INFORMACINĖS VISUOMENĖS PLĖTROS KOMITETO PRIE SUSISIEKIMO MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL TARPŽINYBINĖS MOKESTINIŲ DUOMENŲ SAUGYKLOS, INFORMACINĖS VISUOMENĖS PLĖTROS STEBĖSENOS INFORMACINĖS SISTEMOS IR INFORMACIJOS RINKMENŲ SĄRAŠO DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2016 m. balandžio 29 d. Nr. T-28
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimo Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7, 11, 19 ir 31 punktais,

1. T v i r t i n u Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo duomenų saugos nuostatus.

2. P a v e d u Projektų skyriui iki šių metų rugpjūčio 1 d. parengti, nustatyta tvarka suderinti ir pateikti tvirtinti Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo saugaus elektroninės informacijos tvarkymo taisykles, veiklos tęstinumo valdymo planą, ir naudotojų administravimo taisykles.

3. S k i r i u Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo duomenų saugos įgaliotine Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos (toliau – Komitetas) Projektų skyriaus vyriausiąją specialistę Irmą Zdanavičienę.

4. S k i r i u:

4.1. Tarpžinybinės mokestinių duomenų saugyklos administratoriumi Komiteto Projektų skyriaus vyriausiąjį specialistą Virginijų Martinaitį;

4.2. Informacinės visuomenės plėtros stebėsenos informacinės sistemos administratoriumi Komiteto Planavimo ir stebėsenos skyriaus vedėją Arminą Rakauską;

4.3. Informacijos rinkmenų sąrašo administratoriumi Komiteto Informacinių išteklių skyriaus vyriausiąjį specialistą Denį Voišnį.

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

5.1. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2007 m. rugpjūčio 22 d. įsakymą Nr. T-112 „Dėl Informacijos rinkmenų sąrašo duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais;

5.2. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2007 m. rugsėjo 27 d. įsakymą Nr. T-133 „Dėl Tarpžinybinės mokestinių duomenų saugyklos duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais;

5.3. Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2011 m. liepos 13 d. įsakymo Nr. T-96 „Dėl Informacinės visuomenės plėtros stebėsenos informacinės sistemos nuostatų ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ 1.2, 2 ir 3 punktus.

Direktorius Ramūnas Čepaitis

PATVIRTINTA
Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2016 m. balandžio 29 d. įsakymu Nr. T-28

TARPŽINYBINĖS MOKESTINIŲ DUOMENŲ SAUGYKLOS, INFORMACINĖS VISUOMENĖS PLĖTROS STEBĖSENOS INFORMACINĖS SISTEMOS IR INFORMACIJOS RINKMENŲ SĄRAŠO DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui, dirbančiam su Tarpžinybine mokestinių duomenų saugykla, Informacinės visuomenės plėtros stebėsenos informacine sistema ir Informacijos rinkmenų sąrašu (toliau – IVPK IS), IVPK IS naudotojų supažindinimo su Saugos nuostatais ir IVPK IS saugos politiką įgyvendinančiais dokumentais (toliau – saugos dokumentai) principus.

2. Saugos nuostatuose vartojamos sąvokos atitinka Saugos nuostatų 9 punkte nurodytuose teisės aktuose vartojamas sąvokas.

3. IVPK IS elektroninės informacijos saugumo užtikrinimo tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti IVPK IS elektroninę informaciją, užtikrinti IVPK IS elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą techninės, programinės ir ryšių įrangos funkcionavimą.

4. IVPK IS elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų IVPK IS elektroninės informacijos saugai užtikrinti, įgyvendinimas ir šių priemonių įgyvendinimo kontrolė;

4.2. teisėtas, saugus ir kokybiškas IVPK IS duomenų tvarkymas;

4.3. teisėtas ir saugus IVPK IS asmens duomenų naudojimas;

4.4. IVPK IS veiklos tęstinumo užtikrinimas.

5. IVPK IS valdytojas ir tvarkytojas bei IVPK IS asmens duomenų valdytojas ir tvarkytojas– Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos (toliau – Komitetas), Gedimino pr. 7, LT-01103 Vilnius.

6. IVPK IS valdytojas ir tvarkytojas vykdo šias funkcijas:

6.1. organizuoja IVPK IS veiklą ir jai vadovauja;

6.2. tvirtina saugos dokumentus:

6.2.1. Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo saugaus elektroninės informacijos tvarkymo taisykles;

6.2.2. Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo veiklos tęstinumo valdymo planą;

6.2.3. Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo naudotojų administravimo taisykles;

6.3. prižiūri, kaip laikomasi teisės aktų, susijusių su IVPK IS tvarkymu ir duomenų saugumu, reikalavimų;

6.4. priima sprendimą dėl IVPK IS informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

6.5. kontroliuoja, kad IVPK IS būtų tvarkomos vadovaujantis Lietuvos Respublikos įstatymais, Saugos nuostatais ir kitais teisės aktais;

6.6. atlieka IVPK IS duomenų bazės techninę priežiūrą ir užtikrina nepertraukiamą IVPK IS veiklą;

6.7. įgyvendina tinkamas organizacines ir technines priemones, kurios skirtos elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

6.8. užtikrina, kad IVPK IS naudotojai, turintys teisę naudotis IVPK IS elektronine informacija numatytoms funkcijoms atlikti, laikytųsi saugos dokumentuose nustatytų reikalavimų;

6.9. organizuoja techninių, programinių priemonių, kurios skirtos IVPK IS eksploatuoti, prižiūrėti ir plėtoti, įsigijimą, jų įdiegimą ir modernizavimą, IVPK IS techninės, programinės įrangos priežiūrą ir tobulinimą;

6.10. pagal kompetenciją atsako už IVPK IS elektroninės informacijos tvarkymo teisėtumą ir saugumą bei IVPK IS saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams ir Saugos nuostatams.

7. IVPK IS saugos įgaliotinis, įgyvendindamas IVPK IS elektroninės informacijos saugą, atlieka šias funkcijas:

7.1. teikia IVPK IS tvarkytojo vadovui pasiūlymus dėl:

7.1.1. IVPK IS administratoriaus skyrimo;

7.1.2. IVPK IS saugos dokumentų priėmimo, keitimo ar panaikinimo;

7.1.3. IVPK IS informacinių technologijų saugos reikalavimų atitikties ir rizikos vertinimo atlikimo;

7.2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių IVPK IS, tyrimą;

7.3. teikia IVPK IS administratoriui privalomus vykdyti nurodymus ir pavedimus;

7.4. konsultuoja IVPK IS naudotojus saugaus elektroninės informacijos tvarkymo klausimais;

7.5. inicijuoja IVPK IS naudotojų mokymą elektroninės informacijos saugumo klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

7.6. organizuoja IVPK IS informacinių technologijų saugos reikalavimų atitikties ir rizikos vertinimą;

7.7. atsako už saugos politikos įgyvendinimą ir saugos dokumentų reikalavimų vykdymą;

7.8. atlieka kitas saugos dokumentuose nurodytas ir Saugos nuostatuose jam priskirtas funkcijas.

8. IVPK IS administratorius, įgyvendindamas IVPK IS saugos reikalavimus, atlieka šias funkcijas:

8.1. suteikia IVPK IS naudotojams teisę naudotis elektronine informacija, reikalinga jiems priskirtoms funkcijoms atlikti;

8.2. informuoja IVPK IS saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir padeda IVPK IS saugos įgaliotiniui informacijos saugos incidentų tyrime ir sprendime;

8.3. teikia IVPK IS tvarkytojui pasiūlymus dėl elektroninės informacijos saugumo organizavimo;

8.4. atsako už tai, kad tvarkant IVPK IS nebūtų pažeisti Saugos nuostatų reikalavimai;

8.5. organizuoja IVPK IS kompiuterinės ir programinės įrangos administravimą ir priežiūrą, kad būtų užtikrintas kokybiškas ir patikimas jos veikimas;

8.6. kontroliuoja ir prižiūri IVPK IS programinės ir kompiuterinės įrangos diegimo procesus;

8.7. kontroliuoja IVPK IS duomenų bazės atsarginių kopijų darymą, tinkamumą ir saugojimą;

8.8. reguliariai ne rečiau kaip kartą per metus ir (arba) po informacinės sistemos pokyčio patikrina IVPK IS sąranką ir IVPK IS būsenos rodiklius.

9. Tvarkant IVPK IS elektroninę informaciją ir užtikrinant jų saugą, vadovaujamasi šiais teisės aktais:

9.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

9.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

9.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

9.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu, Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, (toliau - Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai);

9.5. IVPK IS nuostatais;

9.6. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

9.7. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais 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“;

9.8. Lietuvos Respublikos vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais grupės „Informacijos technologija. Saugumo metodai“ standartais, reglamentuojančiais saugų duomenų tvarkymą;

9.9. Valstybės informacinių sistemų rizikos vertinimo atlikimo Informacinės visuomenės plėtros komitete prie Susisiekimo ministerijos taisyklėmis, patvirtintomis Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2016 m. sausio 26 d. įsakymu Nr. T-5 „Dėl Valstybės informacinių sistemų rizikos vertinimo atlikimo Informacinės visuomenės plėtros komitete prie Susisiekimo ministerijos taisyklių patvirtinimo“ (toliau – Rizikos vertinimo taisyklės).

9.10. IVPK IS saugos politikos įgyvendinimo dokumentais.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

10. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ 4.3 ir 5.3 punktu, IVPK IS tvarkoma informacija yra priskiriama žinybinės svarbos informacijos kategorijai, o IVPK IS yra priskiriamas trečiai kategorijai.

11. Pagrindiniai rizikos veiksniai, galintys turėti įtakos IVPK IS elektroninės informacijos saugumui, yra:

11.1. subjektyvūs netyčiniai (IVPK IS tvarkymo klaidos ir pasirikimai, ištrynimas, klaidingas teikimas, fiziniai informacinių technologijų sutrikimai, perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

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

11.3. atsitiktinės subjektyvios aplinkybės (darbuotojų praradimas, gaisrai, vandens poveikis, elektros instaliacijos gedimas ir kita);

11.4. nenugalima jėga (force majeure).

12. IVPK IS saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus bei Rizikos vertinimo taisykles, kasmet organizuoja IVPK IS rizikos įvertinimą ir parengia rizikos įvertinimo ataskaitą; prireikus jis gali organizuoti neeilinį rizikos įvertinimą.

13. IVPK IS tvarkytojas, atsižvelgdamas į IVPK IS rizikos įvertinimo ataskaitą, prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

14. Siekdamas užtikrinti Saugos nuostatuose ir saugos dokumentuose nustatytų reikalavimų įgyvendinimo organizavimą ir įgyvendinimo kontrolę IVPK IS saugos įgaliotinis ne rečiau kaip kartą per metus organizuoja IVPK IS informacinių technologijų saugos reikalavimų atitikties vertinimą, kurio metu:

14.1. įvertinama realios IVPK IS elektroninės informacijos saugos situacijos atitiktis Saugos nuostatų, saugos dokumentų ir kitų teisės aktų reikalavimams;

14.2. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų IVPK IS naudotojų kompiuterizuotų darbo vietų bei visų tarnybinių stočių įdiegta programinė įranga ir jos sąranka;

14.3. patikrinama (įvertinama) IVPK IS naudotojams ir administratoriams suteiktų teisių atitiktis vykdomoms funkcijoms;

14.4. įvertinamas pasirengimas užtikrinti IVPK IS veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui.

15. Atlikus IVPK IS informacinių technologijų saugos atitikties vertinimą, IVPK IS saugos įgaliotinis rengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir nustatytų trūkumų šalinimo įgyvendinimo terminus nustato IVPK IS valdytojas.

16. IVPK IS elektroninės informacijos saugumo priemonės turi būti parenkamos atsižvelgiant į Saugos nuostatų 11 punkte išvardytus rizikos veiksnius, galinčius turėti įtakos IVPK IS elektroninės informacijos saugumui.

17. Parenkamos tokios saugos priemonės, kad būtų užtikrintas IVPK IS veiklos tęstinumas, patiriama kuo mažiau išlaidų ir užtikrinamas saugus IVPK IS darbas.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

18.1. IVPK IS tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą (virusų, šnipinėjimo programinę įrangą ir kt.), kurios turi būti reguliariai atnaujinamos automatiniu būdu ne rečiau kaip kartą per parą;

18.2. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu;

18.3. kenksmingosios programinės įrangos aptikimo priemonės veikia nuolat realiu laiku.

19. Programinės įrangos, įdiegtos tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

19.1. IVPK IS darbui gali būti naudojama tik legali ir patikrinta programinė įranga;

19.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

19.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka IVPK IS administratorius.

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

20.1. kompiuterių tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis bei įsilaužimų aptikimo ir prevencijos įranga;

20.2. visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

20.3. naudojamos turinio filtravimo sistemos.

21. Leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos:

21.1. prie IVPK IS prisijungiama nuotoliniu būdu naudojant interneto naršyklę (HTTPS protokolą);

21.2. prieigą prie IVPK IS suteikia, apriboja ir panaikina administratorius;

21.3. teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam IVPK IS naudotojui;

21.4. IVPK IS naudotojų prieiga prie IVPK IS elektroninės informacijos leidžiama tik per registravimo ir slaptažodžių sistemą;

21.5. IVPK IS naudotojams, savo tarnybinėms funkcijoms vykdyti naudojantiems nešiojamus kompiuterius IVPK IS elektroninės informacijos perdavimui kompiuterių tinklais, šiuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis, papildomas IVPK IS naudotojo tapatybės patvirtinimas ir elektroninės informacijos šifravimas;

21.6. IVPK IS naudotojai gali jungti prie nešiojamo kompiuterio ir naudoti išorinius įrenginius ir laikmenas tik savo darbo funkcijų vykdymui.

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

22.1. tiesioginė prieiga prie IVPK IS elektroninės informacijos suteikiama įgyvendinus IVPK IS naudotojų administravimo taisyklėse nurodytas IVPK IS naudotojų autentifikavimo priemones;

22.2. per metus turi būti užtikrintas IVPK IS prieinamumas ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis;

22.3. IVPK IS elektroninė informacija perduodama automatiniu būdu arba asinchroniniu režimu pagal duomenų teikimo sutartis, kuriose nustatytos perduodamos elektroninės informacijos specifikacijos, kopijų skaičius ir kitos elektroninės informacijos perdavimo sąlygos ir tvarka;

22.4. IVPK IS elektroninė informacija, perduodama ne per IVPK IS tvarkytojams priklausančias duomenų perdavimo linijas, privalo būti šifruojama;

22.5. IVPK IS elektroninės informacijos perdavimui naudojamas Saugus valstybinis duomenų perdavimo tinklas arba kitas šifruotas perdavimo kanalas, užtikrinantis saugų informacijos perdavimą.

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

23.1. IVPK IS duomenų bazė yra kopijuojama ir saugoma taip, kad įvykus nenumatytai situacijai IVPK IS veikla būtų visiškai atkurta per 16 valandų;

23.2. atsarginės elektroninės informacijos kopijos saugomos kitoje patalpoje, nei IVPK IS duomenų bazė.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

24. IVPK IS saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendraisiais elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimais, Informacinių technologijų saugos atitikties vertinimo metodika, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą, kelti kvalifikaciją kvalifikacijos kėlimo kursuose, saugaus darbo su duomenimis seminaruose.

25. IVPK IS saugos įgaliotiniu 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.

26. IVPK IS administratoriumi skiriamas darbuotojas, išmanantis darbą su IVPK IS taikomąja programine įranga ir gebantis atlikti funkcijas, susijusias su IVPK IS naudotojų teisių valdymu.

27. IVPK IS administratorius turi būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais ir kontroliuoti paslaugų teikėjus, administruojančius ir prižiūrinčius IVPK IS techninę ir programinę įrangą.

28. IVPK IS naudotojai privalo turėti darbo kompiuteriu įgūdžių, būti susipažinę su saugos dokumentais.

29. IVPK IS saugos įgaliotinis periodiškai inicijuoja IVPK IS naudotojų mokymą elektroninės informacijos saugos klausimais, įvairiais būdais (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės priimtiems naujiems darbuotojams ir panašiai) informuoja juos apie elektroninės informacijos saugos problemas.

V SKYRIUS
IVPK IS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

30. Tvarkyti IVPK IS duomenis gali tik įgalioti IVPK IS naudotojai, kurie yra susipažinę su saugos dokumentais bei programinėmis priemonėmis sutikę laikytis juose nustatytų reikalavimų.

31. IVPK IS administratorių su Saugos nuostatais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai supažindina IVPK IS saugos įgaliotinis per 10 darbo dienų nuo IVPK IS įteisinimo, o su kitais saugos dokumentais – per 10 darbo dienų nuo šių dokumentų patvirtinimo.

32. IVPK IS naudotojų supažindinimas su saugos dokumentais ir atsakomybe už saugos dokumentuose nustatytų reikalavimų nesilaikymą bei informacija apie saugos dokumentų priėmimą, pakeitimą ar pripažinimą netekusiais galios užtikrinamas programinėmis IVPK IS priemonėmis.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

33. IVPK IS saugos įgaliotinis organizuoja arba atlieka saugos reikalavimų atitikties vertinimą ne rečiau kaip kartą per metus. Saugos dokumentai yra svarstomi atlikus rizikos analizę ar informacinių technologijų saugos reikalavimų atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams Komitete.

34. IVPK IS Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijos, saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijos, saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

35. IVPK IS saugos įgaliotinis, IVPK IS duomenų valdymo įgaliotinis, IVPK IS administratorius ir IVPK IS naudotojai, pažeidę Saugos nuostatų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

_____

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2016-03-29 raštu Nr. 1D-1916