LIETUVOS RESPUBLIKOS VYRIAUSIASIS VALSTYBINIS DARBO INSPEKTORIUS

ĮSAKYMAS

DĖL LIETUVOS RESPUBLIKOS VALSTYBINĖS DARBO INSPEKCIJOS PRIE SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS VALDOMŲ INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2019 m. birželio 28 d. Nr. EV-197
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybinės darbo inspekcijos įstatymo 8 straipsnio 2 dalies 1 punktu, Lietuvos Respublikos kibernetinio saugumo įstatymo 13 straipsnio 5 dalimi, 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, 12, 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:

1. T v i r t i n u pridedamus Lietuvos Respublikos valstybinės darbo inspekcijos prie Socialinės apsaugos ir darbo ministerijos valdomų informacinių sistemų duomenų saugos nuostatus;

2. S k i r i u:

2.1. Lietuvos Respublikos valstybinės darbo inspekcijos prie Socialinės apsaugos ir darbo ministerijos (toliau – VDI) Informacinių technologijų ir dokumentų valdymo skyriaus (toliau – IT skyrius) vyriausiąją specialistę Gretą Lelekauskaitę:

2.1.1 VDI valdomų informacinių sistemų (toliau – informacinės sistemos) saugos įgaliotiniu;

2.1.2. kibernetinio saugumo vadovu, atsakingu už informacinių sistemų kibernetinio saugumo organizavimą ir užtikrinimą;

2.2. informacinių sistemų koordinuojančiu administratoriumi VDI IT skyriaus vedėją Andrių Račkauską;

2.3. informacinių sistemų naudotojų administratoriumi VDI IT skyriaus vyriausiąją specialistę Valeriją Mačiulienę;

2.4. informacinių sistemų infrastruktūros administratoriumi VDI IT skyriaus vyriausiąjį

specialistą Raimondą Barkauską;

2.5. informacinių sistemų interneto svetainių administratoriumi VDI IT skyriaus vyriausiąjį specialistą Vilių Bagdoną;

2.6. informacinių sistemų kompiuterizuotų darbo vietų administratoriumi VDI IT skyriaus vyriausiąjį specialistą Justiną Grigaravičių.

3. Į p a r e i g o j u

3.1. informacinių sistemų saugos įgaliotinį per 6 mėnesius nuo šio įsakymo įsigaliojimo dienos teisės aktų nustatyta tvarka parengti ir pateikti Lietuvos Respublikos vyriausiajam valstybiniam darbo inspektoriui tvirtinti informacinių sistemų saugos politiką įgyvendinančius dokumentus;

3.2. VDI IT skyriaus vedėją Andriui Račkauską per 1 mėnesį nuo šio įsakymo įsigaliojimo dienos teisės aktų nustatyta tvarka parengti ir pateikti Lietuvos Respublikos vyriausiajam valstybiniam darbo inspektoriui tvirtinti įsakymą dėl Lietuvos Respublikos valstybinio darbo inspektoriaus 2010 m. rugsėjo 9 d. įsakymo Nr. V-293 „Dėl informacinių sistemų veiklos tęstinumo valdymo ir veiklos atkūrimo grupių sudarymo“ pakeitimo.

4. P r i p a ž į s t u netekusiais galios:

4.1. Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2010 m. liepos 14 d. įsakymą Nr. V-227 „Dėl Potencialiai pavojingų įrenginių valstybės registro duomenų saugos nuostatų patvirtinimo“;

4.2. Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2009 m. balandžio 1 d. įsakymą Nr. V-102 „Dėl DSS IS administravimo“ su visais pakeitimais ir papildymais;

4.3. Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2010 m. gegužės 25 d. įsakymą Nr. V-170 „Dėl Potencialiai pavojingų įrenginių valstybės registro administravimo“ su visais pakeitimais ir papildymais;

4.4. Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2011 m. lapkričio 5 d. įsakymą Nr. V-274 „Dėl darbuotojų saugos ir sveikatos klausimais atestavimo informacinės sistemos administravimo“ su visais pakeitimais ir papildymais;

4.5. Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2010 m. liepos 14 d. įsakymą Nr. V-225 „Dėl interneto svetainės administravimo“ su visais pakeitimais ir papildymais;

4.6. Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2016 m. vasario 19 d. įsakymą Nr. EV-54 „Dėl Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2014 m. spalio 23 d. įsakymo Nr. V-479 „Dėl saugos įgaliotinio skyrimo“ pakeitimo“.

4.7. Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2018 m. balandžio 20 d. įsakymą Nr. EV-95 „Dėl Lietuvos Respublikos valstybinės darbo inspekcijos prie Socialinės apsaugos ir darbo ministerijos valdomų informacinių sistemų duomenų saugos nuostatų patvirtinimo“.

5. P a v e d u:

5.1. VDI Informacinių technologijų ir dokumentų valdymo skyriaus vedėjui organizuoti šio įsakymo paskelbimą Teisės aktų registre (įsakymo 2 punktas neskelbiamas) ir VDI išorinėje ir vidinėje interneto svetainėje;

5.2. informacinių sistemų saugos įgaliotiniui, Lietuvos Respublikos valstybinės darbo inspekcijos prie Socialinės apsaugos ir darbo ministerijos Dokumentų valdymo tvarkos aprašo, patvirtinto Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2015 m. birželio 18 d. įsakymu Nr. V-211 „Dėl Lietuvos Respublikos valstybinės darbo inspekcijos prie Socialinės

apsaugos ir darbo ministerijos Dokumentų valdymo tvarkos aprašo patvirtinimo” nustatyta tvarka,

su šiuo įsakymu Dokumentų valdymo sistemos priemonėmis pasirašytinai supažindinti VDI darbuotojus – informacinių sistemų naudotojus;

5.3. šio įsakymo vykdymo kontrolę VDI kancleriui.

Lietuvos Respublikos vyriausiasis
valstybinis darbo inspektorius Jonas Gricius

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2019-06-19 raštu Nr. (4.2 E) 6K-412

PATVIRTINTA
Lietuvos Respublikos vyriausiojo valstybinio darbo inspektoriaus 2019 m. birželio 28 d. įsakymu Nr. EV-197

LIETUVOS RESPUBLIKOS VALSTYBINĖS DARBO INSPEKCIJOS PRIE SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS VALDOMŲ INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos valstybinės darbo inspekcijos prie Socialinės apsaugos ir darbo ministerijos valdomų informacinių sistemų saugos (kibernetinio saugumo) nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos Respublikos valstybinės darbo inspekcijos prie Socialinės apsaugos ir darbo ministerijos (toliau - Valstybinė darbo inspekcija) valdomų informacinių sistemų - Darbo sąlygų darbo vietose nuolatinės stebėsenos informacinės sistemos, Potencialiai pavojingų įrenginių valstybės registro, Darbuotojų saugos ir sveikatos klausimais atestavimo sistemos, vidaus administravimo informacinių sistemų (toliau kartu – informacinės sistemos) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Saugos nuostatuose vartojamos sąvokos:

2.1. **informacinių sistemų komponentai** – kompiuteriai, operacinės sistemos, duomenų bazės ir jų valdymo sistemos, taikomųjų programų sistemos, kompiuterių tinklo užkardos, įsilaužimų aptikimo ir prevencijos sistemos, elektroninės informacijos perdavimo tinklai, duomenų saugyklos, bylų tarnybinės stotys ir kita techninė ir programinė įranga, kurios pagrindu funkcionuoja informacinės sistemos ir užtikrinama informacinėse sistemose tvarkomos elektroninės informacijos sauga (kibernetinis saugumas);

2.2. **informacinių sistemų naudotojas** – Valstybinės darbo inspekcijos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, ar kitas asmuo, informacinių sistemų veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją;

2.3. **išorinis informacinių sistemų naudotojas** – su Valstybine darbo inspekcija tarnybos (darbo) santykiais nesusijęs asmuo, kuris informacinių sistemų veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudoja ir (ar) tvarko elektroninę informaciją;

2.4. **kibernetinio saugumo vadovas** – informacinių sistemų valdytojo paskirtas kompetentingas darbuotojas, valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, ar padalinys, atsakingas už informacinių sistemų kibernetinio saugumo organizavimą ir užtikrinimą;

2.5. **saugos (kibernetinio saugumo) dokumentai** – Saugos nuostatai, informacinių sistemų valdytojo patvirtinti informacinių sistemų saugos (kibernetinio saugumo) politiką įgyvendinantys dokumentai: informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės, informacinių sistemų veiklos tęstinumo valdymo planas, informacinių sistemų naudotojų administravimo taisyklės;

2.6. vartojama sąvoka **galinis įrenginys** suprantama taip, kaip ji apibrėžta Lietuvos Respublikos elektroninių ryšių įstatyme;

2.7. kitos Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašą, patvirtintą 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“, kituose teisės aktuose bei Lietuvos „Informacijos technologija. Saugumo metodai“ grupės standartuose apibrėžtas sąvokas.

3. Informacinių sistemų saugos (kibernetinio saugumo) dokumentų taikymas ir naudojimas:

3.1. Informacinių sistemų saugos (kibernetinio saugumo) dokumentai taikomi:

3.1.1. Valstybinei darbo inspekcijai (buveinės adresas – Algirdo g. 19, 03607 Vilnius), kuri yra Darbo sąlygų darbo vietose nuolatinės stebėsenos informacinės sistemos, Potencialiai pavojingų įrenginių valstybės registro, Darbuotojų saugos ir sveikatos klausimais atestavimo sistemos ir vidaus administravimo informacinių sistemų – Dokumentų valdymo sistemos, Personalo pokyčių valdymo sistemos, Rizikos vertinimo sistemos, Kokybės valdymo sistemos, Personalo atsakomybių ir atstovavimo sričių registro (DAARS) valdytojas ir tvarkytojas;

3.1.2. saugos įgaliotiniui, kibernetinio saugumo vadovui, informacinių sistemų administratoriams, informacinių sistemų naudotojams, informacinėms sistemoms funkcionuoti reikalingų paslaugų teikėjams;

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

3.3. Už informacinių sistemų saugos (kibernetinio saugumo) dokumentų santraukos parengimą atsakingas kibernetinio saugumo vadovas. Informacinių sistemų saugos (kibernetinio saugumo) dokumentų santrauka rengiama remiantis būtinumo žinoti principu.

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

3.5. Konkrečioms informacinėms sistemoms saugos (kibernetinio saugumo) dokumentuose nustatyti saugos organizaciniai ir techniniai reikalavimai taikomi atsižvelgiant į Saugos nuostatų 20 punkte joms priskirtą elektroninės informacijos svarbos kategoriją. Valstybinė darbo inspekcija, kaip informacinių sistemų valdytojas ir tvarkytojas, kiekvienai konkrečiai informacinei sistemai užtikrina saugos priemonių, skirtų ne žemesnei kategorijai negu Saugos nuostatuose informacinei sistemai priskirtai kategorijai, taikymą.

3.6. Saugos įgaliotinis, suderinęs su kibernetinio saugumo vadovu, sudaro saugos (kibernetinio saugumo) dokumentuose nustatytų informacinių sistemų saugos organizacinių ir techninių reikalavimų sąvadą pagal informacinių sistemų kategorijas (toliau - saugos reikalavimų sąvadas). Saugos reikalavimų sąvadui taikomos Saugos nuostatų 3.2 – 3.4 papunkčiuose nustatytos konfidencialumo nuostatos.

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

4.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti informacinių sistemų elektroninę informaciją;

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

4.3. vykdyti elektroninės informacijos saugos (kibernetinių saugumo) incidentų prevenciją, reaguoti į elektroninės informacijos saugos (kibernetinius saugumo) incidentus ir juos operatyviai suvaldyti, atkuriant įprastą informacinių sistemų veiklą.

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

5.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.2. informacinių sistemų veiklos tęstinumo užtikrinimas;

5.3. asmens duomenų apsauga;

5.4. informacinių sistemų naudotojų mokymas;

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

6. Už elektroninės informacijos saugą (kibernetinį saugumą) atsako Valstybinė darbo inspekcija, kaip informacinių sistemų valdytojas ir tvarkytojas.

7. Valstybinė darbo inspekcija, kaip informacinių sistemų valdytojas:

7.1. atsako už elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

7.2. tvirtina informacinių sistemų saugos (kibernetinio saugumo) politiką įgyvendinančius dokumentus, kitus dokumentus, susijusius su elektroninės informacijos sauga, ir jų pakeitimus;

7.3. skiria saugos įgaliotinį, kibernetinio saugumo vadovą ir informacinių sistemų administratorius;

7.4. priima sprendimus dėl informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo;

7.5. prižiūri ir kontroliuoja, kad informacinės sistemos būtų tvarkomos vadovaujantis Lietuvos Respublikos įstatymais, informacinių sistemų nuostatais, šiais Saugos nuostatais, informacinių sistemų saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais;

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

7.7. priima sprendimus dėl informacinių technologijų rizikos ir atitikties saugos reikalavimams vertinimo atlikimo;

7.8. prireikus tvirtina rizikos valdymo priemonių planą, informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

7.9. atlieka kitas Saugos nuostatuose ir kituose teisės aktuose informacinių sistemų valdytojo kompetencijai priskirtas funkcijas.

8. Valstybinė darbo inspekcija, kaip informacinių sistemų tvarkytojas:

8.1. užtikrina nepertraukiamą informacinių sistemų veikimą;

8.2. užtikrina informacinių sistemų elektroninės informacijos saugą (kibernetinį saugumą) ir saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais (automatiniu būdu);

8.3. užtikrina informacinių sistemų sąveiką su susijusiais registrais ir informacinėmis sistemomis;

8.4. teikia informacinių sistemų valdytojo vadovui pasiūlymus dėl informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo;

8.5. rengia ir įgyvendina techninių ir programinių priemonių kūrimo ir plėtros planus, investicinius projektus;

8.6. ne rečiau kaip kartą per metus organizuoja elektroninės informacijos saugos (kibernetinio saugumo) dokumentų persvarstymą (peržiūrėjimą);

8.7. organizuoja informacinių sistemų naudotojams mokomuosius ir pažintinius kursus informacinių sistemų elektroninės informacijos tvarkymo klausimais;

8.8. atlieka kitas Saugos nuostatuose ir kituose teisės aktuose informacinių sistemų tvarkytojo kompetencijai priskirtas funkcijas.

9. Informacinių sistemų valdytojo paskirtas saugos įgaliotinis, koordinuodamas ir prižiūrėdamas informacinių sistemų saugos politikos įgyvendinimą, atlieka šias funkcijas:

9.1. teikia informacinių sistemų valdytojo vadovui pasiūlymus dėl:

9.1.1. administratoriaus (administratorių) paskyrimo ir reikalavimų administratoriui (administratoriams) nustatymo;

9.1.2. informacinių technologijų saugos atitikties vertinimo 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“;

9.2. teikia informacinių sistemų valdytojo vadovui pasiūlymus dėl elektroninės informacijos (kibernetinio saugumo) dokumentų priėmimo ir keitimo;

9.3. koordinuoja elektroninės informacijos saugos (kibernetinio saugumo) incidentų tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, elektroninės 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;

9.4. teikia informacinių sistemų administratoriams ir informacinių sistemų naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimo;

9.5. organizuoja informacinių sistemų rizikos ir informacinių technologijų saugos atitikties vertinimą;

9.6. organizuoja informacinių sistemų naudotojams ir administratoriams mokomuosius ir pažintinius kursus informacinių sistemų elektroninės informacijos saugos klausimais;

9.7. atlieka kitas Saugos nuostatuose, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių 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 saugos įgaliotiniui priskirtas funkcijas.

10. Informacinių sistemų valdytojo paskirtas kibernetinio saugumo vadovas 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“, kituose teisės aktuose nustatytas funkcijas. Kibernetinio saugumo vadovas ir saugos įgaliotinis gali būti tas pats asmuo.

11. Saugos įgaliotinis ir kibernetinio saugumo vadovas negali atlikti informacinių sistemų administratoriaus funkcijų.

12. Informacinių sistemų administratoriai gali būti skiriami kelioms valdytojo valdomoms informacinėms sistemoms ir (ar) kelių Saugos nuostatų 13 punkte apibrėžtų informacinių sistemų administratorių grupių funkcijoms atlikti.

13. Informacinių sistemų administratoriai pagal atliekamas funkcijas skirstomi į šias grupes:

13.1. koordinuojantis administratorius, kuris prižiūri informacinių sistemų administratorių veiklą, siekdamas užtikrinti tinkamą informacinių sistemų administratorių funkcijų vykdymą;

13.2. informacinių sistemų naudotojų administratoriai, kurie atlieka informacinių sistemų naudotojų teisių valdymo funkcijas (informacinių sistemų naudotojų duomenų administravimas, klasifikatorių tvarkymas, informacinių sistemų naudotojų veiksmų, registracijos žurnalų įrašų analizė ir kt.);

13.3. informacinių sistemų komponentų administratoriai, kurie atlieka funkcijas, susijusias su jų kompetencijai priskirtais informacinių sistemų komponentais:

13.4. kompiuterių tinklo administratorius atlieka šias funkcijas:

13.4.1. užtikrina kompiuterinių tinklų veikimą;

13.4.2. projektuoja kompiuterinius tinklus;

13.4.3. diegia, konfigūruoja ir prižiūri kompiuterinių tinklų aktyviąją įrangą;

13.4.4. užtikrina kompiuterinių tinklų saugumą;

13.5. tarnybinių stočių administratorius atlieka šias funkcijas:

13.5.1. užtikrina tarnybinių stočių veikimą;

13.5.2. konfigūruoja tarnybinių stočių tinklo prieigą;

13.5.3. administruoja tarnybinių stočių naudotojų registracijos į tarnybines stotis duomenis;

13.5.4. stebi ir analizuoja tarnybinių stočių veiklą;

13.5.5. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

13.5.6. diegia tarnybinių stočių programinės įrangos atnaujinamus;

13.5.7. užtikrina tarnybinių stočių saugą;

13.6. duomenų bazių administratorius atlieka šias funkcijas:

13.6.1. užtikrina duomenų bazių veikimą;

13.6.2. tvarko duomenų bazių programinę įrangą;

13.6.3. administruoja duomenų bazių naudotojų registracijos į duomenų bazes duomenis;

13.6.4. kuria ir atkuria atsargines elektroninės informacijos kopijas;

13.6.5. stebi duomenų bazes ir optimizuoja jų funkcionavimą;

13.7. saugos administratorius, kuris atlieka informacinių sistemų pažeidžiamų vietų nustatymo, saugumo reikalavimų atitikties nustatymo ir stebėsenos funkcijas;

13.8. kitų informacinių sistemų komponentų administratoriai atlieka funkcijas, susijusias su naudotojų darbo vietų techninės ir programinės įrangos ir, pareigybių aprašymuose priskirtos kompetencijos ribose kitų, informacinių sistemų komponentų sąranka, veikimo stebėsena ir analize, profilaktine priežiūra, programinės įrangos diegimu ir konfigūravimu, trikdžių diagnostika ir šalinimu, nepertraukiamo informacinių sistemų veikimo užtikrinimu, pasiūlymų dėl jų veikimo optimizavimo teikimu.

14. Informacinių sistemų administratoriai yra atsakingi už tinkamą saugos (kibernetinio saugumo) dokumentuose ir pareigybių aprašymuose jiems priskirtų funkcijų vykdymą.

15. Informacinių sistemų administratoriai privalo:

15.1. vykdyti visus saugos įgaliotinio ir kibernetinio saugumo vadovo nurodymus bei pavedimus dėl informacinių sistemų saugos (kibernetinio saugumo) užtikrinimo;

15.2. pagal saugos (kibernetinio saugumo) dokumentuose ir pareigybių aprašymuose priskirtą kompetenciją reaguoti į elektroninės informacijos saugos (kibernetinio saugumo) incidentus;

15.3. nuolat teikti saugos įgaliotiniui ir kibernetinio saugumo vadovui informaciją apie saugą užtikrinančių informacinių sistemų komponentų būklę.

16. Informacinių sistemų komponentų administratoriai:

16.1. atlikdami informacinių sistemų sąrankos pakeitimus turi laikytis informacinių sistemų pokyčių valdymo tvarkos, nustatytos informacinių sistemų valdytojo tvirtinamose informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse;

16.2. privalo patikrinti (peržiūrėti) jiems priskirtų informacinių sistemų komponentų sąranką ir informacinių sistemų komponentų būsenos rodiklius ne rečiau kaip kartą per metus ir (arba) po informacinių sistemų pokyčio.

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

17.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

17.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

17.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

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

17.5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

17.6. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

17.7. 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;

17.8. Lietuvos standartai LST ISO/IEC 27002 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir LST ISO/IEC 27001 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai.“, kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys elektroninės informacijos saugos valdymą;

17.9. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugos ir kibernetinio saugumo valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

18. Informacinėse sistemose tvarkoma elektroninė informacija vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Klasifikavimo gairių aprašas) priskiriama šioms elektroninės informacijos svarbos kategorijoms:

18.1. Darbo sąlygų darbo vietose nuolatinės stebėsenos informacinėje sistemoje tvarkoma elektroninė informacija priskiriama svarbios elektroninės informacijos kategorijai vadovaujantis Klasifikavimo gairių aprašo 8.1, 8.2 ir 8.3 papunkčių nuostatomis;

18.2. Potencialiai pavojingų įrenginių valstybės registre tvarkoma elektroninė informacija priskiriama svarbios elektroninės informacijos kategorijai vadovaujantis Klasifikavimo gairių aprašo 8.1 ir 8.4 papunkčių nuostatomis;

18.3. Darbuotojų saugos ir sveiktos klausimais atestavimo sistemoje ir vidaus administravimo informacinėse sistemose tvarkoma informacija priskiriama mažiausios svarbos elektroninės informacijos kategorijai vadovaujantis Klasifikavimo gairių aprašo 10 punkto nuostatomis.

19. Informacinės sistemos pagal tvarkomos elektroninės informacijos svarbą priskiriamos šioms kategorijoms:

19.1. Darbo sąlygų darbo vietose nuolatinės stebėsenos informacinė sistema ir Potencialiai pavojingų įrenginių valstybės registras priskiriama antrajai kategorijai vadovaujantis Klasifikavimo gairių aprašo 12.2 papunkčiu;

19.2. Darbuotojų saugos ir sveikatos klausimais atestavimo sistema ir vidaus administravimo informacinės sistemos priskiriamos ketvirtajai kategorijai vadovaujantis Klasifikavimo gairių aprašo 12.4 papunkčiu.

20. Informacinėse sistemose tvarkomi asmens duomenys vadovaujantis 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.

21. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus, kasmet, jei teisės aktai nenustato kitaip, organizuoja informacinių sistemų rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį informacinių sistemų rizikos vertinimą. Informacinių sistemų tvarkytojo rašytiniu pavedimu informacinių sistemų rizikos vertinimą gali atlikti pats saugos įgaliotinis. Kartu su informacinių sistemų rizikos įvertinimu ir (arba) Saugos nuostatų 25 punkte nurodytu informacinių technologijų saugos atitikties vertinimu turi būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinių sistemų kibernetiniam saugumui, vertinimas.

22. Informacinių sistemų rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama informacinių sistemų valdytojo 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:

22.1. 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);

22.2. 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);

22.3. 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.

23. Atsižvelgdamas į rizikos vertinimo ataskaitą, informacinių sistemų valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame taip pat numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

24. 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 reikalavimams stebėsenos sistemai, Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymas Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

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

25.1. informacinių sistemų informacinių technologijų saugos atitikties vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus, jei teisės aktai nenumato kitaip;

25.2. informacinių sistemų atitikties 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“, nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

26. 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.

27. Kibernetinių atakų imitavimas atliekamas šiais etapais:

27.1. 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 valdytojo vadovu ir vykdomas tik gavus jo rašytinį pritarimą;

27.2. 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 kitą sėkmingai kibernetinei atakai įvykdyti reikalingą informaciją. Šiame etape turi būti teikiamos tarpinės ataskaitos apie vykdomas veiklas ir jos rezultatus;

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

27.4. 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. Kiekvienas aptiktas pažeidžiamumas turi būti detalizuojamas ir pateikiamos rekomendacijos jam pašalinti. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos įvertimu. Jeigu nustatoma incidentų valdymo ir šalinimo, taip pat informacinių sistemų valdytojo įstaigos nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinami veiklos tęstinumo planai.

28. Informacinių sistemų saugos atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje, patvirtintoje Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, nustatyta tvarka. Atlikus informacinių technologijų saugos atitikties vertinimą, saugos įgaliotinis rengia ir teikia informacinių sistemų valdytojo 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 informacinių sistemų valdytojo vadovas.

29. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas informacinių sistemų valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymas Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

30. Elektroninės informacijos saugos (kibernetinio saugumo) būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) priemonėmis, jas parenkant vadovaujantis šiais pagrindiniais principais:

30.1. saugos priemonės turi būti valdomos centralizuotai;

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

30.3. likutinė rizika turi būti sumažinta iki priimtino lygio;

30.4. kur galima, būtina įdiegti prevencines informacijos saugos priemones.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

31. Informacinėse sistemose naudojamų svetainių saugos valdymo reikalavimai:

31.1. svetainės turi atitikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, reikalavimus, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimus, patvirtintus Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

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

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

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

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

32. Programinės įrangos, skirtos informacinėms sistemoms apsaugoti nuo kenksmingos programinės įrangos, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

32.1. tarnybinėse stotyse ir vidinių informacinių sistemų naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo ir stebėjimo realiu laiku priemonės;

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

32.3. kenksmingos programinės įrangos aptikimo priemonės turi atsinaujinti automatiškai ne rečiau kaip kartą per 24 valandas. Informacinių sistemų komponentų administratoriai turi būti automatiškai informuojami elektroniniu paštu apie tai, kuriems informacinių sistemų posistemiams, funkciškai savarankiškoms sudedamosioms dalims, vidinių informacinių sistemų naudotojų kompiuteriams ir kitiems informacinių sistemų komponentams yra pradelstas kenksmingos programinės įrangos aptikimo priemonių atsinaujinimo laikas, kenksmingos programinės įrangos aptikimo priemonės netinkamai funkcionuoja arba yra išjungtos.

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

33.1. informacinių sistemų tarnybinėse stotyse ir vidinių informacinių sistemų naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga;

33.2. vidinių informacinių sistemų naudotojų kompiuteriuose naudojama programinė įranga turi būti įtraukta į su informacinių sistemų valdytoju suderintą leistinos naudoti programinės įrangos sąrašą. Leistinos programinės įrangos sąrašą turi parengti, ne rečiau kaip kartą per metus peržiūrėti ir prireikus atnaujinti saugos įgaliotinis;

33.3. tarnybinių stočių ir vidinių informacinių sistemų 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;

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

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

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

33.7. taikomoji programinė įranga turi būti testuojama naudojant atskirą testavimo aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB;

33.8. informacinių sistemų 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.

34. Kompiuterių tinklo filtravimo įrangos pagrindinės naudojimo nuostatos:

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

34.2. kompiuterių tinklų perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešuose ryšių tinkluose naršančių vidinių informacinių sistemų 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;

34.3. apsaugai nuo elektroninės informacijos neteisėto atskleidimo turi būti naudojama duomenų srautų analizės ir kontrolės įranga;

34.4. turi būti naudojamos turinio filtravimo sistemos;

34.5. turi būti naudojamos taikomųjų programų kontrolės sistemos.

35. Leistinos kompiuterių naudojimo ribos:

35.1. stacionarius kompiuterius leidžiama naudoti tik informacinių sistemų valdytojo ir tvarkytojo patalpose;

35.2. nešiojamiesiems kompiuteriams, išnešamiems iš informacinių sistemų valdytojo ar informacinių sistemų tvarkytojo patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimai ir pan.);

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

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

36.1. elektroninė informacija teikiama (daugkartinio teikimo atveju ir vienkartinio teikimo atveju) informacinių sistemų nuostatuose nustatyta tvarka;

36.2. 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;

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

36.4. nuotolinis prisijungimas prie informacinių sistemų galimas:

36.4.1. naudojant transporto lygmens protokolus (angl. Transport Layer Secure) (toliau – TLS), reglamentuojančius informacinių sistemų naudotojo ir serverio abipusį tapatumo nustatymą, kad būtų užtikrintas šifruotas ryšys. Siekiant, kad elektroninės informacijos perdavimas iš serverio į interneto naršyklę ir iš interneto naršyklės į serverį būtų saugus, naudojamas TLS sertifikatas, patvirtinantis elektroninės informacijos šaltinio tapatumą ir šifruojantis informacinių sistemų naudotojo ir serverio siunčiamą ir gaunamą elektroninę informaciją. Informacinių sistemų interneto svetainėse TLS šifruota HTTP (angl. HyperText Transfer Protocol) protokolo elektroninė informacija perduodama saugiu HTTPS (angl. HyperText Transfer Protocol Secure) protokolu;

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

36.4.3. naudojant saugaus apvalkalo protokolą (angl. Secure Shell) ir nuotolinio darbalaukio protokolą (angl. Remote Desktop Protocol). Šia galimybe gali būti pasinaudota tik informacinių sistemų administravimo tikslais;

36.5. šifro raktų ilgiai, šifro raktų generavimo algoritmai, šifro raktų apsikeitimo protokolai, sertifikato parašo šifravimo algoritmai ir kiti šifravimo algoritmai turi būti nustatomi atsižvelgiant į Lietuvos ir tarptautinių organizacijų ir standartų rekomendacijas, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtintus Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, reikalavimus, Techninius valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimus, patvirtintus Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

36.6. naudojamų šifravimo priemonių patikimumas turi būti vertinamas neeilinio arba kasmetinio informacinių sistemų rizikos vertinimo metu. Šifravimo priemonės turi būti operatyviai keičiamos nustačius saugumo spragų šifravimo algoritmuose.

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

37.1. atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į priimtiną elektroninės informacijos praradimą (angl. recovery point objetive) ir priimtiną informacinių sistemų neveikimo laikotarpį (angl. recovery time objective);

37.2. atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokios apimties, kad informacinių sistemų veiklos sutrikimo, elektroninės informacijos saugos (kibernetinio) incidento ar elektroninės informacijos vientisumo praradimo atvejais informacinių sistemų neveikimo laikotarpis nebūtų ilgesnis, nei taikoma konkrečioms informacinių sistemų svarbos kategorijoms, nurodytoms Saugos nuostatų 19 punkte, o elektroninės informacijos praradimas atitiktų priimtinumo kriterijus;

37.3. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai, bet ne rečiau kaip atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarkoje, nustatytoje informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse, nurodytais terminais;

37.4. 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;

37.5. atsarginės elektroninės informacijos kopijos turi būti saugomos kitose patalpose, nei yra informacinių sistemų tarnybinės stotys ar įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate. Atsarginių elektroninės informacijos kopijų saugojimo terminai nustatomi atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarkoje;

37.6. atsarginių elektroninės informacijos kopijų darymas turi būti fiksuojamas;

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

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

38. Informacinių sistemų valdytojas, pirkdamas paslaugas, darbus ar įrangą, susijusius su informacinėmis sistemomis, jų projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį Organizaciniams ir techniniams kibernetinio saugumo reikalavimams, taikomiems kibernetinio saugumo subjektams, apraše, patvirtintiems Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, reikalavimams.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

39. Reikalavimai informacinių sistemų naudotojų, informacinių sistemų administratorių, saugos įgaliotinio ir kibernetinio saugumo vadovo kvalifikacijai ir patirčiai:

39.1. vidinių informacinių sistemų naudotojų, administratorių, saugos įgaliotinio, kibernetinio saugumo vadovo kvalifikacija turi atitikti bendruosius ir specialiuosius reikalavimus, nustatytus jų pareigybių aprašymuose;

39.2. visi informacinių sistemų 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, informacinių sistemų elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo saugoti jų paslaptį ir būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį. Asmens įsipareigojimas saugoti paslaptį galioja ir nutrukus su elektroninės informacijos tvarkymu susijusiai veiklai;

39.3. saugos įgaliotinis ir kibernetinio saugumo vadovas privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos (kibernetinio saugumo) srityje, savo darbe vadovautis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, „Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą (kibernetinį saugumą). Informacinių tvarkytojas turi sudaryti sąlygas kelti saugos įgaliotinio ir kibernetinio saugumo vadovo kvalifikaciją;

39.4. saugos įgaliotiniu ar kibernetinio saugumo vadovu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai;

39.5. informacinių sistemų administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti informacinių sistemų ir jose tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti informacinių sistemų komponentus (stebėti informacinių sistemų komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti informacinių sistemų komponentų nepertraukiamą funkcionavimą ir pan.). Informacinių sistemų administratoriai turi būti susipažinę su saugos dokumentais.

40. Informacinių sistemų naudotojų ir informacinių sistemų administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

40.1. informacinių sistemų naudotojams turi būti organizuojami mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais, įvairiais būdais primenama apie elektroninės informacijos saugos (kibernetinio saugumo) problemas.

40.2. 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), informacinių sistemų naudotojų ar informacinių sistemų administratorių poreikius;

40.3. mokymai gali būti vykdomi tiesioginiu ar nuotoliniu būdu. Mokymus gali vykdyti saugos įgaliotinis ar kitas informacinių sistemų valdytojo ir informacinių sistemų tvarkytojo darbuotojas, išmanantis elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, arba elektroninės informacijos saugos (kibernetinio saugumo) mokymų paslaugų teikėjas;

40.4. mokymai informacinių sistemų naudotojams turi būti organizuojami ne rečiau kaip kartą per dvejus metus. Mokymai informacinių sistemų administratoriams turi būti organizuojami pagal poreikį. Už mokymų organizavimą atsakingas saugos įgaliotinis;

40.5. saugos įgaliotinis ne rečiau kaip kartą per dvejus metus organizuoja mokymus informacinių sistemų naudotojams elektroninės informacijos saugos ir kibernetinio saugumo klausimais;

40.6. saugos įgaliotinis informacinių sistemų naudotojus nuolatos informuoja apie aktualias elektroninės informacijos saugos problemas.

V SKYRIUS
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

41. Informacinių sistemų naudotojų ir administratorių supažindinimą su saugos (kibernetinio saugumo) dokumentais ar jų santrauka ir atsakomybe už saugos (kibernetinio saugumo) dokumentų nuostatų pažeidimus organizuoja saugos įgaliotinis.

42. Informacinių sistemų naudotojai ir administratoriai su saugos (kibernetinio saugumo) dokumentais ar jų santrauka turi būti supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo teisinį įrodomumą.

43. Pakartotinai su saugos (kibernetinio saugumo) dokumentais ar jų santrauka informacinių sistemų naudotojai ir administratoriai supažindinami tik iš esmės pasikeitus informacinėms sistemoms arba elektroninės informacijos saugą (kibernetinį saugumą) reglamentuojantiems teisės aktams.

44. Tvarkyti informacinių sistemų elektroninę informaciją gali tik asmenys, susipažinę su saugos (kibernetinio saugumo) dokumentais ir sutikę laikytis jų reikalavimų.

45. Informacinių sistemų naudotojai savo kompetencijos ribose atsako už informacinių sistemų ir jose tvarkomos elektroninės informacijos saugą (kibernetinį saugumą). Saugos įgaliotinis, kibernetinio saugumo vadovas, informacinių sistemų naudotojai, informacinių sistemų administratoriai ar kiti asmenys, pažeidę saugos (kibernetinio saugumo) dokumentų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

46. Informacinių sistemų valdytojas saugos (kibernetinio saugumo) dokumentus turi persvarstyti (peržiūrėti) ne rečiau kaip kartą per kalendorinius metus. Saugos (kibernetinio saugumo) dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos įvertinimą ar informacinių

technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams ar kitiems informacinių sistemų valdytojo ir tvarkytojo veiklos pokyčiams.

_____