Suvestinė redakcija nuo 2018-11-21 iki 2019-07-30

Įsakymas paskelbtas: TAR 2016-04-29, i. k. 2016-10744

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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7 ir 11 punktais ir 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. nutarimo Nr. 387 „Dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, 7 punktu.

Preambulės pakeitimai:
Nr. T-129, 2018-11-19, paskelbta TAR 2018-11-20, i. k. 2018-18646

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 įgaliotiniu Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos (toliau – Komitetas) Informacinių išteklių skyriaus vyriausiąjį specialistą Kęstutį Valeiką.

Punkto pakeitimai:
Nr. T-94, 2018-08-28, paskelbta TAR 2018-08-30, i. k. 2018-13597

4 . S k i r i u:

4 . 1 . Tarpžinybinės mokestinių duomenų saugyklos administratoriumi Komiteto Informacinių technologijų sprendimų skyriaus vyriausiąjį specialistą Virginijų Martinaitį;

4 . 2 . Informacinės visuomenės plėtros stebėsenos informacinės sistemos administratoriumi Komiteto Vertinimo ir stebėsenos skyriaus vedėją Arminą Rakauską;

4.3. Informacijos rinkmenų sąrašo administratore Komiteto Informacinių išteklių skyriaus vyriausiąją specialistę Alioną Olševskają.

Punkto pakeitimai:
Nr. T-94, 2018-08-28, paskelbta TAR 2018-08-30, i. k. 2018-13597

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
(Informacinės visuomenės plėtros komiteto prie
Ūkio ministerijos direktoriaus
2018 m. lapkričio 19 d. įsakymo Nr. T-129
redakcija)

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 (toliau – IVPK IS) duomenų saugos nuostatai (toliau – Saugos nuostatai) apibrėžia IVPK IS elektroninės informacijos ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika).

2. Elektroninės informacijos saugos politika įgyvendinama pagal Informacinės visuomenės plėtros komiteto prie Ūkio ministerijos (toliau – Komitetas) direktoriaus tvirtinamus IVPK IS saugos politiką įgyvendinančius dokumentus: saugaus elektroninės informacijos tvarkymo taisykles, naudotojų administravimo taisykles, veiklos tęstinumo valdymo planą (toliau – saugos politiką įgyvendinantys dokumentai).

3. Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų saugos reikalavimų aprašas), 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. nutarimu 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), vartojamas sąvokas.

4. IVPK IS elektroninės informacijos saugos ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) 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, vykdyti elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai) prevenciją.

5. IVPK IS elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

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

5.2. teisėtas, saugus ir kokybiškas IVPK IS elektroninės informacijos tvarkymas;

5.3. teisėtas ir saugus IVPK IS asmens duomenų naudojimas;

5.4. IVPK IS veiklos tęstinumo užtikrinimas.

6. IVPK IS valdytojas ir tvarkytojas bei IVPK IS asmens duomenų valdytojas ir tvarkytojas yra Komitetas (Gedimino pr. 7, LT-01103 Vilnius).

7. IVPK IS valdytojas ir tvarkytojas vykdo šias funkcijas:

7.1. organizuoja IVPK IS veiklą ir jai vadovauja;

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

7.3. prižiūri, kaip laikomasi teisės aktų, susijusių su IVPK IS tvarkymu ir elektroninės informacijos saugumu, reikalavimų;

7.4. tvirtina IVPK IS Saugos nuostatus, saugos politiką įgyvendinančius dokumentus (toliau kartu – saugos dokumentai) bei kitus dokumentus, susijusius su elektroninės informacijos sauga;

7.5. kontroliuoja, kad IVPK IS būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, Saugos nuostatais, Bendrųjų saugos reikalavimų aprašu, Kibernetinio saugumo reikalavimų aprašu, 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 (toliau - Bendrasis duomenų apsaugos reglamentas) ir kitais IVPK IS elektroninės informacijos saugos valdymą reglamentuojančiais teisės aktais ir standartais;

7.6. skiria IVPK IS saugos įgaliotinį ir kibernetinio saugumo vadovą;

7.7. 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;

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

7.9. 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;

7.10. 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.

8. IVPK IS saugos įgaliotinis, koordinuodamas ir prižiūrėdamas saugos politikos įgyvendinimą atlieka Bendrųjų saugos reikalavimų apraše saugos įgaliotiniui priskirtas funkcijas.

9. Kibernetinio saugumo vadovas atlieka šias funkcijas:

9.1. vykdo kibernetinio saugumo organizavimo ir užtikrinimo funkcijas, nustatytas Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose;

9.2. registruoja ir kaupia informaciją apie IVPK IS elektroninės informacijos saugos ir kibernetinius incidentus, koordinuoja elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai), įvykusių IVPK IS, tyrimą ir bendravimą su atsakingomis institucijomis ir įstaigomis;

10. IVPK IS saugos įgaliotinis ir kibernetinio saugumo vadovas gali būti tas pats asmuo.

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

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

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

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

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

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

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

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

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

12.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

12.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

12.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

12.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

12.5. IVPK IS nuostatais;

12.6. Kibernetinio saugumo reikalavimų aprašu;

12.7. 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“;

12.8. 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“;

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

12.10. 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).

12.11. Bendruoju duomenų apsaugos reglamentu.

12.12.IVPK IS saugos dokumentais;

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS 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 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“ 9 punktu ir 12.3. papunkčiu, IVPK IS tvarkoma informacija yra priskiriama vidutinės svarbos informacijos kategorijai, o IVPK IS yra priskiriama trečiai kategorijai.

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

14.1. 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);

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

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

14.4. nenugalima jėga (force majeure).

15. IVPK IS saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja IVPK IS rizikos įvertinimą ir parengia rizikos įvertinimo ataskaitą; prireikus jis gali organizuoti neeilinį rizikos įvertinimą.

16. 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.

17. 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:

17.1. įvertinama realios IVPK IS elektroninės informacijos saugos situacijos atitiktis Saugos nuostatų, saugos dokumentų, Organizacinių ir techninių kibernetinio saugumo reikalavimų ir kitų teisės aktų reikalavimams;

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

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

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

18. 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.

19. Kartu su pagrindiniu IVPK IS rizikos vertinimu ir (arba) informacinių technologijų saugos atitikties vertinimu organizuojamas ir atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos IVPK IS kibernetiniam saugumui, vertinimas.

20. IVPK IS elektroninės informacijos saugumo priemonės turi būti parenkamos atsižvelgiant į Saugos nuostatų 14 punkte išvardytus rizikos veiksnius, galinčius turėti įtakos IVPK IS elektroninės informacijos saugumui.

21. 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

22. 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:

22.1. 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;

22.2. apsaugai skirta programinė įranga turi automatiškai informuoti (elektroniniu paštu) atsakinguosius darbuotojus apie kompiuterizuotas darbo vietas ir tarnybines stotis, kuriose įdiegta apsaugai skirta programinė įranga netinkamai funkcionuoja, yra išjungta arba neatsinaujina per 24 valandas.

22.3. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu;

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

23. IVPK IS funkcionavimui reikalingą kompiuterinę, techninę ir programinę įrangą, kurios reikia IVPK IS naudotojo funkcijoms vykdyti, diegia ir prižiūri IVPK IS tvarkytojo Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka atrinkti paslaugų teikėjai (toliau – paslaugų teikėjai), kontroliuojami IVPK IS administratoriaus.

24. Paslaugų teikėjų įsipareigojimai dėl IVPK IS elektroninės informacijos saugos užtikrinimo ir atsakomybės turi būti išdėstyti paslaugų teikimo sutartyse.

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

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

25.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

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

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

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

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

26.3. naudojamos turinio filtravimo sistemos.

27. Leistinos kompiuterių (ypač nešiojamųjų) naudojimo ribos:

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

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

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

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

27.5. 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;

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

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

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

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

28.3. 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;

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

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

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

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

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

V SKYRIUS
REIKALAVIMAI PERSONALUI

30. 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.

31. Kibernetinio saugumo vadovas privalo išmanyti kibernetinio saugumo užtikrinimo principus, tobulinti kvalifikaciją kibernetinio saugumo srityje, savo darbe vadovautis Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais, Kibernetinio saugumo reikalavimų aprašu, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais kibernetinį saugumą.

32. IVPK IS saugos įgaliotiniu ir 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.

33. IVPK IS administratoriumi skiriamas darbuotojas, išmanantis darbą su IVPK IS taikomąja programine įranga ir gebantis atlikti funkcijas, susijusias su IVPK IS naudotojų teisių valdymu. IVPK IS administratorius turi būti pasirašęs konfidencialumo pasižadėjimą saugoti asmens duomenų paslaptį;

34. 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.

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

36. 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.

37. IVPK IS tvarkytojo darbuotojai (išskyrus IVPK IS saugos įgaliotinį ir IVPK IS administratorių), kurie dalyvauja IVPK IS priežiūroje, valdyme ir vystyme privalo gerai išmanyti IVPK IS veiklos principus, būti susipažinę ir vykdyti Saugos dokumentuose numatytus reikalavimus ir procedūras.

38. IVPK IS techninę priežiūrą vykdančių įmonių atsakingi darbuotojai turi atitikti paslaugų IVPK IS vystymo ar priežiūros paslaugų pirkimo dokumentuose numatytus kvalifikacinius reikalavimus bei vykdyti paslaugų teikimo sutartyse numatytas veiklas. Tuomet kai perkamos IVPK IS vystymo ar priežiūros paslaugos yra susijusios su prieigos prie IVPK IS bei joje apdorojamos elektroninės informacijos suteikimu, taikomi šie principai:

38.1. IVPK IS techninę priežiūrą vykdančių įmonių darbuotojams prieiga suteikiama pagal IVPK IS naudotojų administravimo taisykles. IVPK IS techninę priežiūrą vykdančių įmonių darbuotojai yra atsakingi už savalaikį IVPK IS saugos įgaliotinio informavimą apie pasikeitimus jų įmonėje, kurie gali įtakoti IVPK IS techninę priežiūrą vykdančių įmonių darbuotojų prieigos prie IVPK IS panaikinimą ar keitimą (pvz., nedelsiant pranešti apie tai, kad prieigą prie IVPK IS turintis darbuotojas nutraukia darbinius santykius su IVPK IS techninę priežiūrą vykdančia įmone);

38.2. neleidžiamas IVPK IS techninę priežiūrą vykdančių įmonių darbuotojų prieigos prie IVPK IS suteikimas grupinių paskyrų pagrindu;

38.3. prieš IVPK IS techninę priežiūrą vykdančių įmonių darbuotojams suteikiant prieigą prie IVPK IS, atitinkami darbuotojai turi pasirašyti konfidencialumo pasižadėjimus ir papildomai turi būti formalizuojami susitarimai tarp IVPK IS tvarkytojo ir IVPK IS techninę priežiūrą teikiančių įmonių, kuriuose būtų nurodyta:

38.3.1. elektroninė informacija ir elektroninės informacijos apdorojimo priemonės, prie kurių IVPK IS techninę priežiūrą teikiančių įmonių darbuotojams suteikiama prieiga;

38.3.2. prieigos tipas (fizinė prieiga, loginė prieiga, nuotolinė prieiga, prieiga lokalioje darbo vietoje);

38.3.3. su prieiga prie IVPK IS susijusios rizikos;

38.3.4. prieigos suteikimo laikotarpis, bei leidžiami prisijungimo laikai paros metu;

38.3.5. IVPK IS techninę priežiūrą teikiančių įmonių darbuotojų galimi atlikti veiksmai IVPK IS;

38.3.6. IT incidentų ir elektroninės informacijos saugos incidentų valdymo nuostatos ar nuorodos į jas;

38.3.7. IVPK IS techninę priežiūrą teikiančių įmonių darbuotojų bei IVPK IS tvarkytojo darbuotojų pareigos ir atsakomybės prieigos suteikimo laikotarpiu;

38.3.8. teisė stebėti IVPK IS techninę priežiūrą teikiančių įmonių darbuotojų veiksmus, atliekamus IVPK IS IT komponentuose;

38.3.9. IVPK IS techninę priežiūrą teikiančios įmonės paslaugų teikimo reikalavimai;

38.3.10. ataskaitos ir informacija, kurią turi teikti IVPK IS techninę priežiūrą teikiančios įmonės, siekiant įrodyti atitiktį paslaugų teikimo reikalavimams;

38.3.11. problemų ir nesutarimų tarp IVPK IS tvarkytojo ir IVPK IS techninę priežiūrą teikiančios įmonės sprendimo nuostatos;

38.3.12. susitarimų keitimo nuostatos;

38.3.13. nuorodos į būtinas vadovautis IVPK IS saugos procedūras ir reikalavimus.

39. Informacijos, susijusios su IVPK IS elektroninės informacijos saugos valdymu, apsikeitimas, apimtis, informacijos teikėjai ir gavėjai yra numatyti konkrečiose IVPK IS elektroninės informacijos saugos valdymo procedūrose ir turi būti vykdomas pagal IVPK IS saugos dokumentų nuostatas.

40. IVPK IS Saugos dokumentai, IVPK IS elektroninės informacijos saugos valdymo įrašai turi būti saugomi ir laiku naikinami.

41. IVPK IS saugomi duomenys bei Saugos dokumentai, IVPK IS elektroninės informacijos saugos valdymo įrašai turi būti klasifikuojami pagal šias taisykles:

41.1. klasifikavimo žymai „Vieša informacija“ priskiriama elektroninei informacijai, kuri naudotojams IVPK IS atvaizduojama neprisijungus prie sistemos (vieša sritis). Tokiai elektroninei informacijai netaikomi specifiniai konfidencialumo, žymėjimo ar naikinimo reikalavimai ir turi būti

užtikrintas tokios elektroninės informacijos vientisumas bei bendrinis IVPK IS taikomas prieinamumo lygis;

41.2. klasifikavimo žymai „Privati informacija“ priskiriama elektroninei informacijai, kuri naudotojams IVPK IS atvaizduojama prisijungus prie sistemos. Tokiai elektroninei informacijai netaikomi specifiniai žymėjimo reikalavimai, tačiau turi būti užtikrintas tokios elektroninės informacijos konfidencialumas (ją atvaizduojant tik atitinkamam autorizuotam naudotojui bei pagal IVPK IS funkcionalumą su elektronine informacija susijusiems IVPK IS tvarkytojo, IVPK IS techninę priežiūrą vykdančių įmonių ar institucijų atsakingiems darbuotojams), vientisumas (užtikrinant, kad elektroninė informacija nebūtų pakeičiama be atitinkamo naudotojo ar pagal IVPK IS funkcionalumą su elektronine informacija susijusių IVPK IS tvarkytojo, IVPK IS techninę priežiūrą vykdančių įmonių ar institucijų atsakingų darbuotojų žinios), prieinamumas (taikant bendrinį IVPK IS prieinamumo lygį);

41.3. klasifikavimo žymai „Jautri informacija“ priskiriama elektroninei informacijai, kuri atvaizduojama IVPK IS administravimo skiltyje, taip pat elektroninė informacija, sudaranti IVPK IS elektroninės informacijos saugos valdymą. Tokiai elektroninei informacijai taikomi specifiniai žymėjimo reikalavimai (tik IVPK IS elektroninės informacijos saugos valdymą sudarantiems dokumentams ir įrašams), turi būti užtikrintas tokios elektroninės informacijos konfidencialumas (ją atvaizduojant tik IVPK IS administratoriui bei pagal IVPK IS funkcionalumą ar IVPK IS elektroninės informacijos saugos valdymo funkcijas su elektronine informacija susijusiems IVPK IS tvarkytojo, IVPK IS techninę priežiūrą vykdančių įmonių ar institucijų atsakingiems darbuotojams), vientisumas (užtikrinant, kad elektroninė informacija nebūtų pakeičiama be IVPK IS administratoriaus ar pagal IVPK IS funkcionalumą ar IVPK IS elektroninės informacijos saugos valdymo funkcijas su elektronine informacija susijusių IVPK IS tvarkytojo, IVPK IS techninę priežiūrą vykdančių įmonių ar institucijų atsakingų darbuotojų žinios), prieinamumas (taikant bendrinį IVPK IS prieinamumo lygį).

42. Elektroninės informacijos laikmenas su bet kurio lygmens elektronine informacija galima be apribojimų pakartotinai naudoti kitos žymos elektroninei informacijai saugoti. Vykdant IVPK IS priežiūrą (pvz., keičiant atsarginių kopijų saugojimo politiką), sankcionuotas bet kurio lygmens IVPK IS elektroninės informacijos ištrynimas iš elektroninės informacijos laikmenų galimas naudojant įprastus operacinių sistemų siūlomus trynimo mechanizmus. Perduodant IVPK IS IT komponentus remontui turi būti užtikrinta, kad elektroninės informacijos laikmenos nebūtų perduotos pašaliniams asmenims. Jei yra poreikis IVPK IS elektroninės informacijos laikmenas perduoti fiziniu būdu, elektroninės informacijos laikmenos perduodamos tiesiogiai gavėjui. Didelės apimties duomenų eksportas galimas tik suderinus su IVPK IS saugos įgaliotiniu.

43. IVPK IS Saugos dokumentai elektroninėje formoje turi būti talpinami IVPK IS tvarkytojo turinio valdymo sistemoje, dokumentą sukūrusio ar už jo sukūrimą atsakingo IVPK IS tvarkytojo darbuotojo. Tokio dokumento pavadinimas turi būti sudaromas taip:

43.1. nurodoma klasifikavimo žyma;

43.2. nurodomas bylos pavadinimas;

43.3. nurodoma bylos versija.

44. IVPK IS Saugos dokumentai turi būti prieinami visiems IVPK IS tvarkytojo darbuotojams, kurie dalyvauja IVPK IS priežiūroje, valdyme ir vystyme.

VII SKYRIUS
IVPK IS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

45. IVPK IS saugos įgaliotinis organizuoja pasirašytiną IVPK IS tvarkytojo darbuotojų, kurie dalyvauja IVPK IS priežiūroje, valdyme ir vystyme, supažindinimą su Saugos dokumentais. IVPK IS techninę priežiūrą vykdančioms įmonėms taikomi IVPK IS elektroninės informacijos saugos valdymo reikalavimai yra išdėstomi atitinkamose sutartyse. Esant poreikiui, IVPK IS naudotojams taikytini IVPK IS elektroninės informacijos saugos valdymo reikalavimai pateikiami susipažinimui elektroninėmis IVPK IS priemonėmis.

46. 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.

47. 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.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

48. 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. Saugos dokumentai turi būti derinami su krašto apsaugos ministro įgaliota institucija, įgyvendinančia valstybės informacinių išteklių politiką, Kibernetinio saugumo reikalavimų aprašo nustatyta tvarka.

49. 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.

50. IVPK IS saugos įgaliotinis, IVPK IS duomenų valdymo įgaliotinis, IVPK IS administratorius, kibernetinio saugumo vadovas ir IVPK IS naudotojai, pažeidę Saugos nuostatų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka. IVPK IS techninę priežiūrą vykdančių įmonių atsakingi darbuotojai pažeidę jiems tarpusavio sutartimi su IVPK IS tvarkytoju privalomus IVPK IS elektroninės informacijos saugos valdymo reikalavimus, atsako pagal atitinkamoje sutartyje numatytą tvarką.

_____

Pakeitimai:

1.
Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos, Įsakymas

Nr. T-52, 2016-08-30, paskelbta TAR 2016-08-30, i. k. 2016-22882
Dėl Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2016 m. balandžio 29 d. įsakymo Nr. T-28 „Dėl Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo duomenų saugos nuostatų patvirtinimo“ pakeitimo

2.
Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos, Įsakymas
Nr. T-94, 2018-08-28, paskelbta TAR 2018-08-30, i. k. 2018-13597
Dėl Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2016 m. balandžio 29 d. įsakymo Nr. T-28 „Dėl Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo duomenų saugos nuostatų patvirtinimo“ pakeitimo

3.
Informacinės visuomenės plėtros komitetas prie Ūkio ministerijos, Įsakymas
Nr. T-129, 2018-11-19, paskelbta TAR 2018-11-20, i. k. 2018-18646
Dėl Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2016 m. balandžio 29 d. įsakymo Nr. T-28 „Dėl Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo duomenų saugos nuostatų patvirtinimo“ pakeitimo