Suvestinė redakcija nuo 2021-08-28

Įsakymas paskelbtas: TAR 2020-04-20, i. k. 2020-08213

INFORMACINĖS VISUOMENĖS PLĖTROS KOMITETO DIREKTORIUS

ĮSAKYMAS DĖL TARPŽINYBINĖS DUOMENŲ SAUGYKLOS IR INFORMACINĖS VISUOMENĖS PLĖTROS STEBĖSENOS INFORMACINĖS SISTEMOS SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ PATVIRTINIMO

2020 m. balandžio 20 d. Nr. TE-37(2020)
Vilnius

Pakeistas teisės akto pavadinimas:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7, 12 ir 13 punktais ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 5.3 papunkčiu ir 6 punktu:

1. T v i r t i n u pridedamus Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos saugos politiką įgyvendinančius dokumentus:

1.1. Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisykles;

1.2. Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos veiklos tęstinumo valdymo planą;

1.3. Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos naudotojų administravimo taisykles.

Punkto pakeitimai:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

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

2.1. Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2007 m. lapkričio 29 d. įsakymą Nr. T-174 „Dėl Saugaus Tarpžinybinės mokestinių duomenų saugyklos elektroninės informacijos tvarkymo taisyklių ir Tarpžinybinės mokestinių duomenų saugyklos naudotojų administravimo taisyklių patvirtinimo“ su visais pakeitimais ir papildymais;

2.2. Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2016 m. gegužės 17 d. įsakymą Nr. T-33 „Dėl Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo saugos politiką įgyvendinančių dokumentų patvirtinimo“;

2.3. Informacinės visuomenės plėtros komiteto direktoriaus 2019 m. liepos 29 d. įsakymą Nr. T-76 „Dėl Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2016 m. gegužės 17 d. įsakymo Nr. T-33 „Dėl Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo saugos politiką įgyvendinančių dokumentų patvirtinimo“ pakeitimo“.

Direktorius Gintautas Mežetis

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2020 m. balandžio 3d. raštu Nr. (4.1 E) 6K-225

PATVIRTINTA
Informacinės visuomenės plėtros komiteto
direktoriaus 2020 m. balandžio 20 d.
įsakymu Nr. TE-37(2020)

TARPŽINYBINĖS DUOMENŲ SAUGYKLOS IR INFORMACINĖS VISUOMENĖS PLĖTROS STEBĖSENOS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

Pakeistas priedo pavadinimas:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato tvarką, užtikrinančią elektroninės informacijos saugos ir kibernetinio saugumo politikos, apibrėžtos Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos saugos nuostatuose, patvirtintuose Informacinės visuomenės plėtros komiteto direktoriaus 2016 m. balandžio 29 d. įsakymu Nr. T-28 „Dėl Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – Saugos nuostatai), įgyvendinimą
Punkto pakeitimai:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

2. Taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu ir Saugos dokumentų turinio 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Aprašas).

3. Taisyklės privalomos Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos (toliau – IVPK IS) naudotojams, IVPK IS priežiūros paslaugų teikėjams ir IVPK IS administratoriui. Už Taisyklių įgyvendinimo organizavimą ir kontrolę atsako IVPK IS saugos įgaliotinis.
Punkto pakeitimai:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

4. Taisyklėse vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme ir Bendrųjų elektroninės

informacijos saugos reikalavimų apraše (toliau – Bendrųjų saugos reikalavimų aprašas) vartojamas sąvokas.

5. IVPK IS tvarkoma informacija yra priskiriama vidutinės svarbos informacijos kategorijai, o IVPK IS yra priskiriama trečiai kategorijai.

6. IVPK IS tvarkoma Tarpžinybinės duomenų saugyklos nuostatuose, patvirtintuose Informacinės visuomenės plėtros komiteto direktoriaus 2007 m. rugsėjo 4 d. įsakymu Nr. T-119 „Dėl Tarpžinybinės duomenų saugyklos nuostatų patvirtinimo" ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos nuostatuose, patvirtintuose Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2011 m. liepos 13 d. įsakymu Nr. T-96 „Dėl Informacinės visuomenės plėtros stebėsenos informacinės sistemos nuostatų ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo" (toliau – IVPK IS nuostatai) III skyriuje išvardinta elektroninė informacija. Už jos tvarkymą atsakingi IVPK IS naudotojai ir IVPK IS administratoriai, kuriems naudotojų administravimo taisyklių nustatyta tvarka suteikta IVPK IS duomenų tvarkymo teisė.

Punkto pakeitimai:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

7. IVPK IS techninės ir kompiuterinės įrangos saugos priemonės:

7.1. visose tarnybinėse stotyse ir kompiuterizuotose darbo vietose įdiegta ir reguliariai atnaujinama virusų ir kenkėjiško kodo aptikimo bei šalinimo programinė įranga, skirta tikrinti kompiuterius ir laikmenas. Kompiuterizuotose darbo vietose naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, kurios reguliariai atnaujinamos;

7.2. pagrindinės tarnybinės stotys, svarbiausi duomenų perdavimo tinklo mazgai ir ryšio linijos yra dubliuojami ir jų techninė būklė nuolat stebima;

7.3. tarnybinės stotys ir svarbiausi elektroninės informacijos perdavimo tinklo mazgai turi įtampos filtrą ir rezervinį elektros energijos tiekimo šaltinį. Rezervinis elektros energijos tiekimo šaltinis užtikrina pagrindinių tarnybinių stočių veikimą ne trumpiau kaip 1 val.

7.4. IVPK IS naudotojui ilgiau kaip 15 (penkiolika) minučių neatliekant jokių veiksmų informacinėse sistemose, taikomoji programinė įranga turi užsirakinti, kad toliau naudotis informacinėmis sistemomis galima būtų tik IVPK IS naudotojui pakartotinai patvirtinus savo tapatybę.

8. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

8.1. IVPK IS darbui naudojama tik legali sisteminė ir taikomoji programinė įranga;

8.2. IVPK IS tarnybinėse stotyse neturi veikti sisteminė ir taikomoji programinė įranga, kuri yra nesusijusi su IVPK IS tvarkymu, IVPK IS naudotoju ir pačios įrangos administravimu;

8.3. turi būti operatyviai ištestuojami ir įdiegiami IVPK IS tarnybiniu stočių ir vidinių IVPK IS naudotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

8.4. IVPK IS tvarkymo darbo vietose naudojama programinė įranga, skirta kovai su kenksmingojo kodo programomis, ir laiku atliekamas visos programinės įrangos atnaujinimas;

8.5. IVPK IS programinis kodas privalo būti apsaugotas nuo paskelbimo neturintiems teisės su juo susipažinti asmenims. IVPK IS programiniam kodui apsaugoti taikomos tos pačios saugos priemonės kaip ir IVPK IS elektroninei informacijai;

8.6. programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka paslaugos teikėjo, kuriam perduotos atlikti valstybės informacinės sistemos techninės ir programinės įrangos priežiūros funkcijos, paskirtas darbuotojas tik IVPK IS administratoriaus nurodymu;

8.7. programinė įranga prižiūrima laikantis gamintojo rekomendacijų;

8.8. programinės įrangos testavimas atliekamas naudojant atskirą testavimo aplinką;

8.9. per metus turi būti užtikrintas IVPK IS prieinamumas 90 proc. laiko darbo metu darbo dienomis.

9. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

9.1. tarnybinės stotys, kompiuterizuotos darbo vietos ir kita kompiuterinė įranga, įjungta į elektroninės informac ijos perdavimo tinklą, yra atskirta nuo viešųjų telekomunikacinių tinklų ugniasienėmis;

9.2. ugniasienės įvykių žurnalai (angl. *Logs*) reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

9.3. ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo ar pažeidimo;

9.4. IVPK IS programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų;

9.5. prie IVPK IS prisijungiant nuotoliniu būdu ar keičiantis informacija su kitais registrais ir informacinėmis sistemomis, viešaisiais telekomunikacijų tinklais perduodamų duomenų konfidencialumas užtikrinamas naudojant virtualų privatų tinklą (angl. *Virtual Private Network, VPN*) ir kitus duomenų šifravimo būdus (SSL, HTTPS ar lygiaverčius).

10. Belaidžio tinklo saugumas ir kontrolė:

10.1. leidžiama naudoti tik su kompetentingu asmeniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidžio tinklo įrenginius, atitinkančius techninius kibernetinio saugumo reikalavimus;

10.2. turi būti naudojamos priemonės, kurios apribotų neleistinus ar saugumo reikalavimų neatitinkančius belaidžius įrenginius arba informuotų kompetentingą asmenį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, apie neleistinos įrangos prijungimą prie IVPK IS infrastruktūros;

10.3. kompiuteriuose, mobiliuosiuose įrenginiuose turi būti išjungta belaidė prieiga, jeigu jos nereikia darbo funkcijoms atlikti, išjungtas lygiarangis (angl. *peer to peer*) funkcionalumas, belaidė periferinė prieiga.

11. IVPK IS patalpų saugos priemonės:

11.1. patalpose, kuriose yra IVPK IS tarnybinės stotys, turi būti įdiegta signalizacija, saugos priemonės, užtikrintos gamintojo rekomenduojamos techninės įrangos darbo sąlygos (aplinkos drėgnumas, darbo vietos temperatūra), turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir (arba) apsaugos tarnybos stebėjimo pulto;

11.2. patalpos, kuriose yra IVPK IS tarnybinės stotys, turi būti atskirtos nuo bendrojo naudojimo patalpų. Į patalpas patekti gali tik įgalioti asmenys, kitus asmenis turi lydėti IVPK IS administratorius arba saugos įgaliotinis;

11.3. prieiga prie patalpų, kuriose yra IVPK IS tarnybinės stotys, turi būti kontroliuojama (registruojami įeinančių ir išeinančių iš patalpų apsilankymai).

12. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių (išmaniųjų telefonų ir planšetinių kompiuterių, naudojančių Android ar iOS operacines sistemas), naudojamų prisijungimui prie informacinių sistemų, naudojimo tvarka:

12.1. prisijungimui prie IVPK IS leidžiama naudoti tik tarnybinius nešiojamuosius kompiuterius;

12.2. išnešti iš patalpų nešiojamieji kompiuteriai negali būti palikti be priežiūros; jei įmanoma, naudotojas turi laikyti nešiojamąjį kompiuterį prie savęs visą laiką, ypač viešosiose vietose;

12.3. turi būti įdiegiami operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

12.4. duomenys, perduodami tarp mobiliojo įrenginio ir informacinės sistemos, turi būti šifruojami taikant VPN technologiją;

12.5. jungiantis prie IVPK IS išteklių, turi būti patvirtinamas tapatumas; mobiliajame įrenginyje ar jo taikomojoje programinėje įrangoje turi būti uždrausta automatiškai išsaugoti slaptažodį.

13. IVPK IS naudojamų svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė:

13.1. atpažinties, tapatumo patvirtinimo ir naudojimosi kontrolės reikalavimai:

13.1.1. draudžiama slaptažodžius saugoti programiniame kode;

13.1.2. svetainės, patvirtinančios nuotolinio prisijungimo tapatumą, turi drausti automatiškai išsaugoti slaptažodžius;

13.2. turi būti įgyvendinti svetainės kriptografijos reikalavimai:

13.2.1. svetainės administravimo darbai turi būti atliekami per šifruotą ryšio kanalą, šifruojant ne trumpesniu kaip 128 bitų raktu;

13.2.2. šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų; sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų;

13.2.3. svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. *Hardware security module*);

13.3. turi būti naudojama svetainės naudotojo įvedamų duomenų tikslumo kontrolė (angl. *Validation*);

13.4. tarnybinė stotis, kurioje yra svetainė, neturi rodyti svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį;

13.5. tarnybinė stotis, kurioje yra svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus HTTP metodus;

13.6. turi būti uždrausta naršyti svetainės aplankuose (angl. *Directory browsing*).

14. Kitos priemonės, naudojamos užtikrinti IVPK IS elektroninės informacijos saugą:

14.1. prisiregistravimo prie IVPK IS ir išsiregistravimo iš jo duomenys (prisijungimo vardas, data, laikas) fiksuojami IVPK IS elektroniniuose veiksmų žurnaluose (toliau — veiksmu žurnalai), kurie prieinami tik atitinkamai IVPK IS administratoriui ir saugos įgaliotiniui. Veiksmų žurnalai yra saugojami IVPK IS duomenų bazėje ir jų apsaugai nuo neteisėto jų duomenų pakeitimo yra taikomos tos pačios saugos priemonės, kaip ir IVPK IS elektroninei informacijai. Už veiksmų žurnalų tvarkymą atsakingas IVPK IS administratorius;

14.2. IVPK IS turi būti įrašomi ir vienerius metus saugomi duomenys apie IVPK IS tarnybinių stočių, taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis tarnybinėse stotyse, IVPK IS taikomojoje programinėje įrangoje, visus IVPK IS naudotoju vykdomus veiksmus, kitus elektroninės informacijos saugai svarbius įvykius, nurodant IVPK IS naudotojo identifikatorių ir elektroninės informacijos saugai svarbaus įvykio ar vykdyto veiksmo laiką; šie duomenys turi būti saugomi ne toje pačioje IVPK IS, kurioje jie įrašomi, taip pat jie turi būti analizuojami ne rečiau kaip kartą per savaitę;

14.3. prisijungimo vardai ir slaptažodžiai, leidžiantys dirbti su IVPK IS tarnybinės stoties programine įranga, turi būti žinomi tik įgaliotam asmeniui;

14.4. IVPK IS naudotojų tapatybei nustatyti ir prieigai prie elektroninės informacijos kontroliuoti būtina naudoti prisijungimo vardų, slaptažodžių ir teisių sistemą;

14.5. IVPK IS administratorius privalo nedelsdamas informuoti apie IVPK IS techninės ir programinės įrangos gedimus, kurie negali būti pašalinami per vieną valandą nuo gedimo pastebėjimo, IVPK IS saugos įgaliotinį.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

15. Elektroninės informacijos įvedimo, keitimo, atnaujinimo ir naikinimo tvarka:

15.1. IVPK IS tvarkomus duomenis įrašyti, keisti, atnaujinti gali tik IVPK IS naudotojai ir administratorius pagal suteiktas prieigos teises;

15.2. IVPK IS elektroninė informacija įrašoma, atnaujinama, keičiama ir naikinama vadovaujantis IVPK IS nuostatais, Saugos nuostatais ir kitais teisės aktais, reglamentuojančiais IVPK IS elektroninės informacijos tvarkymą;

15.3. informacinės sistemos turi turėti įrašytos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones;

15.4. IVPK IS naudotojų duomenis įrašyti, keisti, atnaujinti gali tik naudotojų administratorius;

15.5. IVPK IS naudotojams ar administratoriui, atliekant veiksmus su IVPK IS elektronine informacija automatiškai veiksmų žurnale registruojamas darbo laikas, prisijungimo vardas ir atliekami veiksmai. Šie duomenys skirti elektroninės informacijos vientisumo pažeidimams nustatyti.

15.6. Duomenys, perkelti į IVPK IS archyvą, naikinami IVPK IS nuostatų VI skyriuje nustatyta tvarka.

16. IVPK IS elektroninės informacijos kopijų rengimas:

16.1. IVPK IS elektroninės informacijos kopijos daromos ne rečiau kaip kartą per savaitę ir įrašomos į kompiuterines laikmenas;

16.2. elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijas neteisėtai atkurti elektroninę informaciją;

16.3. IVPK IS elektroninės informacijos kopijos saugomos atskiroje patalpoje taip, kad prireikus būtu galima jas greitai atkurti;

16.4. duomenys apie IVPK IS elektroninės informacijos kopijų darymą (kopijos įrašymo data ir laikas, sistemos administratoriaus vardas, pavardė, pareigos, telefonas) fiksuojami kopijų darymo žurnale;

16.5. sunaikintos ar sugadintos IVPK IS elektroninės informacijos atkūrimą kontroliuoja IVPK IS administratorius.

17. IVPK IS elektroninė informacija kitoms informacinėms sistemoms neteikiama.

18. IVPK IS elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau — neteisėta veikla) nustatymo tvarka:

18.1. IVPK IS administratorius privalo ne rečiau nei kartą per mėnesį peržiūrėti visus IVPK IS veiksmų žurnaluose registruojamus įrašus, siekiant patikrinti, ar nėra vykdoma neteisėta veikla;

18.2. kilus įtarimui, kad su IVPK IS ar jo elektronine informacija yra vykdoma neteisėta veikla, IVPK IS naudotojai privalo nedelsiant informuoti IVPK IS administratorių, kuris turi iškart reaguoti i tokį pranešimą ir imtis visų įmanomų veiksmų, reikalingų neteisėtai veiklai užkirsti;

18.3. IVPK IS saugos įgaliotinis, ne rečiau kaip kartą per 2 metus:

18.3.1. atlieka IVPK IS saugos dokumentų ir realios informacijos saugos situacijos atitikties vertinimą;

18.3.2. atlieka IVPK IS techninės ir programinės įrangos inventorizaciją;

18.3.3. patikrina IVPK IS administratoriaus kompiuterinėje darbo vietoje, IVPK IS tarnybinėse stotyse įdiegtas programas ir jų sąranką;

18.3.4. patikrina IVPK IS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktį;

18.3.5. įvertina pasirengimą užtikrinti IVPK IS veiklos tęstinumą įvykus saugos incidentui.

19. Programinės ir techninės IVPK IS įrangos keitimo ir atnaujinimo tvarka:

19.1. visi IVPK IS pokyčiai, susiję su programinės ir (arba) techninės įrangos keitimu ir (arba) atnaujinimu įgyvendinami tik raštiškai sutikus IVPK IS valdytojui;

19.2. prieš atliekant IVPK IS programinės ir (arba) techninės įrangos keitimą ir (arba) atnaujinimą, kurio metu galimi IVPK IS veikimo sutrikimai, IVPK IS administratorius ją įdiegia ir testuoja, jei tai leidžia programinės ir techninės galimybės, testavimo aplinkoje;

19.3. atlikus testavimą ir konstatavus keičiamos ir (arba) atnaujinamos IVPK IS programinės ir (arba) techninės įrangos sėkmingą veikimą realioje aplinkoje, IVPK IS administratorius pradeda rengti keičiamos ir (arba) atnaujinamos programinės ir (arba) techninės įrangos keitimo ir (arba) atnaujinimo planą, kuriame turi būti:

19.3.1. išdėstytas detalus veiksmų planas, nurodantis atliekamų darbų etapus, eiliškumą, apimtį ir trukmę valandų tikslumu;

19.3.2. paskirti ir nurodyti konkretūs asmenys (vardas, pavardė, pareigos, telefono numeris bei kita kontaktinė informacija), kurie atsakingi už detaliame veiksmų plane įvardintų darbų įgyvendinimą;

19.3.3. išvardintos rizikos, atsirandančios keičiant ir (arba) atnaujinant IVPK IS programinę ir (arba) techninę įrangą, bei veiksmai ir priemonės skirtos jas minimizuoti arba visiškai eliminuoti;

19.3.4. išvardintos atitinkamai IVPK IS naudotojų informavimo priemonės ir būdai apie vykdomų darbų eigą.

20. Visi pokyčiai, galintys sutrikdyti ar sustabdyti IVPK IS darbą, turi būti suderinti su informacinės sistemos valdytojo vadovu ar duomenų valdymo įgaliotiniu ir vykdomi tik gavus jų raštišką pritarimą. Pokyčius turi teisę inicijuoti duomenų valdymo įgaliotinis, saugos įgaliotinis ar administratorius, o įgyvendinti – administratorius.

21. IVPK IS pokyčių (toliau – pokyčiai) valdymo tvarka:

21.1. reikalingi pokyčiai turi būti identifikuojami administratoriaus;

21.2. pokyčių svarbumo apibrėžimas atsižvelgiant į pokyčių svarbą;

21.3. pokyčių įtakos veiklos tęstinumui ir duomenų saugumui pokyčių diegimo metu įvertinimas;

21.4. galimybės atstatyti buvusią duomenų versiją užtikrinimas;

21.5. pokyčių įgyvendinimas.

22. IVPK IS sąrankos aprašai turi būti nuolat atnaujinami ir rodyti esamą informacinės sistemos sąrankos būklę.

23. Pokyčiai, galintys daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti bandomojoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos IVPK IS.

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINĖMS SISTEMOMS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

24. IVPK IS tvarkytojas:

24.1. atsako už prieigos prie programinių, techninių ir kitų išteklių, reikalingų paslaugos teikėjui, teikiančiam IVPK IS priežiūros paslaugą, suteikimo ir panaikinimo organizavimą;

24.2. numato ir išdėsto paslaugų teikimo sutartyje saugos reikalavimus ir jų laikymosi bei atsakomybės sąlygas;

24.3. paskiria asmenį, atsakingą už sutarties reikalavimų vykdymo priežiūrą.

25. IVPK IS saugos įgaliotinis supažindina IVPK IS priežiūros paslaugų teikėją su suteiktos prieigos prie IVPK IS saugos reikalavimais ir sąlygomis.

26. Pasibaigus sutarties su IVPK IS priežiūros paslaugos teikėju galiojimo terminui, IVPK IS administratorius nedelsdamas organizuoja suteiktos prieigos prie IVPK IS panaikinimą.

27. Paslaugos teikėjas, teikiantis IVPK IS prieglobos paslaugas, turi užtikrinti patalpų, techninės ir programinės įrangos bei elektroninės informacijos perdavimo tinklais saugos priemones, išdėstytas Taisyklių III skyriuje ir yra atsakingas už IVPK IS elektroninės informacijos kopijų darymą, saugojimą bei IVPK IS elektroninės informacijos iš kopijų atkūrimą.

28. Detalesni reikalavimai IVPK IS techninę priežiūrą vykdančių įmonių paslaugoms ir saugos užtikrinimo principai išdėstyti IVPK IS Saugos nuostatų 38 punkte.

29. Už paslaugų teikimo kontrolę ir saugos priemonių auditą atsakingas IVPK IS tvarkytojas.

_____

PATVIRTINTA
Informacinės visuomenės plėtros komiteto
direktoriaus 2020 m. balandžio 20 d. įsakymu
Nr. TE-37(2020)

TARPŽINYBINĖS DUOMENŲ SAUGYKLOS IR INFORMACINĖS VISUOMENĖS PLĖTROS STEBĖSENOS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

Pakeistas priedo pavadinimas:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos naudotojų administravimo taisyklės (toliau – Naudotojų administravimo taisyklės) nustato Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos (toliau – IVPK IS) naudotojų įgaliojimus, teises, pareigas ir kontrolės tvarką.
Punkto pakeitimai:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

2. Naudotojų administravimo taisyklėse vartojamos sąvokos:

2.1. **Principas „būtina darbui“** – prieigos prie duomenų principas, reiškiantis, kad asmeniui gali būti suteikta prieigos teisė tik prie tokios apimties duomenų, kokios reikia jo numatytoms funkcijoms atlikti;

2.2. **Principas „būtina žinoti“** – prieigos prie duomenų principas, reiškiantis, kad prieigos teisė prie duomenų gali būti suteikta tik atitinkamą leidimą dirbti ar susipažinti su šiais duomenimis turintiems asmenims;

2.3. **Privilegijuota prieiga** – prieiga prie informacinės sistemos ar jos komponentų, suteikianti galimybę atlikti veiksmus, galinčius sukelti didesnę nei įprastą riziką informacinei sistemai, jos komponentams ar joje tvarkomiems duomenims (informacinių sistemų komponentų administravimas, naudotojų administravimas, specifiniai duomenų tvarkymo veiksmai ir pan.);

2.4. **Privilegijuotas naudotojas** – asmuo (informacinės sistemos naudotojas, administratorius, programuotojas, paslaugų teikėjo darbuotojas ir kt.), kuriam šių Naudotojų administravimo taisyklių nustatyta tvarka suteikta privilegijuota prieiga;

2.5. Kitos Naudotojų administravimo taisyklėse 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“, apibrėžtas sąvokas.

3. Naudotojų administravimo taisyklės taikomos visiems IVPK IS naudotojams, įskaitant privilegijuotus naudotojus.

4. Informacinių sistemų naudotojų prieigos prie informacinių sistemų ir jose tvarkomos elektroninės informacijos suteikimas paremtas „būtina darbui“ ir „būtina žinoti“ principais.

5. Kiekvienas IVPK IS naudotojas turi būti unikaliai identifikuojamas (asmens kodas negali būti naudojamas kaip informacinės sistemos naudotojo identifikatorius). Informacinių sistemų naudotojų prieigos prie elektroninės informacijos teisė realizuota tik per jų registravimo ir slaptažodžių administravimo sistemą.

6. IVPK IS priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą IVPK IS administratoriaus paskyrą, kuria naudojantis negalima atlikti informacinių sistemų naudotojo funkcijų.

II SKYRIUS
NAUDOTOJŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

7. Kiekvienam IVPK IS naudotojui nustatomos atitinkamos teisės tvarkyti IVPK IS elektroninę informaciją. Už šių teisių suteikimą atsakingas IVPK IS administratorius.

8. Kiekvienas IVPK IS naudotojas ar administratorius, jungdamasis prie IVPK IS privalo atlikti tapatumo nustatymo procedūrą, t. y. nurodyti IVPK IS naudotojo vardą ir slaptažodį.

9. IVPK IS naudotojai gali naudotis tik tomis IVPK IS dalimis ir jose apdorojamais duomenimis, prie kurių prieiga jiems yra numatyta pagal pareigas.

10. IVPK IS naudotojams draudžiama leisti kitiems asmenimis naudotis jiems paskirtu prieigos vardu, nebent esant objektyvioms priežastims ir gavus IVPK IS administratoriaus leidimą.

11. Informacinių sistemų naudotojai privalo saugoti tvarkomų asmens duomenų ir informacijos paslaptį 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1) nustatyta tvarka.

12. Esant poreikiui tam pačiam asmeniui vykdyti funkcijas, susijusias su veiksmais, galinčiais sukelti didesnę nei įprastą riziką IVPK IS, jos komponentams ar joje tvarkomiems duomenims (t. y. reikalaujančiais privilegijuotos prieigos) ir veiksmais, tokios rizikos nekeliančiais, šiam asmeniui šių Naudotojų administravimo taisyklių nustatyta tvarka turi būti sukuriamos atskiros naudotojo paskyros (privilegijuoto naudotojo paskyra ir paprasto (neprivilegijuoto) naudotojo paskyra) atitinkamų funkcijų vykdymui.

13. IVPK IS naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai IVPK IS administratoriui, kuris apie tai informuoja IVPK IS saugos įgaliotinį.

14. Privilegijuotam naudotojui ir IVPK IS administratoriui suteikiama pilna prieiga prie jų funkcijoms atlikti reikalingų sistemos bei naudotojų duomenų bei visų sistemos dalių valdymo parametrų bei teisė juos skaityti, redaguoti, atnaujinti, kopijuoti ar naikinti, kai tai reikalinga užtikrinti sistemos veikimą.

III SKYRIUS

SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO NAUDOTOJAMS KONTROLĖS TVARKA

15. IVPK IS naudotojų (įskaitant privilegijuotus) registravimo ir išregistravimo tvarka:

15.1. IVPK IS tvarkytojo ar IVPK IS techninę priežiūrą teikiančios įmonės darbuotojai, pagal IVPK IS saugos politikos dokumentų nuostatas pasirašę konfidencialumo pasižadėjimus ir esant formalizuotam susitarimui tarp IVPK IS tvarkytojo ir IVPK IS techninę priežiūrą teikiančios įmonės, norėdami savo tiesioginių ar projektinių funkcijų atlikimui gauti privilegijuotą prieigą prie atitinkamų IVPK IS IT komponentų, turi kreiptis į IVPK IS administratorių su atitinkamu prašymu, kurio forma nustatyta Naudotojų administravimo taisyklių 1 priede (toliau – prašymas). Pateikiant tokį prašymą turi būti nurodoma kam, kokiu pagrindu, prie kokių IVPK IS komponentų ir kokiam laikotarpiui privilegijuota prieiga turi būti suteikta;

15.2. IVPK IS naudotojui IVPK IS administratorius suteikia IVPK IS naudotojo vardą ir laikiną slaptažodį bei nustato nurodytos apibrėžties prieigą prie elektroninės informacijos;

15.3. kiekvienam IVPK IS naudotojui suteikiamas nesikartojantis vardas;

15.4. kiekvienas IVPK IS naudotojas privalo naudoti tik jam suteiktą IVPK IS naudotojo vardą ir nesudaryti galimybės juo naudotis kitam asmeniui;

15.5. IVPK IS naudotoju vardai kaupiami ir registruojami centralizuotai naudotojų administravimo posistemėje.

16. Reikalavimai IVPK IS naudotojų slaptažodžiams, jų galiojimo trukmei, keitimui ir saugojimui:

16.1. slaptažodis IVPK IS naudotojui negali būti perduodamas neužšifruotas ar užšifruojamas nepatikimais algoritmais;

16.2. tik laikinas slaptažodis gali būti perduodamas neužšifruotas, tačiau atskirai nuo prisijungimo vardo, jei naudotojas neturi techninių galimybių iššifruoti gauto slaptažodžio ar nėra techninių galimybių IVPK IS naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu;

16.3. pirmojo prisijungimo prie IVPK IS metu iš IVPK IS naudotojo turi būti reikalaujama, kad jis pakeistų laikiną slaptažodį;

16.4. kilus įtarimui, kad slaptažodis galėjo būti atskleistas, IVPK IS naudotojas turi nedelsdamas slaptažodį pakeisti;

16.5. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;

16.6. slaptažodį turi sudaryti trijų grupių iš galimų keturių (didžiosios ir mažosios raidės, skaičiai bei specialūs ženklai) simboliai;

16.7. slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius; IVPK IS naudotojų teisės sustabdomos, jei slaptažodis nepakeičiamas laiku;

16.8. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai, adresai ir panašiai);

16.9. IVPK IS naudotojas slaptažodį turi įsiminti; draudžiama slaptažodį užsirašyti ar pasakyti kitam asmeniui;

16.10. naudotojui klaidingai suvedus slaptažodį 5 kartus vartotojo prieiga turi būti blokuojama ir atstatoma tik IVPK IS administratoriaus;

16.11. pasirinkdamas ar keisdamas slaptažodį, IVPK IS naudotojas turi bent kartą slaptažodį pakartoti;

16.12. keičiant slaptažodį, IVPK IS taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių.

17. Papildomi reikalavimai privilegijuotų naudotojų slaptažodžiams:

17.1. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

17.2. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių.

18. IVPK IS naudotojų prieigos prie informacinių sistemų sustabdymo atvejai:

18.1. nustačius IVPK IS elektroninės informacijos konfidencialumo ar vientisumo pažeidimą arba kitų IVPK IS elektroninės informacijos saugą ir tvarkymą reglamentuojančių teisės aktų pažeidimą;

18.2. pastebėjus neteisėtą prisijungimo prie IVPK IS elektroninės informacijos naudojimą;

18.3. IVPK IS naudotojas nušalinamas nuo darbo (pareigų);

18.4. apie prieigos teisių dirbti su IVPK IS elektronine informacija panaikinimą ar laikiną sustabdymą IVPK IS naudotojo įstaigos vadovas arba jo įgaliotas asmuo elektroniniu laišku informuoja IVPK IS administratorių paskutinę IVPK IS naudotojo darbo dieną.

19. IVPK IS duomenų tvarkymas yra atliekamas naudojantis interneto naršykle arba specialia programine įranga.

_____

Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo naudotojų administravimo taisyklių priedas

(Prašymo forma)

_____
(įstaigos pavadinimas)

Informacinės visuomenės plėtros komitetui

PRAŠYMAS
ĮREGISTRUOTI INFORMACINĖS SISTEMOS NAUDOTOJĄ IR SUTEIKTI AR PANAIKINTI NAUDOTOJO PRIEIGOS PRIE INFORMACINĖS SISTEMOS TEISES

_____ Nr. _____
(data) (registracijos numeris)

_____
(sudarymo vieta)

Prašau suteikti / panaikinti (pabraukti reikalingą variantą) prieigos prie informacinės sistemos (-ų) teises šiam asmeniui:
_____

(valstybės tarnautojo ar darbuotojo vardas, pavardė)
_____,
(valstybės tarnautojo ar darbuotojo pareigos)
dirbančiam (-ai) _____,
(įstaigos struktūrinio padalinio pavadinimas)
_____,
(darbo vietos adresas, kabineto ir telefono numeriai, elektroninio pašto adresas)

ir suteikti / panaikinti jam (jai) prieigą prie registro / informacinės sistemos šiomis prieigos teisėmis:

Eil. Nr.	Informacinės sistemos pavadinimas	Prieigos teisės (rolės)	
		Suteikti	Panaikinti

PASTABA:
Prašyme nurodomos tik tos informacinės sistemos, prie kurių prieigą prašoma suteikti ar panaikinti.

_____ _____ _____
(įstaigos vadovo ar jo įgalioto asmens pareigos) (parašas) (vardas, pavardė)

PATVIRTINTA
Informacinės visuomenės plėtros
komiteto direktoriaus
2020 m. balandžio 20 d.
įsakymu Nr. TE-37(2020)

TARPŽINYBINĖS DUOMENŲ SAUGYKLOS IR INFORMACINĖS VISUOMENĖS PLĖTROS STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS.

Pakeistas priedo pavadinimas:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos veiklos tęstinumo valdymo planas (toliau – Planas) reglamentuoja procedūras, atliekamas siekiant tinkamai valdyti Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos (toliau – IVPK IS) elektroninės informacijos saugos ir kibernetinius incidentus (toliau – Incidentas).

Punkto pakeitimai:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

2. Planas parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu ir Saugos dokumentų turinio 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

3. Plane vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme bei Bendrųjų elektroninės informacijos saugos reikalavimų apraše (toliau – Bendrųjų saugos reikalavimų aprašas).

4. Planas įsigalioja įvykus Incidentui arba Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos (toliau – IVPK IS) veiklos tęstinumo valdymo grupės, aprašytos Plano II skyriuje, vadovo sprendimu.

Punkto pakeitimai:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

5. Planas yra privalomas IVPK IS valdytojui, tvarkytojui, saugos įgaliotiniui, IVPK IS administratoriui ir IVPK IS naudotojams (įskaitant privilegijuotus naudotojus - techninę priežiūrą vykdančių įmonių atsakingus darbuotojus).

6. IVPK IS saugos įgaliotinio, administratorių bei naudotoju funkcijos, įgaliojimai ir veiksmai:

6.1. IVPK IS saugos įgaliotinis atsakingas už:

6.1.1. Plane nurodytų veiksmų atlikimo koordinavimą.

6.1.2. Incidentų registravimą, klasifikavimą ir kitos informacijos, apibūdinančios informacijos saugos incidentus, pildymą jo valdomame registre;

6.1.3. savalaikį Incidentų tyrimą, įrodymų rinkimą ir incidento priežasčių nustatymą ir šių veiksmų koordinavimą;

6.1.4. bendravimą ir bendradarbiavimą su atitinkamomis valstybės institucijomis ir įstaigomis;

6.1.5. užregistruotų informacijos saugos incidentų tendencijų analizę.

6.2. IVPK IS administratorius atsakingas už:

6.2.1. IVPK IS duomenų bazės funkcionavimo atkūrimo organizavimą;

6.2.2. IVPK IS veiklos atkūrimui reikalingos įrangos įsigijimo organizavimą;

6.2.3. atsarginių patalpų, naudojamų IVPK IS veiklai atkurti, organizavimą;

6.2.4. IVPK IS elektroninės informacijos atkūrimo organizavimą;

6.2.5. IVPK IS naudotojų ir duomenų gavėjų informavimą apie veiklos sutrikimus ir jų atstatymo laiką;

6.2.6. IVPK IS galimos ir padarytos žalos vertinimą.

6.3. IVPK IS techninę priežiūrą vykdančių įmonių atsakingi darbuotojai atsakingi už:

6.3.1. IVPK tarnybinių stočių veiklos atkūrimą;

6.3.2. IVPK IS elektroninio ryšio įrangos funkcionavimo atkūrimo organizavimą;

6.3.3. IVPK IS duomenų perdavimo tinklo funkcionavimo atkūrimo organizavimą.

7. IVPK IS veiklos atkūrimas finansuojamas Lietuvos Respublikos valstybės biudžeto lėšomis.

8. IVPK IS veikla laikoma atkurta, jeigu yra atkuriamas incidento metu sutrikdytas IVPK IS veikimas, užtikrintas jo duomenų prieinamumas, konfidencialumas ir vientisumas, o IVPK IS naudotojai gali vykdyti darbines funkcijas įprastu būdu. IVPK IS veiklos atkūrimas turi trukti neilgiau kaip 16 valandų.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

9. IVPK IS veiklos tęstinumo valdymo grupė (toliau – VTVG) užtikrina veiklos tęstinumui kylančių grėsmių valdymą ir informacinių sistemų atkūrimo koordinavimą įvykus Incidentui.

10. VTVG grupę sudaro:

10.1. IVPK IS tvarkytojo – Informacinės visuomenės plėtros komiteto (toliau – IVPK) direktorius arba direktoriaus pavaduotojas (VTVG vadovas);

10.2. IVPK IS saugos įgaliotinis (VTVG vadovo pavaduotojas);

10.3. IVPK IS administratorius;

10.4. IVPK IS techninę priežiūrą vykdančios įmonės atsakingi darbuotojai, priklausomai nuo VAG vadovo sprendimo.

11. VTVG funkcijos:

11.1. situacijos analizė ir sprendimų IVPK IS veiklos tęstinumo valdymo klausimais priėmimas;

11.2. bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

11.3. bendravimas su susijusių registrų / informacinių sistemų veiklos tęstinumo valdymo grupėmis arba administratoriais;

11.4. bendravimas su teisėsaugos ir kitomis institucijomis, institucijos darbuotojais ir kitomis interesų grupėmis;

11.5. finansinių ir kitų išteklių, reikalingų informacinių sistemų veiklai atkurti įvykus Incidentui, naudojimo kontrolė;

11.6. IVPK IS elektroninės informacijos fizinė sauga įvykus Incidentui;

11.7. logistika (žmonių, daiktu, įrangos gabenimas ir jo organizavimas).

12. Įvykus Incidentui, veiklą atkuria IVPK IS veiklos atkūrimo grupė (toliau – VAG), kurią sudaro:

12.1. IVPK IS duomenų valdymo įgaliotinis (VAG vadovas);

12.2. IVPK IS saugos įgaliotinis (VAG vadovo pavaduotojas);

12.3. IVPK IS administratorius;

12.4. IVPK IS prieglobos paslaugų teikėjo atstovas;

12.5. išoriniai ekspertai (jei būtina).

13. VAG funkcijos:

13.1. tarnybinių stočių veikimo atkūrimo organizavimas (tinklo ir tarnybinių stočių administratorius);

13.2. kompiuterių tinklo veikimo atkūrimo organizavimas (tinklo ir tarnybinių stočių administratorius ir kompiuterizuotų darbo vietų administratorius);

13.3. informacinių sistemų elektroninės informacijos atkūrimo organizavimas (tinklo ir tarnybinių stočių administratorius ir informacinių sistemų administratorius);

13.4. taikomųjų programų veikimo atkūrimo organizavimas (tinklo ir tarnybinių stočių administratorius ir informacinių sistemų administratorius);

13.5. kompiuterizuotų darbo vietų veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas (kompiuterizuotų darbo vietų administratorius);

13.6. kitos VAG pavestos funkcijos.

14. Esant Incidentui, VTVG ir VAG organizuoja pasitarimus, atsižvelgdamos į VTVG pirmojo susitikimo metu nustatytą dažnumą, palaiko ryšius visomis tuo metu prieinamomis priemonėmis (el. paštu, mobiliuoju ryšiu ir kt.). VTVG ir VAG turi teisę kviesti į pasitarimus informacinių sistemų tvarkytojų atstovus.

15. Reaguojant į Incidentus ir juos valdant, turi būti vadovaujamasi veiksmais, išdėstytais IVPK IS veiklos atkūrimo detaliajame plane, pateiktame šio Plano priede.

16. IVPK IS veiklos atkūrimo detalųjį planą rengia IVPK IS administratorius. IVPK IS saugos įgaliotinis įvertina parengtą planą ir informuoja IVPK IS tvarkytojo vadovą.

17. Apie įvykdytus veiklos atkūrimo etapus atsakingi asmenys nedelsdami informuoja VAG vadovą.

18. VAG vadovas nuolat informuoja VTVG grupės narius apie IVPK IS veiklos atkūrimo eigą.

19. VTVG ir VAG nariai rengia susitikimus, įvykus esminiams IVPK IS pokyčiams.

20. Atsarginės patalpos, naudojamos IVPK IS veiklai atkurti, turi atitikti visus reikalavimus, keliamus pagrindinėms IVPK IS tarnybinių stočių patalpoms, nurodytus IVPK IS saugaus elektroninės informacijos tvarkymo taisyklių II skyriuje.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

21. Veiklos tęstinumo vykdymui reikalingą detalią informaciją sudaro:

21.1. IVPK IS kompiuterinės ir programinės įrangos sąrašas ir šios įrangos parametrai (dokumentas, kuriame nurodyti informacinių technologijų įrangos parametrai ir už šios įrangos priežiūrą atsakingi administratoriai, minimalus informacinės sistemos veiklai atkurti, nesant administratoriaus, reikiamos kompetencijos ar žinių lygis);

21.2. IVPK IS minimalus funkcijų sąrašas (dokumentas, kuriame nurodyta minimalaus informacinių technologijų įrangos funkcijų, skirtų informacinės sistemos veiklai užtikrinti įvykus Incidentui, sąrašas);

21.3. IVPK IS techninė dokumentacija (dokumentas, kuriame nurodyti pastato, kuriame yra IVPK IS įranga, aukšto patalpų brėžiniai ir juose pažymėti tarnybinės stotys, kompiuterių tinklo ir telefonų tinklo mazgai, kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos, elektros įvedimo pastate vietos);

21.4. kompiuterių tinklo fizinio ir loginio sujungimo schemos;

21.5. sutarčių, susijusių su IVPK IS, sąrašas (dokumentas, kuriame nurodytos elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys, atsakingi už šių sutarčių įgyvendinimo priežiūrą asmenys);

21.6. IVPK IS elektroninės informacijos kopijavimo laikmenų sąrašas (dokumentas, kuriame nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos);

21.7. VTVG ir VAG narių sąrašas su kontaktiniais duomenimis.

22. Už dokumentų, nurodytų Valdymo plano 21.1–21.4 ir 21.6 papunkčiuose, parengimą ir prireikus atnaujinimą yra atsakingas IVPK IS administratorius. Už dokumentų, nurodytų Plano 21.5 ir 21.7 papunkčiuose, parengimą ir prireikus atnaujinimą yra atsakingas IVPK IS saugos įgaliotinis.

23. Už dokumentų, nurodytų Plano 21 punkte, saugojimą yra atsakingas IVPK IS saugos įgaliotinis.

24. Tuo atveju, kai naudojama (pagal nuomos, panaudos ar kitas sutartis) visa IVPK IS techninė įranga ar jos dalis, priklausanti ir esanti trečiosios šalies patalpose – sutarties su trečiąja šalimi data ir numeris, sutarties kopija turi būti saugoma IVPK IS administratoriaus (administratorių).

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

25. Plano veiksmingumo išbandymą organizuoja IVPK IS saugos įgaliotinis.

26. Plano veiksmingumas išbandomas ne rečiau kaip kartą per 2 metus.

27. Prieš įdiegiant naujus IVPK IS komponentus arba pasikeitus veiklos aplinkai saugos įgaliotinis turi peržiūrėti Planą ir, esant reikalui, atlikti neeilinį Plano veiksmingumo išbandymą.

28. Plano veiksmingumo išbandyme turi dalyvauti visi VTVG ir VAG nariai. Esant poreikiui, į Plano veiksmingumo išbandymą gali būti pakviesti ekspertai, paslaugu teikėjų atstovai.

29. Išbandžius Plano veiksmingumą, IVPK IS saugos įgaliotinis parengia Plano veiksmingumo išbandymo ataskaitą (toliau – ataskaita) ir pateikti ją VTVG. Plano kito išbandymo data nurodoma ataskaitoje.

30. Plano veiksmingumo bandymo metu pastebėti trūkumai remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

_____

Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo veiklos tęstinumo valdymo plano priedas

TARPŽINYBINĖS DUOMENŲ SAUGYKLOS IR INFORMACINĖS VISUOMENĖS PLĖTROS STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALAUS PLANAS.”

Pakeistas priedo pavadinimas:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

1. Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos veiklos atkūrimo detalaus plano priede pateikiami galimi esminių sutrikimų scenarijai Tarpžinybinės duomenų saugyklos ir Informacinės visuomenės plėtros stebėsenos informacinės sistemos (toliau – IVPK IS) tvarkytojo patalpose. Tais atvejais, kuomet esminiai sutrikimai įvyksta IVPK IS tarnybinių stočių patalpose, turi būti vadovaujamasi IVPK IS prieglobos paslaugų teikėjo veiklos tęstinumo planu, o IVPK IS veiklos tęstinumo valdymo grupė (toliau – VTVG) ir IVPK IS veiklos atkūrimo grupė (toliau – VAG) turi bendradarbiauti su IVPK IS prieglobos paslaugų teikėju sprendžiant esminio sutrikimo scenarijus.

Punkto pakeitimai:
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138

2. Galimi esminių sutrikimų scenarijai IVPK IS tvarkytojo patalpose:

2.1. Gaisras IVPK IS tvarkytojo patalpose. Reagavimo veiksmai ir IVPK IS veiklos atstatymo veiksmai gaisro atveju pateikiami šio priedo 1 ir 2 lentelėse:

1 lentelė. Reagavimo veiksmai gaisro IVPK IS tvarkytojo patalpose atveju.

Eil. Nr.	Reagavimo veiksmai	Atsakingi asmenys
1.	Esant būtinumui, pavojaus skelbimas, elgsenos nenumatytos situacijos metu rekomendavimas ir darbuotojų evakavimas;	VTVG vadovas (jam nesant – visi IVPK IS tvarkytojo darbuotojai)
2.	Ugniagesių, gelbėjimo, greitosios pagalbos ar kitų tarnybų informavimas;	VTVG vadovas (jam nesant – visi VIISP tvarkytojo darbuotojai)
3.	Esant poreikiui, pirmosios medicininės pagalbos suteikimas;	Visi darbuotojai
4.	Gaisro gesinimas ankstyvoje stadijoje, nekeliant pavojaus darbuotojų gyvybei;	Visi darbuotojai
5.	Komunalinių komunikacijų, galinčių sukelti papildomą pavojų, atjungimas;	VTVG vadovas (jam nesant – visi IVPK IS tvarkytojo darbuotojai)
6.	Koordinuojančių ir operatyvią veiklą vykdančių darbuotojų paskyrimas;	VTVG vadovas

2 lentelė. IVPK IS veiklos atstatymo veiksmai gaisro VIISP tvarkytojo patalpose atveju.

Eil. Nr.	IVPK IS veiklos atstatymo veiksmai	Atsakingi asmenys
1.	Ugniagesių tarnybos paklausimas dėl leidimo dirbti pavojaus zonoje, rekomendacijų darbui gavimas ir darbuotojų informavimas apie rekomenduojamus darbo būdus;	VAG vadovas
2.	Darbo perkėlimas į alternatyvias darbo vietas (pvz.. namuose).	VTVG vadovas
3.	Žalos įvertinimas, priemonių plano įvykio pasekmėms likviduoti sudarymas ir įgyvendinimas;	VAG vadovas
4.	Darbinių funkcijų grąžinimas į esamas ar naujai parinktas patalpas.	VTVG vadovas

2.2. Energijos tiekimo sutrikimai IVPK IS tvarkytojo patalpose. Reagavimo veiksmai ir IVPK IS veiklos atstatymo veiksmai energijos tiekimo sutrikimų atvejais pateikiami šio priedo 3 ir 4 lentelėse:

3 lentelė. Reagavimo veiksmai energijos tiekimo sutrikimų IVPK IS tvarkytojo patalpose atvejais.

Eil. Nr.	Reagavimo veiksmai	Atsakingi asmenys
1.	Energijos tiekimo sistemos veiklos patikrinimas	IVPK IS administratorius
2.	Esant būtinumui, tarnybinių stočių ir kitos techninės įrangos, jautrios energijos tiekimo sutrikimams, išjungimas	IVPK IS administratorius
3.	Kreipimasis į savo elektros energijos tiekimo tarnybą dėl sutrikimo pašalinimo trukmės prognozės	Administratorė
4.	Sutrikimo pašalinimo trukmės prognozės ir rekomenduojamos elgsenos nenumatytos situacijos metu skelbimas	VTVG vadovas
5.	Esant reikalui, atsarginių patalpų IVPK IS tvarkytojo veiklai užtikrinti ir darbo vietoms išdėstyti, suradimas (pvz., darbo perkėlimas į namus)	VTVG vadovas

4 lentelė. IVPK IS veiklos atstatymo veiksmai energijos tiekimo sutrikimų IVPK IS tvarkytojo patalpose atvejais.

Eil. Nr.	Veiklos atstatymo veiksmai	Atsakingi asmenys
1.	Pažeisto vietos elektros tinklo, užtikrinančio IVPK IS tvarkytojo veiklą, atkūrimo organizavimas	VAG vadovas
2.	Išjungtų tarnybinių stočių ir kitos techninės įrangos įjungimas	IVPK IS administratorius
3.	Žalos įvertinimas, priemonių plano įvykio pasekmėms likviduoti sudarymas ir įgyvendinimas	VAG vadovas

2.3. Ryšio sutrikimai IVPK IS tvarkytojo patalpose. Reagavimo veiksmai ir IVPK IS veiklos atstatymo veiksmai ryšio sutrikimų atvejais pateikiami šio priedo 5 ir 6 lentelėse:

5 lentelė. Reagavimo veiksmai ryšio sutrikimų IVPK IS tvarkytojo patalpose atvejais.

Eil. Nr.	Reagavimo veiksmai	Atsakingi asmenys
1.	Paslaugų teikėjų informavimas, atsižvelgus į sutrikimo pobūdį	IVPK IS administratorius
2.	Sutrikimo pašalinimo prognozės skelbimas ir darbuotojų informavimas apie darbo sustabdymą dėl nepalankių sąlygų	VTVG vadovas
3.	Alternatyvaus ryšio ar alternatyvių darbo sąlygų organizavimas	VTVG vadovas
4.	Infrastruktūros pakeitimai, esant poreikiui	IVPK IS administratorius

6 lentelė. IVPK IS veiklos atstatymo veiksmai ryšio sutrikimų IVPK IS tvarkytojo patalpose atvejais.

Eil. Nr.	Veiklos atstatymo veiksmai	Atsakingi asmenys
1.	Žalos bei panašaus pobūdžio įvykių tendencijų įvertinimas	VAG vadovas
2.	Esant poreikiui, kreipimasis į kitus ryšio paslaugų teikėjus	VTVG vadovas

---

Pakeitimai:

1.
Informacinės visuomenės plėtros komitetas, Įsakymas
Nr. TE-57(2021), 2021-08-27, paskelbta TAR 2021-08-27, i. k. 2021-18138
Dėl Informacinės visuomenės plėtros komiteto direktoriaus 2020 m. balandžio 20 d. įsakymo Nr. TE-37(2020) „Dėl Tarpžinybinės mokestinių duomenų saugyklos, Informacinės visuomenės plėtros stebėsenos informacinės sistemos ir Informacijos rinkmenų sąrašo saugos politiką įgyvendinančių dokumentų patvirtinimo“ pakeitimo