PATVIRTINTA
Rokiškio rajono savivaldybės administracijos
direktoriaus 2023 m. birželio 28 d.
įsakymu Nr. AV-488

ROKIŠKIO RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Rokiškio rajono savivaldybės administracijos informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja informacinių sistemų ir kitų informacinių technologijų priemonių, kurių valdytojas yra Rokiškio rajono savivaldybės administracija (toliau – IS), elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos vietos savivaldos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas).

3. IS elektroninės informacijos saugumo ir kibernetinio saugumo užtikrinimo tikslas – apsaugoti IS tvarkomos elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

4. IS elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų IS elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė;

4.2. IS veiklos tęstinumo užtikrinimas;

4.3. IS naudotojų mokymas.

5. Saugos nuostatai privalomi Rokiškio rajono savivaldybės administracijai, įmonės kodas 188772248, Sąjūdžio g. 1, LT-42136, Rokiškis, IS naudotojams, IS saugos įgaliotiniui ir IS administratoriui, IS funkcionuoti reikalingų paslaugų teikėjams.

6. IS valdytojas ir tvarkytojas yra Rokiškio rajono savivaldybės administracija.

7. IS valdytojas atsako už IS elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą, politikos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą bei vykdo šias funkcijas:

7.1. rengia ir tvirtina IS elektroninės informacijos saugos (kibernetinio saugumo) politiką įgyvendinančius dokumentus;

7.2. kontroliuoja, kaip laikomasi IS elektroninės informacijos saugos (kibernetinio saugumo) politiką įgyvendinančių dokumentų ir kitų teisės aktų, reglamentuojančių elektroninės informacijos tvarkymo teisėtumą ir saugos valdymą;

7.3. priima sprendimus dėl IS techninių ir programinių priemonių, būtinų IS elektroninės informacijos saugai (kibernetiniam saugumui) užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

7.4. skiria IS saugos įgaliotinį (toliau – Saugumo įgaliotinis);

7.5. skiria IS administratorių (toliau – administratorius);

7.6. vykdo kitas Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą (kibernetinį saugumą), IS valdytojui priskirtas funkcijas.

8. IS tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimo užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka bei vykdo šias funkcijas:

8.1. pagal kompetenciją įgyvendina IS elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus;

8.2. užtikrina Saugos nuostatų, saugos politiką įgyvendinančių dokumentų ir IS valdytojo priimtų teisės aktų, susijusių su IS elektroninės informacijos sauga (kibernetiniu saugumu), tinkamą įgyvendinimą;

8.3. pagal kompetenciją užtikrina IS elektroninės informacijos saugą (kibernetinį saugumą);

8.4. prižiūri IS duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, įsilaužimų aptikimo sistemas, elektroninės informacijos perdavimo tinklus, kompiuterius, operacines sistemas ir kitus IS komponentus, užtikrina jų veikimą;

8.5. vykdo kitas Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą (kibernetinį saugumą), IS tvarkytojui priskirtas funkcijas.

9. Saugos įgaliotinio funkcijos ir atsakomybė:

9.1. teikia IS valdytojo vadovui pasiūlymus dėl:

9.1.1. administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo;

9.1.2. Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų priėmimo arba keitimo;

9.1.3. informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

9.2. koordinuoja elektroninės informacijos saugos incidentų tyrimą, išskyrus atvejus, kai šią funkciją atlieka IS valdytojo vadovo įsakymu sudaryta informacijos saugos darbo grupė;

9.3. organizuoja IS rizikos vertinimą;

9.4. 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“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

9.5. supažindina administratorių ir IS naudotojus su Saugos nuostatų, saugos politiką įgyvendinančių dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą;

9.6. teikia administratoriui ir IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimu;

9.7. organizuoja IS naudotojų mokymus elektroninės informacijos saugos (kibernetinio saugumo) klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

9.8. vykdo kitas Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą (kibernetinį saugumą), saugos įgaliotiniui ir asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, nustatytas funkcijas.

10. Administratoriaus funkcijos ir atsakomybė:

10.1. užtikrina IS komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimo aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą;

10.2. parengia ir diegia saugos priemones bei užtikrina jų atitiktį Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimams;

10.3. atsako už IS naudotojų registravimą ir prieigos teisių nustatymą;

10.4. pagal kompetenciją vertina IS naudotojų pasirengimą dirbti su IS;

10.5. dalyvauja vykdant saugumo reikalavimų įgyvendinimo stebėseną;

10.6. nuolat teikia saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę, neveikiančias ar netinkamai veikiančias IS elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo priemones, Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų pažeidimus, registruoja elektroninės informacijos saugos incidentus ir apie juos informuoja saugos įgaliotinį, teikia siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

10.7. daro IS elektroninės informacijos atsargines kopijas ir atsako už kopijų saugojimą;

10.8. pagal kompetenciją teikia siūlymus dėl IS palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

10.9. atlieka kitas IS tvarkytojo, saugos įgaliotinio pavestas, Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

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

11.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

11.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

11.3. Kibernetinio saugumo įstatymas;

11.4. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

11.5. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

11.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

11.7. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas 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“;

11.8. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugą (kibernetinį saugumą) bei asmens duomenų tvarkymą, IS valdytojo ir tvarkytojo veiklą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

12. IS tvarkomos elektroninės informacijos kategorija – mažiausios svarbos informacija. IS tvarkomos elektroninės informacijos priskyrimo mažiausios svarbos informacijai kriterijus – Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Klasifikavimo gairių aprašas), 10 punktas, t. y. Mažiausios svarbos informacijos kategorijai priskiriama informacija, kuri nepatenka į Aprašo 6.1–6.3 papunkčiuose nurodytas kategorijas;

13. IS pagal tvarkomos informacijos svarbą priskiriama ketvirtai kategorijai. IS priskyrimo ketvirtai kategorijai kriterijus – Klasifikavimo gairių aprašo 12.4. punktas, t. y. IS tvarkoma mažiausios svarbos informacija.

14. Saugumo įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, kasmet organizuoja rizikos vertinimą. Prireikus (po esminių organizacinių ar sisteminių pokyčių, nustačius naujų rizikos veiksnių ar pan.) Saugumo įgaliotinis gali organizuoti neeilinį rizikos vertinimą. IS valdytojo vadovo rašytiniu pavedimu rizikos vertinimą gali atlikti pats Saugumo įgaliotinis. Rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu.

15. Rizikos vertinimas įforminamas rizikos vertinimo ataskaitoje. Rizikos vertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Rizikos vertinimo ataskaita pateikiama IS valdytojui.

16. Svarbiausi rizikos veiksniai yra šie:

16.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

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

16.3. 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.

17. Rizikos veiksniai rizikos vertinimo ataskaitoje turi būti išdėstyti pagal prioritetus ir priimtiną rizikos lygį.

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

19. Siekiant įvertinti IS saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, Saugumo įgaliotinis ne rečiau kaip vieną kartą per metus organizuoja informacinių technologijų saugos atitikties vertinimą, kurio metu:

19.1. įvertinama saugos politiką įgyvendinančių dokumentų ir realios informacijos saugos situacijos atitiktis;

19.2. inventorizuojama IS techninė ir programinė įranga;

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

19.4. įvertinama IS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;

19.5. įvertinamas pasirengimas užtikrinti IS veiklos tęstinumą įvykus saugos incidentui.

20. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama IS valdytojo vadovui. Įvertinus informacinių technologijų saugos atitikties vertinimo ataskaitą, prireikus rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato IS valdytojo vadovas.

21. IS atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

22. Elektroninės informacijos saugos (kibernetinio saugumo) priemonės (techninės, programinės, organizacinės ir kitos elektroninės informacijos saugos (kibernetinio saugumo) priemonės) parenkamos vadovaujantis šiais priemonių parinkimo principais:

22.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

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

22.3. kur galima, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės informacijos saugos (kibernetinio saugumo) priemonės.

23. Rizikos vertinimo ataskaita, rizikos įvertinimo ir rizikos valdymo priemonių plano kopija, informacinių technologijų saugos atitikties vertinimo ataskaita, pastebėtų trūkumų šalinimo plano kopija ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikiamos Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

24. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai nustatomi pagal Saugos nuostatų 13 punkte nustatytą IS svarbos kategoriją ir vadovaujantis Saugos nuostatų 11 punkte nurodytais teisės aktais.

25. Organizacinių ir techninių elektroninės informacijos saugos (kibernetinio saugumo) priemonių užtikrinimas turi būti grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos elektroninės informacijos saugai (kibernetiniam saugumui), rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus.

26. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai detalizuojami saugos politiką įgyvendinančiuose dokumentuose.

27. Programinės įrangos, skirtos IS nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

27.1. Tarnybinių stočių ir kompiuterinėse darbo vietose turi būti įdiegtos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios atnaujinamos automatiniu būdu ne rečiau kaip kartą per parą.

27.2. Naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų.

28. Detalios programinės įrangos, skirtos apsaugoti IS nuo kenksmingos programinės įrangos, naudojimo nuostatos ir jos atnaujinimo reikalavimai nustatomi IS saugaus elektroninės informacijos tvarkymo taisyklėse.

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

29.1. turi būti naudojama tik legali ir IS naudotojų funkcijoms vykdyti ir IS administruoti būtina programinė įranga;

29.2. programinė įranga turi būti nuolatos atnaujinama laikantis gamintojo reikalavimų;

29.3. turi būti įdiegta prieigos prie elektroninės informacijos per registravimą, teisių suteikimą ir slaptažodžius sistema;

29.4. IS naudotojams draudžiama patiems diegti bet kokią programinę įrangą.

30. Kompiuterių tinklo filtravimo įrangos pagrindinės naudojimo nuostatos:

30.1. Elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami;

30.2. IS programinė įranga privalo turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų;

30.3. IS perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių IS naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

30.4. IS elektroninės informacijos apsaugai naudojama įsilaužimų prevencijos sistema – tinklo saugumo prietaisas, įrengiamas IS prieigose ir skirtas aptikti tinklų ir (arba) sistemų

kenksmingą veiklą, fiksuoti informaciją apie šią veiklą, bandyti blokuoti (sustabdyti) šią veiklą ir apie tai pranešti administratoriui.

31. Detalios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos IS saugaus elektroninės informacijos tvarkymo taisyklėse.

32. Leistinos kompiuterių naudojimo ribos:

32.1. stacionarūs ir nešiojamieji IS naudotojų kompiuteriai ir kiti mobilieji įrenginiai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi IS duomenys ir informacija;

32.2. nešiojamuosiuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose turi būti taikomos papildomos saugos priemonės – elektroninės informacijos šifravimas ir prisijungimo ribojimas;

32.3. nuotoliniu būdu jungiantis prie IS yra naudojama VPN technologija;

32.4. IS naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

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

33.1. IS elektroninė informacija automatiniu būdu perduodama, koduotu kanalu TCP/IP protokolu, prieiga prie duomenų ribojama pagal IP adresą;

33.2. IS elektroninė informacija perduodama realiu laiku arba asinchroniniu režimu pagal duomenų teikimo ir gavimo sutartis, kuriose nustatytos perduodamų duomenų specifikacijos, perdavimo sąlygos ir tvarka;

33.3. IS elektroninė informacija automatiniu būdu teikiama XML formatu.

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

34.1. Elektroninės informacijos atsarginės kopijos daromos automatiniu būdu kartą per parą ir saugomos paskutinių 14 dienų atsarginės kopijos. Kopijos turi būti saugomos kitoje patalpoje, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota. Elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų).

34.2. Prireikus atkurti kopijas teisę tam turi tik administratorius. Periodiškai, bet ne rečiau kaip kartą per pusmetį, turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai. Patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas.

35. Detali kopijų darymo ir saugojimo tvarka nustatoma IS saugaus elektroninės informacijos tvarkymo taisyklėse.

36. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai detalizuojami saugos politiką įgyvendinančiuose dokumentuose.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

37. Saugumo įgaliotinis privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti elektroninės informacijos saugos (kibernetinio saugumo) srities kvalifikaciją, savo darbe vadovautis Lietuvos Respublikos ir Europos Sąjungos teisės aktų, reglamentuojančių elektroninės informacijos saugą, nuostatomis, turėti atitinkamą kvalifikaciją įgyvendinti elektroninės informacijos saugos (kibernetinio saugumo) politiką, taip pat turėti darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties.

38. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą galiojančią administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių

įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

39. Administratorius privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti IS ir tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti IS komponentus (stebėti komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti komponentų nepertraukiamą funkcionavimą ir pan.), būti susipažinęs su saugos politiką įgyvendinančiais dokumentais, darbo saugos taisyklėmis.

40. IS naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, elektroninės informacijos tvarkymą. IS naudotojai, tvarkantys duomenis ir informaciją, privalo saugoti jų paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

41. Saugos įgaliotinio, administratoriaus, IS naudotojų kvalifikacija turi atitikti reikalavimus, nustatytus jų pareiginiuose nuostatuose ar pareigybės aprašyme.

42. IS naudotojų mokymą ir informavimą elektroninės informacijos saugos (kibernetinio saugumo) klausimais planuoja bei organizuoja Saugumo įgaliotinis. IS naudotojai apie elektroninės informacijos saugos (kibernetinio saugumo) problemas, gerąją praktiką elektroninės informacijos saugos (kibernetinio saugumo) srityje informuojami siunčiant priminimus, konsultuojant elektroniniu paštu ar per dokumentų valdymo sistemą, rengiant ir pateikiant atmintines, organizuojant teminius seminarus ir mokymus ir kitais būdais.

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

44. Mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kt. teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.).

45. Mokymai IS naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus.

46. Mokymai saugos įgaliotiniui ir administratoriui turi būti organizuojami pagal poreikį.

V SKYRIUS
IS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

47. Tvarkyti IS elektroninę informaciją gali tik IS naudotojai, kurie yra susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir sutikę laikytis jų reikalavimų. IS naudotojai atsako už IS ir tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją.

48. IS naudotojus su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir atsakomybe už jų reikalavimų nesilaikymą supažindina Saugumo įgaliotinis.

49. IS naudotojų supažindinimas su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ar jų pakeitimais turi būti vykdomas šiais atvejais:

49.1. prieš suteikiant naudotojams prieigą prie IS;

49.2. pakeitus Saugos nuostatus ir (ar) saugos politiką įgyvendinančius dokumentus;

49.3. periodiškai, mokymų elektroninės informacijos saugos (kibernetinio saugumo) temomis metu.

50. IS naudotojų supažindinimo su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais tvarka nustatyta IS naudotojų administravimo taisyklėse.

51. IS naudotojai, administratorius ir Saugumo įgaliotinis, pažeidę Saugos nuostatų, saugos politiką įgyvendinančių dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

52. Saugos dokumentai persvarstomi (peržiūrimi) atlikus rizikos įvertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems IS valdytojo veiklos pokyčiams, bet ne rečiau kaip kartą per metus.
