saugumu, 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, elektroninių ryšių tinklo darbui trukdantį elektroninių ryšių infrastruktūros įrengimo,

naudojimo ir apsaugos sąlygų ar taisyklių pažeidimą, jeigu nuo nuobaudos paskyrimo praėję mažiau kaip vieni metai.

45. Administratoriai privalo išmanyti informacijos saugos principus, turi būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą; turi būti pasirašę pasižadėjimą saugoti asmens duomenų paslaptį, nuolat kelti savo kvalifikaciją kvalifikacijos kėlimo kursuose, saugaus darbo su duomenimis seminaruose ir mokymuose ir būti susipažinę su Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentais ir kitais Informacinės sistemos duomenų saugos politikos įgyvendinimo teisės aktais.

46. Informacinės sistemos naudotojai privalo turėti pagrindinius darbo su kompiuteriu įgūdžius, mokėti tvarkyti duomenis, turi būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą; turi būti pasirašę pasižadėjimą saugoti asmens duomenų paslaptį, nuolat kelti savo kvalifikaciją kvalifikacijos kėlimo kursuose, saugaus darbo su duomenimis seminaruose ir mokymuose ir būti susipažinę su Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentais ir kitais Informacinės sistemos duomenų saugos politikos įgyvendinimo teisės aktais.

47. Saugos įgaliotinis, atlikdamas savo funkcijas, turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems informacinės sistemos valdytojo ir tvarkytojo darbuotojams, jeigu tai būtina saugos politikai įgyvendinti.

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

49. Informacinės sistemos tvarkytojas saugos įgaliotiniui ir kibernetinio saugumo vadovui periodiškai, bet ne rečiau kaip kartą per metus, organizuoja mokymus elektroninės informacijos saugos ir kibernetinio saugumo klausimais.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

50. Visi Informacinės sistemos naudotojai privalo būti pasirašytinai supažindinti su saugos dokumentais, savo pareigomis ir atsakomybe, susijusia su Informacinės sistemos elektroninės informacijos sauga.

51. Už naudotojų pasirašytiną supažindinimą su šiais saugos nuostatais, savo pareigomis ir atsakomybe, susijusia su Komisijos informacijos sauga, ir kitais saugos politiką įgyvendinančiais teisės aktais bei atsakomybe už saugos dokumentų pažeidimus yra atsakingas paskirtas saugos įgaliotinis.

52. Pakartotinai su saugos dokumentais Komisijos Informacinės sistemos naudotojai supažindinami tik iš esmės pasikeitus Informacinės sistemos arba elektroninės informacijos saugą reglamentuojantiems teisės aktams. Informacija apie pasikeitimus saugos politiką įgyvendinančiuose teisės aktuose siunčiama elektroniniu būdu (skelbiama Dokumentų valdymo sistemoje).

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

53. Informacinės sistemos valdytojas saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Keičiami saugos dokumentai turi būti derinami su Nacionalinio kibernetinio saugumo centru prie Krašto apsaugos ministerijos. Keičiami saugos dokumentai su Nacionalinio kibernetinio saugumo centru prie Krašto apsaugos ministerijos gali būti nederinami tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika.

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

55. Saugos nuostatai privalomi Informacinės sistemos valdytojo ir tvarkytojo darbuotojams, Informacinės sistemos naudotojams, Informacinės sistemos administratoriui, veiklos administratoriams, saugos įgaliotiniui.

56. Informacinės sistemos naudotojai, administratoriai ir saugos įgaliotinis, pažeidę Saugos nuostatų, Informacinės sistemos duomenų saugos politikos įgyvendinimo dokumentus ir saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako teisės aktų, reglamentuojančių atsakomybę už duomenų saugos pažeidimus, nustatyta tvarka.

57. Ne rečiau kaip kartą per metus arba įvykus esminiams pokyčiams turi būti peržiūrimi ir prireikus atnaujinami Saugos nuostatai.

_____