LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS DĖL LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRO 2011 M. SPALIO 7 D. ĮSAKYMO NR. V-889 „DĖL ELEKTRONINĖS SVEIKATOS PASLAUGŲ IR BENDRADARBIAVIMO INFRASTRUKTŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO“ PAKEITIMO

2017 m. lapkričio 17 d. Nr. V-1302

Vilnius

P a k e i č i u Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. spalio 7 d. įsakymą Nr. V-889 „Dėl Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatų patvirtinimo“ ir jį išdėstau nauja redakcija:

„LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS DĖL ELEKTRONINĖS SVEIKATOS PASLAUGŲ IR BENDRADARBIAVIMO INFRASTRUKTŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 19 ir 26 punktais, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, 5 punktu, Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano, patvirtinto Lietuvos Respublikos Vyriausybės 2016

m. liepos 20 d. nutarimu Nr. 746 „Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“, 9 punktu:

1. T v i r t i n u Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatus (pridedama).

2. N u s t a t a u , kad:

2.1. valstybės įmonės Registrų centro direktorius per 3 mėnesius nuo Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatų patvirtinimo paskiria Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos saugos įgaliotinį, administratorius, kibernetinio saugumo vadovą ir duomenų valdymo įgaliotinį;

2.2. Valstybės įmonė Registrų centras per 6 mėnesius nuo šio įsakymo įsigaliojimo parengia ir pateikia Lietuvos Respublikos sveikatos apsaugos ministerijai tvirtinti Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos veiklos tęstinumo valdymo plano ir Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos naudotojų administravimo taisyklių projektus.

3. P a v e d u įsakymo vykdymą kontroliuoti viceministrui pagal veiklos sritį.“

Sveikatos apsaugos ministras Aurelijus Veryga

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2011 m. spalio 7 d. įsakymu Nr. V-889
(Lietuvos Respublikos sveikatos apsaugos ministro
2017 m. lapkričio 17 d. įsakymo Nr. V-1302 redakcija)

ELEKTRONINĖS SVEIKATOS PASLAUGŲ IR BENDRADARBIAVIMO INFRASTRUKTŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos (toliau – informacinė sistema) duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja informacinės sistemos elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Saugos nuostatuose vartojamos sąvokos:

2.1. **Informacinės sistemos komponentai** – kompiuteriai, operacinės sistemos, duomenų bazės ir jų valdymo sistemos, taikomųjų programų sistemos, ugniasienės, įsilaužimų aptikimo ir prevencijos sistemos, elektroninės informacijos perdavimo tinklai, duomenų saugyklos, bylų serveriai ir kita techninė ir programinė įranga, kurios pagrindu funkcionuoja informacinės sistemos ir užtikrinama jose tvarkomos elektroninės informacijos sauga (kibernetinis saugumas).

2.2. **Kibernetinio saugumo dokumentai (saugos dokumentai)** – informacinės sistemos duomenų saugos nuostatai, informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės, informacinės sistemos veiklos tęstinumo valdymo planas, informacinės sistemos naudotojų administravimo taisyklės.

2.3. **Kibernetinio saugumo vadovas** – informacinės sistemos tvarkytojo paskirtas kompetentingas darbuotojas, dirbantis pagal darbo sutartį, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą.

2.4. Kitos Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių apraše, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinės sistemos, registrų ir kitų informacinės sistemos klasifikavimo gairių apraše, patvirtintuose Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinės sistemos, registrų ir kitų informacinės sistemos klasifikavimo gairių aprašo patvirtinimo“, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinės sistemos ir kitų informacinės sistemos elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinės sistemos ir kitų informacinės sistemos elektroninės informacijos saugos reikalavimų

patvirtinimo“, ir kituose teisės aktuose bei Lietuvos „Informacijos technologija. Saugumo metodai“ grupės standartuose.

3. Kibernetinio saugumo dokumentų taikymas ir naudojimas:

3.1. Kibernetinio saugumo dokumentai taikomi:

3.1.1. Lietuvos Respublikos sveikatos apsaugos ministerijai (Vilniaus g. 33, LT-01506 Vilnius) – informacinės sistemos valdytojai;

3.1.2. valstybės įmonei Registrų centrui (toliau – Registrų centras) (Vinco Kudirkos g. 18-3, Vilnius) – informacinės sistemos pagrindinei tvarkytojai;

3.1.3. sveikatinimo įstaigoms – informacinės sistemos tvarkytojoms;

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

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

3.3. už kibernetinio saugumo dokumentų santraukos parengimą atsakingas kibernetinio saugumo vadovas. Kibernetinio saugumo dokumentų santrauka rengiama vadovaujantis būtinumo žinoti principu;

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

4. Elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetinės kryptys:

4.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

4.2. informacinės sistemos veiklos tęstinumo užtikrinimas;

4.3. asmens duomenų apsauga;

4.4. informacinės sistemos naudotojų mokymas;

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

5. Elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo tikslai:

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

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

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

6. Lietuvos Respublikos sveikatos apsaugos ministerijos funkcijos:

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

6.2. koordinuoti Registrų centro ir techninės bei programinės įrangos priežiūros funkcijas teikiančio paslaugų teikėjo darbą, jei tokios funkcijos paslaugų teikėjui perduotos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka; nustatyta tvarka atlikti jų veiklos priežiūrą;

6.3. atlikti informacinės sistemos elektroninės informacijos tvarkymo ir elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų laikymosi priežiūrą ir kontrolę;

6.4. nagrinėti Registrų centro pasiūlymus dėl informacinės sistemos veiklos, elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo ir priimti dėl jų sprendimus;

6.5. priimti sprendimus dėl informacinės sistemos techninių ir programinių priemonių, būtinų informacinės sistemos elektroninės informacijos saugai (kibernetiniam saugumui) užtikrinti, įsigijimo, diegimo ir modernizavimo;

6.6. priimti įsakymus dėl informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo;

6.7. užtikrinti veiksmingą ir spartų informacinės sistemos pokyčių valdymo planavimą;

6.8. pavesti informacinės sistemos tvarkytojams paskirti informacinės sistemos administratorius;

6.9. prireikus tvirtinti rizikos įvertinimo ir rizikos valdymo priemonių planą;

6.10. prireikus tvirtinti informacinės sistemos informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

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

7. Registrų centro, kaip pagrindinio informacinės sistemos tvarkytojo, funkcijos:

7.1. užtikinti informacinės sistemos nepertraukiamą veiklą;

7.2. užtikrinti informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą) ir saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais (automatiniu būdu);

7.3. užtikrinti informacinės sistemos sąveiką su susijusiais registrais ir informacinėmis sistemomis;

7.4. užtikrinti Lietuvos Respublikos sveikatos apsaugos ministerijos priimtų teisės aktų ir rekomendacijų tinkamą įgyvendinimą elektroninės informacijos saugos (kibernetinio saugumo) srityje;

7.5. teikti Lietuvos Respublikos sveikatos apsaugos ministerijai pasiūlymus dėl informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo;

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

7.7. Informacinės sistemos valdytojui pavedus skirti saugos įgaliotinį, kibernetinio saugumo vadovą ir informacinės sistemos administratorius;

7.8. ne rečiau kaip kartą per metus organizuoti kibernetinio saugumo dokumentų peržiūrėjimą;

7.9. organizuoti informacinės sistemos naudotojams mokomuosius ir pažintinius kursus informacinės sistemos elektroninės informacijos tvarkymo klausimais;

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

8. Sveikatinimo įstaigų, kaip informacinės sistemos tvarkytojų, funkcijos:

8.1. užtikrinti tinkamą Lietuvos Respublikos sveikatos apsaugos ministerijos priimtų teisės aktų ir rekomendacijų įgyvendinimą;

8.2. nustatyti darbo organizavimo principus ir tvarką, kurie užtikrintų saugų informacinės sistemos elektroninės informacijos tvarkymą;

8.3. užtikrinti, kad informacinė sistema būtų tvarkoma laikantis saugos dokumentuose nustatytų reikalavimų;

8.4. teikti pasiūlymus Lietuvos Respublikos sveikatos apsaugos ministerijai, kaip tobulinti informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą).

9. Už elektroninės informacijos saugą (kibernetinį saugumą) pagal kompetenciją atsako informacinės sistemos valdytojas ir tvarkytojai.

10. Informacinės sistemos valdytojas atsako už elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir įgyvendinimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

11. Informacinės sistemos tvarkytojai atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimo užtikrinimą ir kibernetinio saugumo dokumentuose nustatytų reikalavimų įgyvendinimą.

12. Saugos įgaliotinio funkcijos:

12.1. teikti informacinės sistemos tvarkytojo vadovui pasiūlymus dėl:

12.1.1. informacinės sistemos administratorių paskyrimo ir reikalavimų jiems nustatymo;

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

12.2. teikti informacinės sistemos valdytojo vadovui pasiūlymus dėl kibernetinio saugumo dokumentų priėmimo, keitimo;

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

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

12.5. organizuoti rizikos ir informacinių technologijų saugos atitikties įvertinimą;

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

13. Kibernetinio saugumo vadovas atlieka Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše ir kituose teisės aktuose nustatytas funkcijas. Kibernetinio saugumo vadovas ir saugos įgaliotinis gali būti tas pats asmuo.

14. Saugos įgaliotinis ir kibernetinio saugumo vadovas negali atlikti informacinės sistemos administratoriaus funkcijų.

15. Informacinės sistemos administratorių grupės:

15.1. koordinuojantis administratorius, kuris prižiūri informacinės sistemos administratorių veiklą, siekdamas užtikrinti tinkamą informacinės sistemos administratorių funkcijų vykdymą;

15.2. informacinės sistemos naudotojų administratorius, kuris atlieka funkcijas, susijusias su informacinės sistemos naudotojų teisių valdymu (informacinės sistemos naudotojų duomenų administravimu, klasifikatorių tvarkymu, informacinės sistemos naudotojų veiksmų registracijos žurnalų įrašų analize ir kt.);

15.3. informacinės sistemos komponentų administratoriai, kurie atlieka funkcijas, susijusias su informacinės sistemos komponentais, šių informacinės sistemos komponentų sąranka:

15.3.1. kompiuterių tinklų administratorius atlieka šias funkcijas:

15.3.1.1. užtikrina kompiuterių tinklų veikimą;

15.3.1.2. projektuoja kompiuterių tinklus;

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

15.3.1.4. užtikrina kompiuterių tinklų saugumą.

15.3.2. tarnybinių stočių administratorius atlieka šias funkcijas:

15.3.2.1. užtikrina tarnybinių stočių veikimą;

15.3.2.2. konfigūruoja tarnybinių stočių tinklo prieigą;

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

15.3.2.4. stebi ir analizuoja tarnybinių stočių veiklą;

15.3.2.5. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

15.3.2.6. diegia tarnybinių stočių programinės įrangos atnaujinimus;

15.3.2.7. užtikrina tarnybinių stočių saugą;

15.3.3. duomenų bazių administratorius atlieka šias funkcijas:

15.3.3.1. užtikrina duomenų bazių veikimą;

15.3.3.2. tvarko duomenų bazių programinę įrangą;

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

15.3.3.4. kuria ir atkuria atsargines elektroninės informacijos kopijas;

15.3.3.5. stebi duomenų bazes ir optimizuoja jų funkcionavimą;

15.4. saugos administratorius, kuris atlieka funkcijas, susijusias su informacinės sistemos pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena.

16. Informacinės sistemos administratoriai yra atsakingi už tinkamą kibernetinio saugumo dokumentuose nustatytų funkcijų vykdymą.

17. Informacinės sistemos administratoriai privalo vykdyti visus saugos įgaliotinio ir kibernetinio saugumo vadovo nurodymus ir pavedimus dėl informacinės sistemos saugos (kibernetinio saugumo) užtikrinimo, pagal kompetenciją reaguoti į elektroninės informacijos saugos (kibernetinio saugumo) incidentus ir nuolat teikti saugos įgaliotiniui ir kibernetinio saugumo vadovui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

18. Atlikdami informacinės sistemos sąrankos pakeitimus, informacinės sistemos komponentų administratoriai turi laikytis informacinės sistemos pokyčių valdymo tvarkos, nustatytos informacinės sistemos valdytojo tvirtinamose informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

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

20. Teisės aktai, kuriais vadovaujamasi tvarkant informacinės sistemos elektroninę informaciją ir užtikrinant jos saugą:

20.1. Lietuvos Respublikos kibernetinio saugumo įstatymas;

20.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

20.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

20.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

20.5. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas;

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

20.7. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“;

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

20.9. Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001, ir kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys informacijos saugą;

20.10. kiti teisės aktai, reglamentuojantys informacinių sistemų elektroninės informacijos tvarkymą, elektroninės informacijos saugą, kibernetinį saugumą bei informacinių sistemų valdytojo ir tvarkytojo veiklą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

21. Informacinėje sistemoje tvarkoma elektroninė informacija priskiriama ypatingos svarbos elektroninės informacijos kategorijai. Elektroninė informacija šiai kategorijai priskiriama vadovaujantis Klasifikavimo gairių aprašo 7.1–7.3 papunkčių nuostatomis.

22. Informacinė sistema pagal juose tvarkomos informacijos svarbą, vadovaujantis Klasifikavimo gairių aprašo 12.1 papunkčiu, priskiriama pirmajai kategorijai.

23. Informacinėje sistemoje automatiniu būdu tvarkomi ypatingi asmens duomenys priskiriami trečiajam saugos lygiui, vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms 11.3 papunkčiu.

24. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus, kasmet organizuoja informacinės sistemos rizikos įvertinimą. Prireikus, saugos įgaliotinis gali organizuoti neeilinį informacinės sistemos rizikos įvertinimą. Informacinės sistemos tvarkytojo rašytiniu pavedimu informacinės sistemos rizikos įvertinimą gali atlikti pats saugos įgaliotinis. Kartu su informacinės sistemos rizikos įvertinimu ir (arba) Saugos nuostatų 31 punkte nurodytu informacinių technologijų saugos atitikties vertinimu turi būti

atliekamas grėsmių ir pažeidžiamumo, galinčio turėti įtakos informacinės sistemos kibernetiniam saugumui, vertinimas.

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

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

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

25.3. 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.

26. Atsižvelgdamas į rizikos vertinimo ataskaitą, informacinės sistemos 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.

27. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

28. Siekiant užtikrinti saugos dokumentuose nustatytų elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų įgyvendinimo organizavimą ir kontrolę, turi būti organizuojamas informacinės sistemos informacinių technologijų saugos atitikties vertinimas:

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

28.2. informacinės sistemos atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

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

30. Kibernetinių atakų imitavimas atliekamas šiais etapais:

30.1. Planavimo etapas. Parengiamas kibernetinių atakų imitavimo planas, kuriame apibrėžiami kibernetinių atakų imitavimo tikslai ir darbų apimtis, pateikiamas darbų grafikas, aprašomi planuojamų imituoti kibernetinių atakų tipai (išorinės ir (ar) vidinės), kibernetinių atakų imitavimo būdai (juodosios dėžės (angl. *Black Box*), baltosios dėžės (angl. *White Box*) ir (arba) pilkosios dėžės (angl. *Grey Box*), galima neigiama įtaka veiklai, kibernetinių atakų imitavimo metodologija, programiniai ir (arba) techniniai įrankiai ir priemonės, nurodomi už plano vykdymą atsakingi asmenys ir jų kontaktai. Kibernetinių atakų imitavimo planas turi būti suderintas su informacinių sistemų tvarkytojo vadovu ir vykdomas tik gavus jo raštišką pritarimą.

30.2. Žvalgybos (angl. *Reconnaissance*) ir aptikimo (angl. *Discovery*) etapas. Surenkama informacija apie perimetrą, tinklo mazgus, tinklo mazguose veikiančių serverių ir kitų tinklo įrenginių operacines sistemas ir programinę įrangą, paslaugas (angl. *Services*), pažeidžiamumą, konfigūracijas ir kt. sėkmingai kibernetinei atakai įvykdyti reikalingą informaciją. Šiame etape turi būti teikiamos tarpinės ataskaitos apie vykdomas veiklas ir jos rezultatus.

30.3. Kibernetinių atakų imitavimo etapas. Atliekami kibernetinių atakų imitavimo plane numatyti testai. Šiame etape turi būti teikiamos tarpinės ataskaitos apie vykdomas veiklas ir jos rezultatus;

30.4. Ataskaitos parengimo etapas. Kibernetinių atakų imitavimo rezultatai turi būti išdėstomi informacinių technologijų saugos vertinimo ataskaitoje. Kibernetinių atakų imitavimo plane numatyti testų rezultatai turi būti detalizuojami ataskaitoje ir lyginami su planuotais rezultatais. Kiekvienas aptiktas pažeidžiamumas turi būti detalizuojamas ir pateikiamos pašalinimo rekomendacijos. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos įvertimu. Jeigu nustatoma incidentų valdymo ir šalinimo, taip pat organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinami veiklos tęstinumo planai.

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

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

33. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

34. Elektroninės informacijos saugos (kibernetinio saugumo) būklės gerinimas: techninės, programinės, organizacinės ir kitos informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) priemonės pasirenkamos atsižvelgiant į informacinės sistemos valdytojo turimus išteklius, vadovaujantis šiais principais:

34.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

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

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

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

35. Informacinėse sistemose naudojamų svetainių saugos valdymo reikalavimai:

35.1. svetainės turi atitikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo reikalavimus, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimus;

35.2. svetainių saugasienės turi būti sukonfigūruotos taip, kad prie svetainių turinio valdymo sistemų (toliau – TVS) būtų galima jungtis tik iš vidinio informacinių sistemų tvarkytojo kompiuterio tinklo arba nustatytų IP (angl. *Internet Protocol*) adresų;

35.3. turi būti pakeistos numatytos (angl. *Default*) prisijungimo prie svetainių TVS ir administravimo skydų (angl. *Panel*) nuorodos (angl. *Default path*) ir slaptažodžiai;

35.4. turi būti užtikrinama, kad prie svetainių TVS ir administravimo skydų būtų galima jungtis tik naudojantis šifruotu ryšiu;

35.5. informacinėse sistemose naudojamų svetainių sauga turi būti vertinama informacinių sistemų rizikos įvertinimo metu ir (arba) informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu Saugos nuostatų II skyriuje nustatyta tvarka.

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

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

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

36.3. kenksmingos programinės įrangos aptikimo priemonės turi atsinaujinti automatiškai ne rečiau kaip kartą per 24 valandas. Informacinės sistemos komponentų administratorius turi būti automatiškai informuojamas elektroniniu paštu apie tai, kurių informacinės sistemos posistemių, funkciškai savarankiškų sudedamųjų dalių, vidinių informacinės sistemos naudotojų kompiuterių ir kitų informacinės sistemos komponentų yra pradelstas kenksmingos programinės įrangos aptikimo priemonių atsinaujinimo laikas, kenksmingos programinės įrangos aptikimo priemonės netinkamai funkcionuoja arba yra išjungtos.

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

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

37.2. vidinių informacinės sistemos naudotojų kompiuteriuose naudojama programinė įranga turi būti įtraukta į su informacinės sistemos valdytoju suderintą Leistinos naudoti

programinės įrangos sąrašą. Leistinos naudoti programinės įrangos sąrašą turi parengti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti saugos įgaliotinis;

37.3. tarnybinių stočių ir vidinių informacinės sistemos naudotojų kompiuterių operacinės sistemos kibernetiniam saugumui užtikrinti naudojamų priemonių ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai, klaidų pataisymai turi būti operatyviai išbandomi ir įdiegiami;

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

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

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

37.7. programinė įranga turi būti testuojama naudojant atskirą testavimo aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms;

37.8. informacinės sistemos programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP*) interneto svetainėje www.owasp.org.

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

38.1. kompiuterių tinklai turi būti atskirti nuo viešųjų elektroninių ryšių tinklų (interneto) naudojant ugniasienes, automatinę įsilaužimų aptikimo ir prevencijos įrangą, atkirtimo nuo paslaugos, dedikuoto atkirtimo nuo paslaugos įrangą;

38.2. kompiuterių tinklų perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešuose ryšių tinkluose naršančių vidinių informacinės sistemos 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;

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

38.4. turi būti naudojamos turinio filtravimo sistemos;

38.5. turi būti naudojamos taikomųjų programų kontrolės sistemos.

39. Leistinos kompiuterių naudojimo ribos:

39.1. stacionarius kompiuterius leidžiama naudoti tik informacinės sistemos valdytojo ir informacinės sistemos tvarkytojo patalpose;

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

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

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

40.1. elektroninė informacija teikiama (daugkartinio teikimo atveju ir vienkartinio teikimo atveju) informacinės sistemos nuostatuose nustatyta tvarka;

40.2. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą naudojamas šifravimas, virtualus privatus tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas. Elektroninei informacijai teikti ir (ar) gauti gali būti naudojamas Saugus valstybinis duomenų perdavimo tinklas;

40.3. elektroninė informacija automatiniu būdu turi būti teikiama ir (ar) gaunama tik pagal informacinės sistemos nuostatuose, duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas;

40.4. nuotolinis prisijungimas prie informacinės sistemos galimas:

40.4.1. naudojant perdavimo lygmens protokolus (angl. *Transport Layer Secure, TLS*), reglamentuojančius abipusį tapatumo nustatymą tarp informacinės sistemos naudotojo ir serverio, kad būtų užtikrintas šifruotas ryšys. Saugiam elektroninės informacijos perdavimui tarp serverio ir interneto naršyklės naudojamas TLS sertifikatas, patvirtinantis elektroninės informacijos šaltinio tapatumą, kuris šifruoja tarp informacinės sistemos naudotojo ir serverio siunčiamą elektroninę informaciją. Informacinės sistemos interneto svetainėse TLS šifruota HTTP (angl. *HyperText Transfer Protocol*) protokolo elektroninė informacija perduodama saugiu HTTPS (angl. *HyperText Transfer Protocol Secure*) protokolu;

40.4.2. naudojant virtualų privatų tinklą. Virtualiame tinkle turi būti naudojamas IPsec (angl. *Internet Protocol Security*) protokolų rinkinys;

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

40.5. šifro raktų ilgiai, šifro raktų generavimo algoritmai, šifro raktų apsikeitimo protokolai, sertifikato parašo šifravimo algoritmai bei kiti šifravimo algoritmai turi būti nustatomi atsižvelgiant į Lietuvos ir tarptautinių organizacijų ir standartų rekomendacijas, organizacinius ir techninius kibernetinio saugumo reikalavimus, Techninius valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinės sistemos ir kitų informacinės sistemos elektroninės informacijos saugos reikalavimus;

40.6. naudojamų šifravimo priemonių patikimumas turi būti vertinamas neeilinio arba kasmetinio informacinės sistemos rizikos vertinimo metu. Šifravimo priemonės turi būti operatyviai keičiamos nustačius saugumo spragų šifravimo algoritmuose.

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

41.1. atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į priimtiną elektroninės informacijos praradimą (angl. *recovery point objetive*) ir priimtiną informacinės sistemos neveikimo laikotarpį (angl. *recovery time objective*);

41.2. atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokia apimtimi, kad informacinės sistemos veiklos sutrikimo, elektroninės informacijos saugos (kibernetinio) incidento ar elektroninės informacijos vientisumo praradimo atvejais informacinės

sistemos neveikimo laikotarpis nebūtų ilgesnis, nei nustatyta konkrečioms informacinės sistemos svarbos kategorijoms, nurodytoms Saugos nuostatų 24 punkte, o elektroninės informacijos praradimas atitiktų priimtinumo kriterijus;

41.3. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai periodiškai, bet ne rečiau kaip nustatyta informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse, nurodytais terminais;

41.4. elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, dėl kurių nebūtų galima neteisėtai atkurti elektroninės informacijos;

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

41.6. atsarginių elektroninės informacijos kopijų darymas turi būti fiksuojamas;

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

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

42. Informacinės sistemos valdytojas ir (arba) informacinės sistemos tvarkytojas, pirkdamas paslaugas, darbus ar įrangą, susijusią 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 ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo reikalavimams.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

43. Informacinės sistemos naudotojų, informacinės sistemos administratorių, saugos įgaliotinio ir kibernetinio saugumo vadovo kvalifikacijos ir patirties reikalavimai:

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

43.2. visi informacinės sistemos naudotojai privalo turėti pagrindinių darbo kompiuteriu, taikomosiomis programomis įgūdžių, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, informacinės sistemos elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo laikyti jų paslaptį ir būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą;

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

43.4. saugos įgaliotiniu ar kibernetinio saugumo vadovu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinės sistemos 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 jos paskyrimo praėję mažiau kaip vieni metai;

43.5. informacinės sistemos administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti informacinės sistemos ir jose tvarkomos elektroninės informacijos saugą (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.). Informacinių sistemų administratoriai turi būti susipažinę su saugos dokumentais.

44. Informacinės sistemos naudotojų ir informacinės sistemos administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

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

44.2. 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, kibernetinio saugumo vadovo, informacinės sistemos naudotojų ar informacinės sistemos administratorių poreikius;

44.3. 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.).

44.4. informacinės sistemos naudotojams ir informacinės sistemos administratoriams mokymus gali vykdyti saugos įgaliotinis ar kitas informacinės sistemos valdytojo ar informacinės sistemos tvarkytojo darbuotojas, išmanantis elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, arba elektroninės informacijos saugos (kibernetinio saugumo) mokymų paslaugų teikėjas. Saugos įgaliotiniui ir kibernetinio saugumo vadovui mokymus gali vykdyti tik aukštos kvalifikacijos elektroninės informacijos saugos (kibernetinio saugumo) mokymų paslaugų teikėjas;

44.5. mokymai informacinės sistemos naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per dvejus metus. Mokymai saugos įgaliotiniui, kibernetinio saugumo vadovui ir informacinės sistemos administratoriams turi būti organizuojami pagal poreikį. Už mokymų organizavimą atsakingas saugos įgaliotinis;

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

45. Informacinės sistemos naudotojų supažindinimą su saugos dokumentais ar jų santrauka, atsakomybe už saugos dokumentų nuostatų pažeidimus organizuoja saugos įgaliotinis.

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

47. Pakartotinai su saugos dokumentais ar jų santrauka informacinės sistemos naudotojai supažindinami tik iš esmės pasikeitus informacinėms sistemoms arba elektroninės informacijos saugą (kibernetinį saugumą) reglamentuojantiems teisės aktams.

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

49. Informacinės sistemos naudotojai atsako už informacinės sistemos ir jose tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją. Informacinės sistemos naudotojai, informacinės sistemos administratoriai ir saugos įgaliotinis, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

50. Informacinės sistemos valdytojas saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Saugos dokumentai turi būti derinami su Lietuvos Respublikos vidaus reikalų ministerija ir Nacionaliniu kibernetinio saugumo centru. Keičiami saugos dokumentai gali būti nederinami su Lietuvos Respublikos vidaus reikalų ministerija ir Nacionaliniu kibernetinio saugumo centru tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos ir kibernetinio saugumo politikos nekeičiantys pakeitimai arba taisoma teisės technika. Nacionaliniam kibernetinio saugumo centrui turi būti pateiktos keičiamų saugos dokumentų kopijos.

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