PATVIRTINTA
Nacionalinio maisto ir veterinarijos
rizikos vertinimo instituto direktoriaus
2022 m. vasario 3 d. įsakymu Nr. 1A-21

NACIONALINIO MAISTO IR VETERINARIJOS RIZIKOS VERTINIMO INSTITUTO INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacinių sistemų (toliau – IS) duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato sistemose tvarkomos elektroninės informacijos saugos tikslus, elektroninės informacijos saugos užtikrinimo prioritetines kryptis, saugų elektroninės informacijos valdymą, organizacinius, techninius ir personalui keliamus reikalavimus, naudotojų supažindinimo su saugos dokumentais principus ir taisykles, apibrėžia elektroninės informacijos saugos politiką.

2. Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ ir kituose teisės aktuose vartojamas sąvokas.

3. Saugos nuostatai reguliuoja saugų informacinės sistemos elektroninės informacijos tvarkymą ir yra privalomi visiems informacinės sistemos elektroninę informaciją tvarkantiems fiziniams ir juridiniams asmenims, administratoriams, kibernetinio saugumo vadovui ir saugos įgaliotiniui.

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

4.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

4.2. informacinės sistemos veiklos tęstinumo užtikrinimas;

4.3. IS duomenų bazės kopijų darymas, saugant jas archyve;

4.4. IS elektroninės informacijos saugojimas nuo žalingos programinės įrangos poveikio;

4.5. įrengiant saugias informacinei sistemai tvarkyti skirtas patalpas ir kompiuterizuotas darbo vietas jose;

4.6. tobulinti IS naudotojų kvalifikaciją;

4.7. įgyvendinti IS elektroninės informacijos integralumą su registrais ir informacinėmis sistemomis;

4.8. asmens duomenų apsauga;

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

5. IS elektroninės informacijos saugumo užtikrinimo tikslai:

5.1. sudaryti sąlygas automatizuotu būdu saugiai rinkti, apdoroti, kaupti, saugoti elektroninę informaciją ir ją teikti archyvo registrams, informacinėms sistemoms, suinteresuotiems juridiniams ir fiziniams asmenims;

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. Saugos nuostatai nustato IS saugos politiką (toliau – saugos politika). Saugos politika įgyvendinama, vadovaujantis saugaus elektroninės informacijos tvarkymo taisyklėmis, informacinių sistemų veiklos tęstinumo valdymo planu, naudotojų administravimo taisyklėmis ir kitais teisės aktais, reglamentuojančiais IS duomenų tvarkymo teisėtumą ir saugų duomenų valdymą.

7. Saugos nuostatai, saugaus elektroninės informacijos tvarkymo taisyklės, veiklos tęstinumo valdymo planas, naudotojų administravimo taisyklės (toliau visi kartu – IS saugos dokumentai) privalomi:

7.1. IS valdytojui – Nacionaliniam maisto ir veterinarijos rizikos vertinimo institutui;

7.2. IS pagrindiniam tvarkytojui – Nacionalinio maisto ir veterinarijos rizikos vertinimo institutui;

7.3. IS naudotojams – IS valdytojo valstybės tarnautojams ar darbuotojams, dirbantiems pagal darbo sutartį, arba IS tvarkytojo darbuotojams, pagal kompetenciją naudojantiems ir (ar) tvarkantiems elektroninę informaciją;

7.4. IS saugos įgaliotiniui;

7.5. IS administratoriams.

8. Informacinės sistemos valdytojo funkcijos:

8.1. pagal kompetenciją atsako už saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą;

8.2. tvirtina IS saugos dokumentus ir kitus teisės aktus, kuriuose reglamentuojamas IS tvarkymo teisėtumas ir IS elektroninės informacijos sauga;

8.4. skiria IS saugos įgaliotinį, paveda jam organizuoti IS saugos politiką ir kontroliuoti jos įgyvendinimą;

8.3. analizuoja IS saugos įgaliotinio pateiktus siūlymus, priima sprendimus dėl IS techninių ir programinių priemonių, būtinų IS elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

8.5. atlieka kitas IS Saugos nuostatų ir IS saugos dokumentuose jam nustatytas funkcijas;

8.6. kontroliuoja, kad būtų skiriami pakankami, racionaliai ir taupiai naudojami darbo, materialiniai ir finansiniai ištekliai, susiję su informacinės sistemos tvarkymu.

9. Saugos įgaliotinio funkcijos:

9.1. atsako už tinkamą IS elektroninės informacijos saugos priemonių įgyvendinimą;

9.2. teikia IS valdytojo vadovui siūlymus dėl IS sisteminės priežiūros ir tvarkymo administratoriaus paskyrimo ir reikalavimų jiems nustatymo;

9.3. teikia IS valdytojo vadovui siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo;

9.4. teikia IS valdytojui siūlymus dėl IS saugos dokumentų priėmimo arba keitimo;

9.5. koordinuoja elektroninės informacijos saugos ir kibernetinio saugumo incidentų tyrimą, bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos ir kibernetinio saugumo incidentus, neteisėtas veiklas, susijusias su elektroninės informacijos saugos ir kibernetinio saugumo incidentais.

9.6. organizuoja IS rizikos įvertinimą ir parengia rizikos įvertinimo ataskaitą;

9.7. teikia sisteminės priežiūros ir tvarkymo administratoriams ir IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su IS saugos politikos įgyvendinimu;

9.8. turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems IS valdytojo darbuotojams, jeigu tai būtina saugos politikai įgyvendinti;

9.9. supažindina sisteminės priežiūros ir tvarkymo administratorius ir IS naudotojus su IS saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą, organizuoja IS naudotojų mokymą elektroninės informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

9.10. atlieka kitas IS valdytojo pavestas, IS saugos dokumentuose jam priskirtas funkcijas.

10. Administratoriai yra šie:

10.1. informacinės sistemos administratorius (toliau – administratorius) – informacinės sistemos administratorius, atsakingas už informacinės sistemos administravimą, klasifikavimo sistemų valdymą, duomenų mainų ir archyvavimo komponentus;

10.2 informacinės sistemos lokalios tarnybinės stoties administratorius – lokalios tarnybinės stoties administratorius, atsakingas už lokalios tarnybinės stoties administravimą, duomenų valdymą, paieškos ir duomenų teikimo komponentus.

11. Administratoriaus funkcijos ir atsakomybės:

11.1. užtikrina IS techninės ir programinės įrangos įdiegimą ir funkcionavimą;

11.2. diegia ir prižiūri programinę įrangą, reikalingą IS naudotojų funkcijoms vykdyti;

11.3. suteikia teisę IS naudotojams naudotis elektronine informacija, kurios reikia jų funkcijoms atlikti;

11.4. užtikrina IS duomenų bazėje naudojamų klasifikatorių atnaujinimą automatiniu būdu;

11.5. užtikrina IS komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazių valdymo sistemų, ugniasienių, įsilaužimų aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą, pagal kompetenciją nustato IS pažeidžiamas vietas;

11.6. užtikrina sąveikos su susijusiais registrais ir informacinėmis sistemomis technologinį funkcionavimą;

11.7. užtikrina, kad IS elektroninė informacija, gauta iš susijusių registrų ir informacinių sistemų, būtų nuolat atnaujinama ir atitiktų susijusiuose registruose ir informacinėse sistemose esančią elektroninę informaciją;

11.8. pagal kompetenciją dalyvauja, vykdant saugumo reikalavimų įgyvendinimo stebėseną;

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

11.10. informuoja IS saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

11.12. atlieka kitas IS valdytojo, IS saugos įgaliotinio pavestas, IS saugos dokumentuose jam nustatytas funkcijas.

11.13. atsako už tinkamą saugos dokumentuose nustatytų funkcijų vykdymą.

12. informacinės sistemos lokalios tarnybinės stoties administratoriaus funkcijos ir atsakomybės:

12.1. užtikrina kompiuterių tinklų veikimą konkrečioje lokalioje tarnybinėje stotyje;

12.2. diegia, konfigūruoja ir prižiūri kompiuterių tinklų aktyviąją įrangą konkrečioje lokalioje tarnybinėje stotyje;

12.3. reguliariai, ne rečiau kaip kartą per metus ir (arba) po informacinės sistemos pokyčio patikrina (užtikrina) informacinės sistemos sąranką, būsenos rodiklius konkrečioje lokalioje tarnybinėje stotyje.

12.4. atsako už tinkamą saugos dokumentuose nustatytų funkcijų vykdymą.

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

13.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

13.2. Lietuvos Respublikos dokumentų ir archyvų įstatymas;

13.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

13.4. Lietuvos respublikos asmens duomenų teisinės apsaugos įstatymas;

13.5. 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“;

13.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

13.7. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašai, patvirtinti 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“;

13.8. 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);

13.9. Lietuvos standartai LST ISO/IEC 27001 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai;

13.10. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą valstybės institucijose.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

14. Informacinėje sistemoje tvarkoma elektroninė informacija priskiriama vidutinės svarbos elektroninės informacijos kategorijai. Elektroninė informacija šiai kategorijai priskiriama 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 2016 m. rugpjūčio 11 d. nutarimu Nr. 826 „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), 6.3, 9.1, 9.2, 9.3, 9.4, 9.5 ir 9.6 papunkčiais.

15. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimogairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2016 m. rugpjūčio 11 d. nutarimu Nr. 826 „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“, 12.3 papunkčiu, IS priskiriamas trečiajai informacinių sistemų kategorijai.

16. IS saugos įgaliotinis:

16.1. saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja visų informacinių sistemų rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį informacinių sistemų rizikos įvertinimą.

16.2. IS rizikos įvertinimą išdėsto įvertinimo ataskaitoje. IS įvertinimo ataskaita rengiama, atsižvelgus į rizikos veiksnius, galinčius turėti ar turinčius įtakos IS elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę, galimus rizikos valdymo būdus. Svarbiausieji rizikos veiksniai yra šie:

16.2.1. 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);

16.2.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis elektronine informacija, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

16.2.3. 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;

16.3. Rizikos įvertinimo ataskaita pateikiama IS valdytojui.

17. Atsižvelgus į rizikos vertinimo ataskaitą, prireikus rengiamas IS rizikos įvertinimo ir rizikos valdymo priemonių planas, kuriame numatomos techninės ir administracinės veiksnius šalinančios priemonės, priemonių vykdymo terminai, vykdytojai ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

18. IS elektroninei informacijai, techninei, programinei įrangai, patalpoms IS valdytojo įstaigoje vertinti naudojama penkiabalė rizikos veiksnių tikėtumo ir žalos vertinimo metodika:

18.1. nereikšminga rizikos veiksnių tikimybė, žala – 1 balas;

18.2. maža rizikos veiksnių tikimybė, žala – 2 balai;

18.3. vidutinė rizikos veiksnių tikimybė, žala – 3 balai;

18.4. didelė rizikos veiksnių tikimybė, žala – 4 balai;

18.5. labai didelė rizikos veiksnių tikimybė, žala – 5 balai.

19. IS saugos priemonės parenkamos, įvertinus galimus rizikos veiksnius IS elektroninės informacijos vientisumui ir prieinamumui.

20. IS elektroninės informacijos saugos priemonių parinkimo pagrindiniai principai yra tokie:

20.1. saugos priemonės turi būti valdomos centralizuotai;

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

20.3. likutinė rizika turi būti sumažinta iki priimtino lygio;

20.4. kur galima, būtina įdiegti prevencines informacijos saugos priemones;

20.5. IS veiklos tęstinumo ir elektroninės informacijos sauga turi būti užtikrinama, patiriant kuo mažiau išlaidų.

21. Siekiant įvertinti IS saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per dvejus metus organizuojamas IS informacinių technologijų saugos atitikties vertinimas:

21.1. įvertinama IS saugos dokumentų ir realios informacijos saugos situacijos atitiktis;

21.2. inventorizuojama IS techninė ir programinė įranga;

21.3. patikrinama (įvertinama) IS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis IS saugos dokumentams;

21.4. įvertinamas pasirengimas užtikrinti IS veiklos tęstinumą, įvykus saugos incidentui.

22. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama IS informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama IS valdytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus skiria ir įgyvendinimo terminus nustato IS valdytojo vadovas.

23. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijos, informacinių technologijų saugos atitikties vertinimo ataskaitos bei pastebėtų trūkumų šalinimo plano kopijos teikiamos Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ 48 punkte nustatytais terminais.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

23.1. IS tarnybinėse stotyse ir kompiuterinėse darbo vietose turi būti kenksmingos programinės įrangos aptikimo priemonės, kuriose turi būti reguliariai tikrinami atnaujinamai automatiniu būdu ne rečiau kaip kartą per parą;

23.2. turi būti naudojamos priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą, veikiančią sisteminiuose kataloguose esančiose tarnybinės stoties rinkmenose ir visuose kompiuterių tinklo kompiuteriuose;

23.3. turi būti naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų.

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

24.1. turi būti naudojama tik legali, programinė įranga;

24.2. programinė įranga turi būti nuolat atnaujinama, laikantis gamintojo reikalavimų;

24.3. programinę įrangą diegti, šalinti ir konfigūruoti gali tik IS sisteminės priežiūros ir tvarkymo administratorius, saugos įgaliotinis ar jo paskirti asmenys;

24.4. turi būti įdiegta prieigos prie IS elektroninės informacijos per registravimąsi, teisių suteikimą ir slaptažodžius sistema;

24.5. turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie IS elektroninės informacijos, atliktus veiksmus.

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

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

25.2. IS programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atjungimo, atskyrimo nuo paslaugos (angl. *DOS*), dedikuoto atjungimo, atskyrimo nuo paslaugos (angl. *DDOS*);

25.3. informacinės sistemos tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių 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;

25.4. turi būti naudojamos turinio filtravimo sistemos;

26. Leistinos kompiuterių naudojimo ribos:

26.1. stacionarūs ir nešiojamieji naudotojų kompiuteriai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš duomenų laikmenų ir kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi elektroniniai duomenys ir informacija;

26.2. kompiuteriuose turi būti naudojamas įjungimo slaptažodis;

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

26.5. išvežti iš patalpų nešiojamieji kompiuteriai negali būti palikti be priežiūros viešose vietose; kelionės metu nešiojamieji kompiuteriai turi būti saugomi.

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

27.1. 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;

27.2. elektroninė informacija iš susijusių registrų gaunama tik pagal duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

27.3. prieigos prie elektroninės informacijos teises gali suteikti tik IS sisteminės priežiūros ir tvarkymo administratorius. IS naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

27.4. prieiga prie IS elektroninės informacijos leidžiama tik per registravimosi slaptažodžių sistemą.

27.5. pasibaigus IS naudotojo darbo sutarčiai, teisė naudotis IS elektronine informacija turi būti panaikinta. IS naudotojui prieiga prie IS turi būti ribojama ar sustabdoma, kai vyksta IS naudotojo veiklos tyrimas, naudotojas turi ilgalaikes atostogas arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos.

28. IS atsarginės duomenų bazės kopijos daromos automatiniu būdu kiekvieną dieną, esant aktyviai IS duomenų bazei. Prireikus jas atkurti turi teisę tik sisteminės priežiūros ir tvarkymo administratorius ar jį pavaduojantis asmuo. Kopijų darymo ir saugojimo tvarka nustatoma IS saugaus elektroninės informacijos tvarkymo taisyklėse;

29. 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

30. IS saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat 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, arba elektroninių ryšių infrastruktūros įrengimo, naudojimo, apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jo paskyrimo praėję mažiau kaip vieneri metai.

31. 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 subjektams, aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą ir kibernetinį saugumą. Informacinės sistemos valdytojas turi sudaryti sąlygas kelti saugos įgaliotinio ir kibernetinio saugumo vadovo kvalifikacijas.

32. 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 laikyti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

33. Administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, mokėti užtikrinti informacinės sistemos ir joje 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 privalo būti susipažinę su saugos dokumentais.

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

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

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

34.3. 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 ir administratorių poreikius;

34.4. 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.);

34.5. naudotojų, administratorių mokymus organizuoja saugos įgaliotinis. Mokymus gali vykdyti saugos įgaliotinis ar kitas informacinės sistemos valdytojo 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;

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

V SKYRIUS
IS NAUDOTOJŲ SUPAŽINDINIMO SU IS SAUGOS DOKUMENTAIS PRINCIPAI

35. Naudotojų supažindinimą su saugos dokumentais, atsakomybe už saugos dokumentų nuostatų pažeidimus organizuoja saugos įgaliotinis.

36. 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 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.

37. 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.

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

39. Naudotojai atsako už informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą pagal savo kompetenciją. Naudotojai, administratoriai, kibernetinio saugumo vadovas 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

40. Informacinės sistemos valdytojas 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 pokyčiams.

41. Informacinės sistemos valdytojas saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Saugos dokumentai turi būti derinami su Lietuvos Respublikos krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių saugos politiką. Keičiami saugos dokumentai gali būti nederinami su Lietuvos Respublikos 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.

_____