VYRIAUSIOSIOS TARNYBINĖS ETIKOS KOMISIJOS PIRMININKAS

ĮSAKYMAS DĖL VYRIAUSIOSIOS TARNYBINĖS ETIKOS KOMISIJOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2018 m. balandžio 12 d. Nr. T-14
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 30 straipsniu, 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 ir 19 punktais, Lietuvos Respublikos vyriausiosios tarnybinės etikos komisijos įstatymo 13 straipsnio 2 dalimi:

1. T v i r t i n u Vyriausiosios tarnybinės etikos komisijos duomenų saugos nuostatus (pridedama).

2. S k i r i u Prevencijos skyriaus vedėją Eveliną Matulaitienę saugos įgaliotine (kibernetinio saugumo vadove).

3. P a v e d u per 2 mėnesius nuo Vyriausiosios tarnybinės etikos komisijos (toliau – Komisija) duomenų saugos nuostatų patvirtinimo dienos Komisijos Prevencijos skyriui parengti ir teikti Komisijos pirmininkui patvirtinti saugos politiką įgyvendinančius dokumentus.

Komisijos narys, laikinai einantis
Komisijos pirmininko pareigas Saulius Katuoka

PATVIRTINTA
Vyriausiosios tarnybinės etikos komisijos
pirmininko
2018 m. balandžio 12 d. įsakymu Nr. T-14

VYRIAUSIOSIOS TARNYBINĖS ETIKOS KOMISIJOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Vyriausiosios tarnybinės etikos komisijos (toliau - Komisija arba VTEK) duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Privačių interesų registro (toliau – PIR), Privačių interesų deklaracijų tvarkymo informacinės sistemos (toliau - PIDTIS) ir Lobistų informacinės sistemos (toliau - LOBIS) veiklos elektroninės informacijos saugos (kibernetinio saugumo) valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui ir naudotojų supažindinimo su saugos dokumentais principus.

2. VTEK saugos politiką papildomai reglamentuoja šie dokumentai (toliau – Saugos politikos dokumentai):

2.1. VTEK saugaus elektroninės informacijos tvarkymo taisyklės;

2.2. VTEK naudotojų administravimo taisyklės;

2.3. VTEK veiklos tęstinumo valdymo planas.

3. Saugos nuostatuose vartojamos sąvokos atitinka PIR, PIDTIS ir LOBIS nuostatuose, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarime Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas), Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 (Lietuvos Respublikos Vyriausybės 2016 m. rugpjūčio 11 d. nutarimo Nr. 826 redakcija) „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), Bendruosiuose reikalavimuose organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintuose 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) ir kituose teisės aktuose bei Lietuvos standartuose LST ISO/IEC 27002:2014 ir LST ISO/IEC 27001:2013 vartojamas sąvokas.

4. VTEK duomenų saugos tikslas – užtikrinti PIR, PIDTIS ir LOBIS elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei tinklo įrangos funkcionavimą. Duomenų saugai užtikrinti kompleksiškai naudojamos organizacinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo, atsakomybės, elektroninės informacijos saugos (kibernetinio saugumo) lygio kėlimo, saugos priemonių projektavimo ir diegimo principus.

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

5.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas naudojant organizacines, technines ir programines priemones:

5.1.1. elektroninės informacijos konfidencialumas užtikrinamas techninėmis ir organizacinėmis priemonėmis ribojant priėjimą prie asmens duomenų ir ypatingų asmens duomenų, priėjimą suteikiant tik teisėtiems PIR, PIDTIS ir LOBIS tvarkytojo naudotojams, kurių tapatybė yra nustatyta, ir tik prie tos elektroninės informacijos, kuri yra būtina naudotojo veiklos funkcijoms vykdyti, supažindinant PIR, PIDTIS ir LOBIS administratorių ir naudotojus su konfidencialaus asmens duomenų tvarkymo principais;

5.1.2. elektroninės informacijos vientisumas užtikrinamas valdant teisėtą elektroninės informacijos ar PIR, PIDTIS ir LOBIS keitimą, kontroliuojant duomenų įvedimą, stebint ir reaguojant į galimą neteisėtą duomenų ar PIR, PIDTIS ir LOBIS keitimą ar sunaikinimą, PIR, PIDTIS ir LOBIS administratorių ir naudotojus supažindinant su klaidų ir vientisumo pažeidimo nustatymo ir koregavimo metodais ir tvarkų aprašais.;

5.1.3. elektroninės informacijos prieinamumas užtikrinamas organizacinėmis ir technologinėmis priemonėmis valdant PIR, PIDTIS ir LOBIS, jų elementų ar duomenų keitimus, naudojant perteklines ar alternatyvias registrų ir duomenų tinklų technologines priemones, atliekant PIR, PIDTIS ir LOBIS ir veiklos tęstinumo valdymo plano bandymus.

5.2. kitos prioritetinės kryptys:

5.2.1. organizacinių saugaus darbo su duomenimis, asmens duomenimis ir ypatingais asmens duomenimis priemonių įgyvendinimas ir kontrolė (duomenų gavėjų ir teikėjų, tvarkytojų teisių, įpareigojimų, atsakomybės ribų, detalių saugaus elektroninės informacijos tvarkymo taisyklių nustatymas, mokymai);

5.2.2. technologinė elektroninės informacijos apdorojimo priemonių (tarnybinių stočių saugojimo patalpų, tarnybinių stočių, elektroninės informacijos perdavimo įrangos, programinės įrangos) apsauga;

5.2.3. programinių apsaugos priemonių taikymas ir programinės įrangos diegimo kontrolė (apsaugos nuo kenksmingos programinės įrangos, programinės įrangos diegimo, naudojimo ir atnaujinimo taisyklių nustatymas).

6. Saugos nuostatai taikomi:

6.1. PIR, PIDTIS ir LOBIS valdytojui ir tvarkytojui, PIR, PIDTIS ir LOBIS saugos įgaliotiniui (kibernetinio saugumo vadovui), PIR, PIDTIS ir LOBIS administratoriui ir PIR, PIDTIS ir LOBIS naudotojams.

7. PIR, PIDTIS ir LOBIS valdytojas ir tvarkytojas yra Vyriausioji tarnybinės etikos komisija (Vilniaus g. 27, LT-01402 Vilnius).

8. Komisijos, kaip PIR, PIDTIS ir LOBIS valdytojo ir tvarkytojo funkcijos:

8.1. atsako už saugos politikos formavimą, įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

8.2. organizuoja PIR, PIDTIS ir LOBIS veiklą ir jai vadovauja;

8.3. tvirtina dokumentus, susijusius su PIR, PIDTIS ir LOBIS sauga;

8.4. priima sprendimą dėl PIR, PIDTIS ir LOBIS informacinių technologijų saugos atitikties vertinimo atlikimo;

8.5. priima sprendimą dėl PIR, PIDTIS ir LOBIS rizikos vertinimo atlikimo;

8.6. priima sprendimą dėl įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio PIR, PIDTIS ir LOBIS veiklai vertinimo (testavimo);

8.7. užtikrina PIR, PIDTIS ir LOBIS pokyčių valdymą;

8.8. užtikrina, kad PIR, PIDTIS ir LOBIS veiktų nepertraukiamai;

8.9. skiria PIR, PIDTIS ir LOBIS saugos įgaliotinį (kibernetinio saugumo vadovą) ir paveda jam organizuoti ir kontroliuoti PIR, PIDTIS ir LOBIS saugos politikos įgyvendinimą;

8.10. skiria PIR, PIDTIS ir LOBIS administratorių ir paveda jam užtikrinti PIR, PIDTIS ir LOBIS kompiuterinės įrangos ir naudotojų kompiuterizuotų darbo vietų saugų funkcionavimą, administruoti PIR, PIDTIS ir LOBIS duomenų bazę (-es) saugos dokumentų ir kitų teisės aktų nustatyta tvarka;

8.11. Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų

ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos (toliau - ARSIS) tvarkytojui teikia prašymus užregistruoti PIR, PIDTIS ir LOBIS saugos įgaliotinį (kibernetinio saugumo vadovą) ir kitus už duomenų pateikimą paskirtus atsakingus asmenis ARSIS naudotojais ir suteikti jiems prieigos teises;

8.12. ARSIS nuostatų nustatyta tvarka teikia ARSIS patvirtintų saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas, rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas, informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas;

8.13. Registrų ir valstybės informacinių sistemų registro nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2012 m. spalio 16 d. nutarimu Nr. 1263 „Dėl Registrų sąrašo reorganizavimo į Registrų ir valstybės informacinių sistemų registrą ir registrų ir valstybės informacinių sistemų registro nuostatų patvirtinimo“, nustatyta tvarka, pateikia šiam registrui patvirtintus Saugos nuostatus ar jų pakeitimus bei kitus reikiamus duomenis ar dokumentų kopijas;

8.14. Pirkdamas paslaugas, darbus ar įrangą, susijusius su PIR, PIDTIS ir LOBIS, jų projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose nustato, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas privalo užtikrinti atitiktį Kibernetinio saugumo reikalavimų apraše patvirtintiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams;

8.15. PIR, PIDTIS ir LOBIS valdytojo ir duomenų gavėjų sutarčių dėl duomenų teikimo nustatyta tvarka automatiškai teikia PIR, PIDTIS ir LOBIS duomenis duomenų gavėjams bei užtikrina duomenų saugą iki duomenys pasiekia duomenų gavėją sutartyse numatytomis sąlygomis ir tvarka;

8.16. užtikrina naudotojų darbo vietose naudojamų organizacinių, techninių ir programinių priemonių, užtikrinančių duomenų saugą, diegimą ir priežiūrą;

8.17. atlieka kitas PIR, PIDTIS ir LOBIS nuostatų, Saugos nuostatų ir teisės aktų nustatytas saugaus elektroninės informacijos tvarkymo funkcijas.

9. Saugos įgaliotinis (kibernetinio saugumo vadovas):

9.1. įgyvendina duomenų saugą, vadovaudamasis duomenų saugą reglamentuojančiais dokumentais bei duomenų saugą reglamentuojančiais teisės aktais;

9.2. atsako už PIR, PIDTIS ir LOBIS saugos politikos dokumentų reikalavimų vykdymą ir saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

9.3. teikia valdytojui siūlymus dėl:

9.3.1. saugos dokumentų priėmimo, keitimo ar panaikinimo;

9.3.2. PIR, PIDTIS ir LOBIS informacinių technologijų saugos atitikties vertinimo atlikimo;

9.4. nustato reikalavimus administratoriui ir teikia PIR, PIDTIS ir LOBIS valdytojo vadovui siūlymus dėl administratoriaus paskyrimo;

9.5. registruoja elektroninės informacijos saugos (kibernetinio saugumo) incidentus;

9.6. koordinuoja elektroninės informacijos saugos (kibernetinio saugumo) incidentų, įvykusių PIR, PIDTIS ir LOBIS, tyrimą ir bendradarbiauja su kompetentingoms institucijoms, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo (kibernetinio saugumo) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetinio saugumo) incidentais;

9.7. teikia administratoriui ir naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos ir kibernetinio saugumo politikos įgyvendinimu;

9.8. pasirašytinai supažindina administratorių ir naudotojus su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais, kuriais turi būti vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, bei atsakomybę už šių reikalavimų nesilaikymą;

9.9. organizuoja administratoriaus, naudotojų kvalifikacijos tobulinimą duomenų saugos ir kibernetinio saugumo klausimais, reguliariai jiems primena saugos problemas (elektroniniu paštu, parengia atmintines naujai priimtiems darbuotojams ir pan.);

9.10. organizuoja rizikos įvertinimą (prireikus ir neeilinius rizikos vertinimus);

9.11. atlieka kitas Saugos nuostatuose, saugos politiką įgyvendinančiuose dokumentuose ir teisės aktuose nustatytas saugos įgaliotinio funkcijas.

10. PIR, PIDTIS ir LOBIS administratorius:

10.1. atsako už PIR, PIDTIS ir LOBIS funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugų administravimą ir veiklos užtikrinimą;

10.2. registruoja PIR, PIDTIS ir LOBIS naudotojus, tvarko (suteikia, sustabdo, panaikina) naudotojų prieigos teises naudotis PIR, PIDTIS ir LOBIS paskirtoms funkcijoms atlikti;

10.3. vertina naudotojų pasirengimą darbui su PIR, PIDTIS ir LOBIS;

10.4. pagal kompetenciją rengia pasiūlymus dėl PIR, PIDTIS ir LOBIS kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir duomenų saugos užtikrinimo;

10.5. atlieka PIR, PIDTIS ir LOBIS sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų) priežiūrą ir administravimą, pažeidžiamų vietų nustatymą ir saugos priemonių parinkimą bei jų atitiktį saugos politiką įgyvendinančių dokumentų reikalavimams;

10.6. nustatęs PIR, PIDTIS ir LOBIS klaidas ar pažeidžiamas vietas, nedelsiant informuoja saugos įgaliotinį (kibernetinio saugumo vadovą) bei imasi visų būtinų priemonių galimiems incidentams išvengti;

10.7. imasi visų būtinų priemonių PIR kompiuterinio tinklo saugumui užtikrinti;

10.8. imasi visų reikiamų priemonių, skirtų apsaugoti PIR duomenis nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

10.9. diegia programinės įrangos atnaujinimus, nustato automatinio atnaujinimo procedūras;

10.10. vykdo visus saugos įgaliotinio (kibernetinio saugumo vadovo) nurodymus, susijusius su PIR, PIDTIS ir LOBIS saugos (kibernetinio saugumo) užtikrinimu;

10.11. nuolat teikia saugos įgaliotiniui (kibernetinio saugumo vadovui) informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;

10.12. patikrina (peržiūri) PIR, PIDTIS ir LOBIS sąranką ir būsenos rodiklius reguliariai, ne rečiau kaip kartą per metus ir po PIR, PIDTIS ir LOBIS pokyčio;

10.13. daro PIR, PIDTIS ir LOBIS duomenų kopijas, periodiškai tikrina duomenų iš kopijų atstatymo galimybes;

10.14. informuoja saugos įgaliotinį (kibernetinio saugumo vadovą) apie pastebėtus saugos dokumentuose nustatytų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones.

11. PIR, PIDTIS ir LOBIS naudotojai:

11.1. vadovaudamiesi Saugos nuostatais, saugaus elektroninės informacijos tvarkymo taisyklėmis, naudotojų administravimo taisyklėmis, pareigybių aprašymais ir kitais teisės aktais, naudoja PIR, PIDTIS ir LOBIS informacijos tvarkymo arba kitais su tiesioginių funkcijų vykdymu susijusiais tikslais;

11.2. informuoja saugos įgaliotinį (kibernetinio saugumo vadovą) ir (ar) administratorių apie pastebėtus saugos dokumentuose nustatytų reikalavimų pažeidimus, programinės įrangos pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones;

11.3. vykdo kitas Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas, susijusias su PIR, PIDTIS ir LOBIS naudojimu ir duomenų sauga;

11.4. atsako už tvarkomų duomenų saugą teisės aktų nustatyta tvarka;

11.5. privalo saugoti duomenų ir informacijos paslaptį, net ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

12. Tvarkant PIR, PIDTIS ir LOBIS duomenis ir užtikrinant saugą vadovaujamasi šiais teisės aktais:

12.1. Lietuvos Respublikos kibernetinio saugumo įstatymu;

12.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

12.3. Lietuvos Respublikos viešųjų ir privačių interesų derinimo valstybinėje tarnyboje įstatymu;

12.4. Lietuvos Respublikos lobistinės veiklos įstatymu;

12.5. Lietuvos Respublikos vyriausiosios tarnybinės etikos komisijos įstatymu;

12.6. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

12.7. Kibernetinio saugumo reikalavimų aprašu;

12.8. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

12.9. 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“ (toliau – Techniniai elektroninės informacijos saugos reikalavimai);

12.10. Bendraisiais reikalavimai asmens duomenų saugumo priemonėms;

12.11. Lietuvos standartais LST EN ISO/IEC 27001:2017, LST EN ISO/IEC 27002:2017, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, reglamentuojančiais saugų duomenų tvarkymą;

12.12. Saugos nuostatais ir kitais teisės aktais, reglamentuojančiais saugų asmens duomenų ir elektroninės informacijos tvarkymą.

II. ELEKTRONINĖS INFORMACIJOS SAUGOS (KIBERNETINIO SAUGUMO) VALDYMAS

13. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2016 m. rugpjūčio 11 d. nutarimu Nr. 826, 9.1 ir 9.3 punktais, PIR ir PIDTIS tvarkoma informacija priskiriama vidutinės svarbos informacijos kategorijai, o LOBIS – mažiausios svarbos informacijos kategorijai.

14. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo 12.3 ir 12.4 punktais, PIR ir PIDTIS priskiriama *trečiai kategorijai,* o LOBIS – *ketvirtajai kategorijai*.

15. Atsižvelgiant į saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką bei vadovaujantis Bendrųjų reikalavimų asmens duomenų saugumo priemonėms 11.2 ir 11.3 papunkčiais, PIR ir PIDTIS tvarkomi asmens duomenys priskiriami *trečiajam* automatiniu būdu tvarkomų asmens duomenų saugumo lygiui, o LOBIS – *antrajam*.

16. Saugos įgaliotinis (kibernetinio saugumo vadovas), atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja PIR rizikos įvertinimą. Prireikus, saugos įgaliotinis (kibernetinio saugumo vadovas) gali organizuoti neeilinį rizikos įvertinimą. Kartu su rizikos įvertinimu ir (arba) saugos nuostatų 25 punkte nurodytu informacinių technologijų saugos atitikties vertinimu turi būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos PIR, PIDTIS ir LOBIS kibernetiniam saugumui, vertinimas. Rizikos veiksnių įvertinimas atliekamas kokybiniu rizikos vertinimo metodu. Atliekant rizikos įvertinimą turi būti vertinamos rizikos, susijusios su:

16.1. informaciniais ištekliais;

16.2. kibernetiniu saugumu;

16.3. tarnybinėmis stotimis ir jų valdymu;

16.4. duomenų perdavimo tinklu, kuriuo teikiami ir gaunami duomenys iš registrų bei informacinių sistemų;

16.5. naudotojų darbo vietomis.

17. Rizikos veiksniai ir grėsmių pasireiškimo tikimybės vertinamos penkių lygių skalėje ir gali įgyti šias reikšmes: labai žemas, žemas, vidutinis, aukštas, labai aukštas.

18. Saugos priemonės parenkamos įvertinus galimus rizikos veiksnius PIR informacinių išteklių vientisumui, konfidencialumui ir prieinamumui bei atsižvelgiant į šiuos principus:

18.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

18.2. elektroninės informacijos saugos (kibernetinio saugumo) priemonių diegimo kaina turi būti adekvati elektroninės informacijos vertei;

18.3. kur įmanoma turi būti įdiegtos prevencinės, detekcinės ir korekcinės elektroninės informacijos saugos (kibernetinio saugumo) priemonės.

19. Rizikos įvertinimo rezultatai pateikiami Rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

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

19.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis duomenims gauti, duomenų pakeitimas ir sunaikinimas, informacinių technologijų duomenų perdavimo tinklais trikdymai, saugos pažeidimai, vagystės ir kt.);

19.3. nenugalimos jėgos (*force majeure*) (audros, gaisrai, vandens poveikis ir kt.).

20. PIR, PIDTIS ir LOBIS valdytojas rizikos įvertinimą gali pavesti (įgalioti) atlikti trečiajai šaliai.

21. Atsižvelgdamas į rizikos įvertinimo ataskaitą, valdytojas, prireikus, tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonių plano priemonėms įgyvendinti.

22. Ne vėliau kaip per 5 darbo dienas nuo dokumentų priėmimo (patvirtinimo) valdytojas pateikia ARSIS rizikos įvertinimo ataskaitos ir rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas.

23. Siekiant užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, Informacinių technologijų saugos atitikties vertinimo metodikos, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2016 m. rugpjūčio 2 d. įsakymu Nr. 1V-534 „Dėl Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymo Nr. 1V-156 „Dėl informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ pakeitimo“, nustatyta tvarka saugos įgaliotinis (kibernetinio saugumo vadovas) ne rečiau kaip kartą per *metus* organizuoja PIR, PIDTIS ir LOBIS informacinių technologijų saugos atitikties vertinimą (apimant Kibernetinio saugumo reikalavimų aprašo nustatytų reikalavimų vertinimą), kurio metu įvertinama saugos dokumentų ir realios duomenų saugos situacijos atitiktis saugos politiką ir kibernetinį saugumą apibrėžiantiems dokumentams.

24. Rekomenduojamos reikalavimų įgyvendinimo lygio nustatymo veiklos nurodytos Informacinių technologijų saugos atitikties vertinimo metodikos 5 punkte.

25. Informacinių technologijų saugos atitikties vertinimo metu turi būti atliekamas kibernetinių atakų imitavimas ir vykdomos kibernetinių incidentų imitavimo pratybos.

26. Kibernetinių atakų imitavimas atliekamas šiais etapais:

26.1. 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 PIR, PIDTIS ir LOBIS valdytojo vadovu ir vykdomas tik gavus jo rašytinį pritarimą;

26.2. 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;

26.3. kibernetinių atakų imitavimo etapas. Atliekami kibernetinių atakų imitavimo plane numatyti testai;

26.4. 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 organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinamas PIR, PIDTIS ir LOBIS veiklos tęstinumo valdymo planas.

27. Atlikus informacinių technologijų saugos atitikties vertinimą, saugos įgaliotinis (kibernetinio saugumo vadovas), prireikus, parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus skiria ir įgyvendinimo terminus nustato PIR valdytojas.

28. ARSIS nuostatų nustatyta tvarka, ne vėliau kaip per 5 darbo dienas nuo dokumentų priėmimo (patvirtinimo) PIR, PIDTIS ir LOBIS valdytojas pateikia šiai sistemai informacinių technologijų saugos atitikties vertinimo ataskaitos ir pastebėtų trūkumų šalinimo plano kopijas.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

29.1. PIR, PIDTIS ir LOBIS tarnybinėse stotyse ir naudotojų kompiuteriuose turi būti įdiegta centralizuotai valdoma ir stebėjimą realiu laiku vykdanti programinė įranga, skirta aptikti ir apsisaugoti nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo el. pašto);

29.2. apsaugai naudojamų kenksmingos programinės įrangos aptikimo priemonių duomenų bazė privalo atsinaujinti ne rečiau kaip kas 24 valandas;

29.3. apsaugai naudojama programinė įranga turi būti sukonfigūruota taip, kad administratoriui būtų siunčiami pranešimai, jei kuriame nors įrenginyje buvo pradelstas kenksmingos programinės įrangos aptikimo priemonės atnaujinimo laikas;

29.4. apsaugai naudojamos programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

30. Programinės įrangos, įdiegtos naudotojų kompiuterinėje įrangoje ir tarnybinėse stotyse, naudojimo nuostatos:

30.1. tarnybinėse stotyse ir naudotojų kompiuterinėje įrangoje naudojama tik legali programinė įranga;

30.2. tarnybinėse stotyse ir naudotojų kompiuterinėje įrangoje naudojamų operacinių sistemų ir kitos programinės įrangos gamintojų rekomenduojami atnaujinimai turi būti operatyviai ištestuojami ir įdiegiami;

30.3. administratorius turi reguliariai, ne rečiau kaip kartą per savaitę įvertinti informaciją apie neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumų svarbos lygius;

30.4. tarnybinėse stotyse negali būti programinės įrangos, nesusijusios su PIR, PIDTIS ir LOBIS duomenų tvarkymu, naudotojų ir programinės įrangos administravimu;

30.5. naudotojų kompiuterinėje įrangoje naudojama darbo funkcijoms atlikti reikalinga programinė įranga;

30.6. saugos įgaliotinis (kibernetinio saugumo vadovas) parengia, su PIR, PIDTIS ir LOBIS valdytojo vadovu suderina ir ne rečiau kaip kartą per metus peržiūri bei prireikus atnaujina leistinos programinės įrangos sąrašą;

30.7. visa programinė įranga prižiūrima laikantis gamintojų rekomendacijų;

30.8. programinę įrangą turi prižiūrėti, diegti, gedimus šalinti tik kvalifikuoti, PIR, PIDTIS ir LOBIS valdytojo ir tvarkytojo vadovo įgalioti asmenys;

30.9. programinė įranga turi būti testuojama naudojant atskirą testavimui skirtą aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendraisiais reikalavimais asmens duomenų saugumo priemonėms;

30.10. programiniai kodai privalo būti apsaugoti nuo atskleidimo neturintiems teisės su jais susipažinti asmenims.

31. kompiuterių tinklo filtravimo įrangos pagrindinės naudojimo nuostatos ir apsaugos priemonės:

31.1. tinklo segmentavimas;

31.2. prieigos kontrolės sąrašai (ACL);

31.3. „statefull“ ugniasienė; tinklo išorinis perimetras apsaugotas interneto prieigos maršruto parinktuvu ir ugniasiene. Išoriniam perimetrui apsaugoti naudojamas statinis 7 lygmens pagal OSI modelį paketų ir „statefull“ (sekantis paketų būsenas) filtravimas;

31.4. ugniasienės įvykių žurnalai (angl. logs) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklėse periodiškai peržiūrimos ir atnaujinamos;

31.5. tinklo adresų transliavimas (NAT/PAT);

31.6. PIR, PIDTIS ir LOBIS 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;

31.7. naudojami filtrai, apsaugantys el. pašte ir viešajame ryšių tinkle naršančių naudotojų kompiuterinę įrangą nuo kenksmingo kodo.

32. Naudojamų svetainių saugos valdymo reikalavimai:

32.1. svetainės turi atitikti reikalavimus nustatytus Kibernetinio saugumo reikalavimų apraše, Bendruosiuose reikalavimuose asmens duomenų saugumo priemonėms bei Techniniuose elektroninės informacijos saugos reikalavimuose;

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

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

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

32.5. Naudojamų svetainių sauga turi būti vertinama PIR rizikos įvertinimo metu ir PIR informacinių technologijų saugos atitikties vertinimo metu, atliekamų Saugos nuostatų II skyriuje nustatyta tvarka.

33. Leistinos kompiuterių naudojimo ribos:

33.1. stacionarieji ir nešiojamieji kompiuteriai, jei juose yra prieiga prie PIR, PIDTIS ir LOBIS ar saugoma su PIR, PIDTIS ir LOBIS susijusi informacija, gali būti išnešami iš Komisijos patalpų ir naudojami ne Komisijos patalpose tik vadovaujantis Komisijos pirmininko įsakymu patvirtintu nešiojamųjų kompiuterių naudojimo darbo vietose tvarkos aprašu.

33.2. naudotojai, naudodami kompiuterius už Komisijos ribų, asmeniškai Lietuvos Respublikos teisės aktų nustatyta tvarka atsako už kompiuterio duomenų saugojimo laikmenose esančių duomenų saugą.

34. Metodai, leidžiantys užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą, duomenų tvarkymą:

34.1. nuotolinis prisijungimas prie PIR, PIDTIS ir LOBIS vykdomas protokolais, skirtais duomenų šifravimui;

34.2. nuotolinis prisijungimas prie PIR, PIDTIS ir LOBIS galimas šiais būdais:

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

34.2.2. naudojant saugaus apvalkalo protokolą (angl. Secure Shell) ir nuotolinio darbalaukio protokolą (angl. Remote Desktop Protocol). Šia galimybe gali būti pasinaudota tik PIR, PIDTIS ir LOBIS administravimo tikslais.

34.3. pagrindinė duomenų pateikimo prieiga yra duomenų perdavimas duomenų perdavimo kanalu, panaudojant saugų HTTPS protokolą. Naudotojai identifikuojami vardu ir slaptažodžiu, jiems suteikiamos PIR, PIDTIS ir LOBIS naudojimosi grupinės ar individualios teisės (rolės). Kaip papildoma priemonė, ribojanti prisijungimą prie PIR, PIDTIS ir LOBIS, yra interneto protokolo (angl. IP) adresų filtravimas.

34.4. elektroninė informacija, perduodama ne per tvarkytojui priklausančias duomenų perdavimo linijas, privalo būti šifruojama;

34.5. 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, Kibernetinio saugumo reikalavimų aprašą, Techninius elektroninės informacijos saugos reikalavimus;

34.6. 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;

34.7. už saugos reikalavimų duomenų teikimo ir (ar) gavimo sutartyse suformulavimą, nustatymą ir įgyvendinimo organizavimą atsakingas saugos įgaliotinis (kibernetinio saugumo vadovas).

34.8. PIR, PIDTIS ir LOBIS naudotojų identifikavimas:

34.8.1. PIR, PIDTIS ir LOBIS naudotojai identifikuojami naudojant naudotojo vardą ir slaptažodį arba naudojant Valstybės informacinių išteklių sąveikumo platformą;

34.8.2. PIR, PIDTIS ir LOBIS naudotojų administravimo taisyklėse nustatomi specialūs slaptažodžių sistemos reikalavimai (periodinis privalomas slaptažodžių keitimas, slaptažodžio ilgio apribojimai ir kt.);

34.8.3. PIR, PIDTIS ir LOBIS naudotojų ir su jais susijusių duomenų tvarkymas detaliai aprašytas PIR, PIDTIS ir LOBIS naudotojų administravimo taisyklėse.

34.9. Apsauga nuo galimų tyčinių naudotojų veiksmų:

34.9.1. nustatomi naudotojų vaidmenys ir jiems priskiriami konkretūs leidžiami atlikti veiksmai;

34.9.2. ribojama naudotojo teisė manipuliuoti duomenimis;

34.9.3. naudotojo teisės suteikiamos ir sustabdomos Personalo skyriaus atsakingo asmens prašymu;

34.9.4. visi naudotojo prisijungimai prie PIR, PIDTIS ir LOBIS registruojami prisijungimų žurnaluose ir saugomi ne trumpiau nei 1 metus;

34.9.5. visi pakeitimai duomenų bazėse yra registruojami elektroniniuose žurnaluose;

34.10. PIR, PIDTIS ir LOBIS duomenų saugos organizacinės priemonės:

34.10.1. veiksmai, užtikrinantys duomenų saugą, nustatomi naudotojų pareigybių aprašymuose;

34.10.2. naudotojai supažindinami su galiojančiais norminiais aktais, reglamentuojančiais duomenų saugą;

34.10.3. naudotojų atsakomybę nustato pasirašomi asmeniniai naudotojų pasižadėjimai;

34.10.4. duomenų saugos dokumentai peržiūrimi ir atnaujinami ne rečiau kaip kartą per metus arba atlikus rizikos įvertinimą ar informacinių technologijų saugos atitikties vertinimą ar pasikeitus teisės aktams, reglamentuojantiems duomenų saugą.

35. Pagrindiniai atsarginių kopijų darymo ir atkūrimo reikalavimai:

35.1. atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į priimtiną elektroninės informacijos praradimo kiekį (angl. recovery point objective) ir priimtiną PIR, PIDTIS ir LOBIS posistemių neveikimo laikotarpį (angl. recovery time objective);

35.2. atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokios apimties, kad PIR, PIDTIS ir LOBIS veiklos sutrikimo, elektroninės informacijos saugos

(kibernetinio) incidento ar elektroninės informacijos vientisumo praradimo atvejais PIR, PIDTIS ir LOBIS neveikimo laikotarpis nebūtų ilgesnis, nei 16 valandų, o elektroninės informacijos praradimas atitiktų priimtinumo kriterijus;

35.3. kopijų darymo, saugojimo ir atstatymo tvarka detaliai aprašyta PIR, PIDTIS ir LOBIS saugaus elektroninės informacijos tvarkymo taisyklėse.

IV. REIKALAVIMAI PERSONALUI

36. Saugos įgaliotinis (kibernetinio saugumo vadovas) privalo išmanyti informacijos saugos (kibernetinio saugumo) užtikrinimo principus, savo darbe vadovautis dokumentais ir teisės aktais, reglamentuojančiais PIR, PIDTIS ir LOBIS duomenų tvarkymą, sugebėti prižiūrėti, kaip įgyvendinama saugos politika, taip pat turėti darbo su duomenų bazėmis, operacinėmis sistemomis, taikomosiomis programomis patirties. Saugos įgaliotinis (kibernetinio saugumo vadovas) privalo tobulinti kvalifikaciją elektroninės informacijos saugos (kibernetinio saugumo) srityje.

37. Saugos įgaliotiniu (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.

38. Administratorius privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti jos saugą, turėti darbo su kompiuterių tinklais patirties, mokėti užtikrinti jų saugą, taip pat turėti sisteminių programinių priemonių administravimo bei priežiūros patirties, mokėti administruoti ir prižiūrėti duomenų bazes, būti susipažinęs su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais.

39. Administratorius privalo sugebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą, atlikti įrangos priežiūrą, trikčių diagnostiką ir šalinimą.

40. Naudotojai privalo turėti darbo su kompiuteriu įgūdžių, mokėti tvarkyti PIR duomenis, turi būti susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais.

41. Tvarkyti PIR, PIDTIS ir LOBIS duomenis gali tik tie naudotojai, kurie yra pasirašę pasižadėjimą saugoti asmens duomenų paslaptį.

42. Naudotojų mokymus informacijos saugos (kibernetinio saugumo) klausimais kasmet inicijuoja saugos įgaliotinis (kibernetinio saugumo vadovas).

43. Naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti saugos įgaliotiniui (kibernetinio saugumo vadovui) ir administratoriui.

44. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią PIR, PIDTIS ir LOBIS saugą, saugos įgaliotinis (kibernetinio saugumo vadovas) užtikrindamas incidentų tyrimą ir valdymą apie tai turi pranešti PIR, PIDTIS ir LOBIS valdytojo vadovui ir kompetentingoms institucijoms Kibernetinio saugumo reikalavimo aprašo ir kitų teisės aktų nustatyta tvarka, tiriančioms elektroninių ryšių tinklų, informacijos saugos (kibernetinio saugumo) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais.

45. Įvykus elektroninės informacijos saugos (kibernetinio saugumo) incidentui, nenumatytai situacijai, saugos įgaliotinio (kibernetinio saugumo vadovo), administratoriaus, naudotojų veiksmus reglamentuoja PIR, PIDTIS ir LOBIS veiklos tęstinumo valdymo planas.

46. Naudotojų ir administratoriaus mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

46.1. Naudotojams turi būti organizuojami mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais, įvairiais būdais primenama apie elektroninės informacijos

saugos (kibernetinio saugumo) problemas (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems naudotojams, administratoriui ir pan.);

46.2. 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), naudotojų ar administratoriaus poreikius;

46.3. mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.). Mokymus gali vykdyti saugos įgaliotinis (kibernetinio saugumo vadovas) ar kitas valdytojo ar tvarkytojo darbuotojas, išmanantis elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, arba elektroninės informacijos saugos (kibernetinio saugumo) mokymų paslaugų teikėjas;

46.4. mokymai naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per dvejus metus. Mokymai administratoriui turi būti organizuojami pagal poreikį. Už mokymų organizavimą atsakingas saugos įgaliotinis;

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

V. PIR NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

47. Tvarkyti PIR, PIDTIS ir LOBIS duomenis gali tik tie naudotojai, kurie yra susipažinę su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais ir raštiškai sutikę laikytis šių teisės aktų reikalavimų.

48. Už naudotojų supažindinimą su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais ir atsakomybe už šiuose teisės aktuose nustatytų reikalavimų nesilaikymą atsako saugos įgaliotinis (kibernetinio saugumo vadovas).

49. Saugos nuostatai ir saugos politiką įgyvendinantys dokumentai skelbiami naudotojams pasiekiamoje interneto svetainėje (intraneto svetainėje).

50. Su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais pakartotinai supažindinama atnaujinus dokumentus arba pasikeitus informacijos saugą (kibernetinį saugumą) reglamentuojantiems teisės aktams. Supažindinimas vykdomas el. paštu, skelbiant informaciją naudotojams pasiekiamoje interneto svetainėje (intraneto svetainėje).

VI. BAIGIAMOSIOS NUOSTATOS

51. Apie Saugos nuostatų ar saugos politiką įgyvendinančių dokumentų pripažinimą netekusiais galios, keitimą ar priėmimą saugos įgaliotinis (kibernetinio saugumo vadovas) nedelsdamas informuoja naudotojus.

52. PIR, PIDTIS ir LOBIS valdytojas ir tvarkytojas, saugos įgaliotinis (kibernetinio saugumo vadovas), administratorius ir naudotojai, pažeidę Saugos nuostatų arba saugų duomenų tvarkymą reglamentuojančių teisės aktų reikalavimus, atsako įstatymų ir kitų teisės aktų nustatyta tvarka.

_____