LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTRAS

ĮSAKYMAS DĖL KAI KURIŲ LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLIŲ, NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ IR VEIKLOS TĘSTINUMO VALDYMO PLANO PATVIRTINIMO

2018-11-26 Nr. 1V-871
Vilnius

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“, 8 ir 12 punktais, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, 5 ir 7 punktais:

1. T v i r t i n u pridedamus:

1.1. Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų saugaus elektroninės informacijos tvarkymo taisykles;

1.2. Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų naudotojų administravimo taisykles;

1.3. Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo planą.

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

2.1. Lietuvos Respublikos vidaus reikalų ministro 2007 m. gruodžio 27 d. įsakymą Nr. 1V-449 „Dėl Vidaus reikalų informacinės sistemos veikos tęstinumo valdymo plano ir Vidaus reikalų informacinės sistemos duomenų saugaus tvarkymo taisyklių patvirtinimo“ (su visais pakeitimais ir papildymais);

2.2. Lietuvos Respublikos vidaus reikalų ministro 2007 m. gruodžio 29 d. įsakymą Nr. 1V-454 „Dėl Lietuvos nacionalinės Šengeno informacinės sistemos veiklos tęstinumo valdymo plano ir

Lietuvos nacionalinės Šengeno informacinės sistemos duomenų saugaus tvarkymo taisyklių patvirtinimo“;

2.3. Lietuvos Respublikos vidaus reikalų ministro 2008 m. vasario 1 d. įsakymą Nr. 1V-46 „Dėl Lietuvos nacionalinės Šengeno informacinės sistemos naudotojų administravimo taisyklių patvirtinimo“;

2.4. Lietuvos Respublikos vidaus reikalų ministro 2008 m. gegužės 6 d. įsakymą Nr. 1V-165 „Dėl Vidaus reikalų informacinės sistemos centrinio duomenų banko naudotojų administravimo taisyklių patvirtinimo“ (su visais pakeitimais ir papildymais);

2.5. Lietuvos Respublikos vidaus reikalų ministro 2016 m. vasario 1 d. įsakymą Nr. 1V-73 „Dėl Integruotos baudžiamojo proceso informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Integruotos baudžiamojo proceso informacinės sistemos veiklos tęstinumo valdymo plano ir Integruotos baudžiamojo proceso informacinės sistemos naudotojų administravimo taisyklių patvirtinimo“;

2.6. Lietuvos Respublikos vidaus reikalų ministro 2016 m. gegužės 10 d. įsakymą Nr. 1V-351 „Dėl Administracinių teisės pažeidimų registro saugaus elektroninės informacijos tvarkymo taisyklių, Administracinių teisės pažeidimų registro naudotojų administravimo taisyklių ir Administracinių teisės pažeidimų registro veiklos tęstinumo valdymo plano patvirtinimo“;

2.7. Lietuvos Respublikos vidaus reikalų ministro 2016 m. gegužės 26 d. įsakymą Nr. 1V-389 „Dėl Lietuvos nacionalinės vizų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, naudotojų administravimo taisyklių ir veiklos tęstinumo valdymo plano patvirtinimo“ (su visais pakeitimais ir papildymais);

2.8. Lietuvos Respublikos vidaus reikalų ministro 2017 m. kovo 24 d. įsakymą Nr. 1V-215 „Dėl Sertifikatų valdymo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Sertifikatų valdymo informacinės sistemos veiklos tęstinumo valdymo plano ir Sertifikatų valdymo informacinės sistemos naudotojų administravimo taisyklių patvirtinimo“.

Vidaus reikalų ministras Eimutis Misiūnas

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2018 m. spalio 17 d. raštu Nr. (4.2)6K-656

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų
ministro 2018 m. lapkričio 26 d.
įsakymu Nr. 1V-871

KAI KURIŲ LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Informacijos tvarkymo taisyklės) nustato tvarką, užtikrinančią saugų Lietuvos Respublikos vidaus reikalų ministerijos valdomų bei Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) tvarkomų registrų ir valstybės informacinių sistemų (toliau – informacinės sistemos), nurodytų Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2017 m. gruodžio 22 d. įsakymu Nr. 1V-883 „Dėl Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų patvirtinimo“ (toliau – Saugos nuostatai) priede, elektroninės informacijos tvarkymą ir informacinių sistemų kibernetinio saugumo politikos įgyvendinimą.

2. Informacijos tvarkymo taisyklėse vartojamos sąvokos:

2.1. **Nuotolinis prisijungimas** – tai toks prisijungimo prie informacinės sistemos būdas, kai informacinės sistemos naudotojas jungiasi prie informacinės sistemos iš kompiuterizuotos darbo vietos, esančios už Vidaus reikalų telekomunikacinio tinklo ribų;

2.2. **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.);

2.3. **Privilegijuotas naudotojas** – asmuo (informacinės sistemos naudotojas, administratorius, programuotojas, paslaugų teikėjo darbuotojas ir kt.), kuriam vidaus reikalų ministro tvirtinamų naudotojų administravimo taisyklių nustatyta tvarka suteikta privilegijuota prieiga;

2.4. **Tiesioginis prisijungimas** – tai toks prisijungimo prie informacinės sistemos būdas, kai informacinės sistemos naudotojas jungiasi prie informacinės sistemos iš kompiuterizuotos darbo vietos, esančios Vidaus reikalų telekomunikaciniame tinkle;

2.5. Kitos Informacijos tvarkymo taisyklėse vartojamos sąvokos atitinka sąvokas, apibrėžtas 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“ ir 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“.

3. Informacinėse sistemose tvarkoma elektroninė informacija nurodyta šių informacinių sistemų nuostatuose, elektroninės informacijos svarbos kategorijos nurodytos Saugos nuostatų priede.

4. Už informacinių sistemų elektroninės informacijos tvarkymą atsakingi Informatikos ir ryšių departamento, kitų informacinių sistemų nuostatuose nustatytų informacinių sistemų tvarkytojų valstybės tarnautojai ar darbuotojai, dirbantys pagal darbo sutartį, kuriems vidaus reikalų ministro tvirtinamų naudotojų administravimo taisyklių nustatyta tvarka suteikta informacinių sistemų duomenų tvarkymo teisė.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

5. Kompiuterinės įrangos saugos priemonės:

5.1. 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;

5.2. tarnybinės stotys apsaugomos nuo elektros srovės nutrūkimo ir svyravimų naudojant rezervinius elektros įvadus, vietinius elektros generatorius, nenutrūkstamo maitinimo šaltinius (UPS) svarbiausiai kompiuterinei įrangai, užtikrinančius šios įrangos veikimą ne mažiau kaip 30 min.;

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

5.4. techninės įrangos įnešimas ir išnešimas iš informacinių sistemų tvarkytojų patalpų turi būti kontroliuojamas:

5.4.1. visa techninė įranga į tarnybinių stočių patalpas įnešama ir išnešama iš jų tik šią įrangą administruojantiems informacinių sistemų komponentų administratoriams leidus;

5.4.2. esant tarnybiniam būtinumui, mobilieji įrenginiai, naudojami prisijungti prie informacinių sistemų, gali būti naudojami ne darbo vietos patalpose; už mobilaus įrenginio fizinę saugą atsakingas mobiliojo įrenginio naudotojas;

5.5. iš stacionarių, nešiojamųjų kompiuterių, mobiliųjų įrenginių ar elektroninės informacijos laikmenų, kurie perduodami remonto, techninės priežiūros paslaugų teikėjui, kitam informacinių sistemų naudotojui arba nurašomi, turi būti neatkuriamai sunaikinta visa nevieša elektroninė informacija;

5.6. kompiuterinių laikmenų ir jose esančios informacijos sunaikinimą atlieka darbuotojai, prižiūrintys kompiuterių techninę įrangą:

5.6.1. kompiuterinėse laikmenose esanti informacija sunaikinama, užtikrinant tokį jose esamos informacijos tinkamą sunaikinimą, kad jos nebūtų galima atkurti standartinėmis ar specialiosiomis duomenų atkūrimo priemonėmis.

5.6.2. į buhalterinę apskaitą įtraukta kompiuterinė įranga nurašoma ir likviduojama, vadovaujantis nustatyta pripažinto nereikalingu arba netinkamu (negalimu) naudoti valstybės turto nurašymo, išardymo ir likvidavimo tvarka;

5.6.3. neveikiančios kompiuterinės laikmenos sunaikinamos fiziškai taip, kad jose esančios informacijos turinio negalima būtų atkurti (pvz., kompaktinio disko plokštelės į ne mažesnius nei 1 kv. cm gabalėlius) arba inicijuojamas perdirbimo paslaugų viešasis pirkimas;

5.6.4. kompiuterinei laikmenai sugedus atliekant informacijos sunaikinimą, laikoma, kad informacija, buvusi laikmenoje, nėra sunaikinta, ir pati laikmena, jei ją ekonomiškai netikslinga taisyti, yra sunaikinama kaip neveikianti laikmena;

5.7. apie tarnybinių stočių, tinklo įrangos gedimus turi būti pranešama ir jie registruojami; jei minėti gedimai yra kibernetiniai incidentai, jie valdomi pagal Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose planą, patvirtintą Lietuvos Respublikos vidaus reikalų ministro 2017 m. rugsėjo 20 d įsakymu Nr. 1V-651 „Dėl Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“;

5.8. informacinių sistemų tvarkytojai atsakingi už tai, kad būtų operatyviai ištestuojami ir įdiegiami informacinių sistemų naudotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; reguliariai, ne rečiau kaip kartą per savaitę, informacinių sistemų tvarkytojai įvertina informaciją apie informacinių sistemų naudotojų darbo vietų kompiuterinei įrangai neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius;

5.9. informacinių sistemų komponentų administratoriai automatizuotu būdu turi būti perspėjami, kai pagrindinėje informacinių sistemų kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja.

6. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

6.1. informacinių sistemų tarnybinių stočių operacinių sistemų ir kitos programinės įrangos operatyviam atnaujinimui yra naudojamos centralizuoto atnaujinimo sistemos;

6.2. programinės įrangos diegimą, konfigūravimą, atnaujinimą ir šalinimą pagal kompetenciją atlieka tarnybinių stočių ir duomenų bazių administratoriai;

6.3. programinė įranga prižiūrima laikantis gamintojo rekomendacijų;

6.4. programinės įrangos testavimas atliekamas naudojant atskirą testavimo aplinką;

6.5. naudojama tik legali, patikrinta, patikimų gamintojų ir informacinių sistemų naudotojų darbo funkcijoms atlikti reikalinga programinė įranga, įtraukta į leistinos programinės įrangos sąrašą, patvirtintą Informatikos ir ryšių departamento direktoriaus ar kito informacinių sistemų tvarkytojo vadovo; pagrindinis saugos įgaliotinis kartu su pagrindiniu administratoriumi arba kito informacinių sistemų tvarkytojo vadovo paskirtas saugos įgaliotinis ne rečiau kaip kartą per metus peržiūri bei prireikus atnaujina leistinos programinės įrangos sąrašą.

7. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

7.1. tarnybinės stotys, kompiuterizuotos darbo vietos ir kita kompiuterinė įranga, įjungta į elektroninės informacijos perdavimo tinklą, yra atskirta nuo viešųjų telekomunikacinių tinklų ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga:

7.1.1. įvykus įvykiui ar veiksmui, galinčiam sukelti elektroninės informacijos saugos incidentą, tai turi būti užfiksuojama audito įrašuose ir automatizuotai kuriamas pranešimas atitinkamam komponentų administratoriui;

7.1.2. sukurtas pranešimas turi būti klasifikuojamas pagal užfiksuotą įvykį;

7.1.3. įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius; naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu Informatikos ir ryšių departamento direktoriaus sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio informacinės sistemos veiklai vertinimas (testavimas);

7.1.4. įsilaužimo aptikimo techninio sprendinio įgyvendinimas, konfigūracija ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo informacinės sistemos

techninės įrangos (kartu nurodant atitinkamas datas (įgyvendinimo, atnaujinimo ir panašiai), atsakingus asmenis, taikymo periodus ir panašiai);

7.2. elektroninės informacijos perdavimo tinklas yra segmentuotas pagal įrenginių atliekamas funkcijas ir turi priskirtus IP adresų intervalus:

7.2.1. paslaugų tarnybinių stočių potinklis, skirtas taikomųjų programų, duomenų bazių tarnybinėms stotims;

7.2.2. kompiuterizuotų darbo vietų ir mobiliųjų įrenginių potinkliai, skirti informacinių sistemų naudotojų, kurie prie informacinių sistemų prisijungia nuotoliniu būdu, kompiuterinėms darbo vietoms, mobiliesiems įrenginiams ir kompiuterinei įrangai;

7.2.3. kompiuterizuotų darbo vietų potinkliai, skirti informacinių sistemų naudotojų, kurie prie informacinių sistemų prisijungia tiesioginiu būdu, kompiuterinėms darbo vietoms ir kompiuterinei įrangai;

7.2.4. informacinių sistemų kūrimo, tobulinimo potinklis, skirtas tarnybinėms stotims, kurios naudojamos kuriant, tobulinant informacines sistemas;

7.2.5. informacinių sistemų testavimo potinklis, skirtas tarnybinėms stotims, kurios naudojamos testuoti sukurtas ar patobulintas informacines sistemas;

7.2.6. administratorių potinklis, skirtas sujungti ir valdyti kitus tinklo segmentus;

7.2.7. elektroninės informacijos perdavimo tinklo aptarnavimo ir saugumo potinklis, skirtas tinklo stebėjimo ir aptarnavimo tarnybinėms stotims;

7.3. prie informacinių sistemų 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);

7.4. informacinėms sistemoms taikomas elektroninės informacijos perdavimo tinklo trijų lygių saugumas – išorė, taikomosios programos, duomenų bazės, kiekvieną iš lygių atskiriant ugniasienėmis;

7.5. jungimasis prie informacinių sistemų iš viešųjų telekomunikacijų tinklų yra griežtai kontroliuojamas ir atliekamas tik per tarpines tarnybines stotis;

7.6. pagrindinių tarnybinių stočių įvykių žurnaluose (angl. *event log*), apsaugotuose nuo neteisėto juose esančių duomenų naudojimo, keitimo, iškraipymo, sunaikinimo, registruojami, nurodant informacinės sistemos naudotojo identifikatorių ir įvykio laiką ir saugomi duomenys apie:

7.6.1. informacinės sistemos įjungimą, išjungimą;

7.6.2. audito funkcijos įjungimą ir išjungimą;

7.6.3. audito įrašų trynimą, kūrimą ar keitimą;

7.6.4. informacinės sistemos ar duomenų perdavimo tinklo parametrų, laiko ir (ar) datos pakeitimą;

7.6.5. sėkmingus ir nesėkmingus bandymus registruotis ir prieiti prie informacinės sistemos elektroninės informacijos;

7.6.6. informacinių sistemų naudotojų ar jų grupių ir administratorių prieigos teisių pakeitimą;

7.6.7. kitus svarbius saugai įvykius;

7.7. duomenis, nurodytus 7.6 papunktyje, ne rečiau nei kartą per savaitę ar įvykus saugos incidentui analizuoja Informatikos ir ryšių departamento Sistemų infrastruktūros administravimo skyrius ir apie analizės rezultatus informuoja Informatikos ir ryšių departamento Sistemų infrastruktūros administravimo skyriaus vedėją; šie duomenys yra prieinami tik informacinių sistemų komponentų administratoriams, kurie yra atsakingi už šių duomenų registravimą ir saugojimą, pagrindiniam saugos įgaliotiniui ir asmenims, įgaliotiems Informatikos ir ryšių departamento direktoriaus;

7.8. priemonės, naudojamos informacinės sistemos sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad registruotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais;

7.9. duomenis, nurodytus 7.8 papunktyje, ne rečiau nei kartą per savaitę ar įvykus saugos incidentui analizuoja Informatikos ir ryšių departamento Telekomunikacijų administravimo skyrius ir apie analizės rezultatus informuoja Informatikos ir ryšių departamento Telekomunikacijų administravimo skyriaus vedėją; šie duomenys yra prieinami tik komponentų administratoriams, kurie yra atsakingi už šių duomenų registravimą ir saugojimą, pagrindiniam saugos įgaliotiniui ir asmenims, įgaliotiems Informatikos ir ryšių departamento direktoriaus;

7.10. informacinių sistemų naudotojų informacinių sistemų duomenų tvarkymo ir peržiūros veiksmai registruojami; už šių veiksmų peržiūrą pagal kompetenciją atsako Informatikos ir ryšių departamento Informacijos apdorojimo ir statistikos skyrius ir Sistemų infrastruktūros administravimo skyrius;

7.11. administratorių ir kitų privilegijuotų naudotojų veiksmai registruojami; už šių veiksmų peržiūrą atsako Informatikos ir ryšių departamento Informacijos saugos skyrius;

7.12. įrašų įvykių žurnaluose laiko žymos turi būti sinchronizuotos ne mažiau kaip vienos sekundės tikslumu; turi būti naudojami mažiausiai 2 laiko sinchronizavimo šaltiniai;

7.13. nustojus fiksuoti duomenis įvykių žurnaluose, apie tai nedelsiant turi būti informuojama Informatikos ir ryšių departamento Informacinių technologijų ir telekomunikacijų pagalbos grupė (toliau – ITT pagalbos grupė) ir pagrindinis saugos įgaliotinis;

7.14. duomenys įvykių žurnaluose turi būti apsaugoti nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo. Duomenys įvykių žurnaluose saugomi:

7.14.1. nurodyti 7.6 papunktyje – ne trumpiau kaip 6 mėn.;

7.14.2. nurodyti 7.10 papunktyje – ne trumpiau kaip 1 metus ir ne ilgiau, kaip nurodyta atitinkamos informacinės sistemos nuostatuose;

7.14.3. nurodyti 7.11 papunktyje – ne trumpiau kaip 1 metus;

7.15. naudojimasis duomenimis įvykių žurnaluose turi būti kontroliuojamas ir fiksuojamas.

8. Elektroninės informacijos perdavimo tinklai stebimi šia tvarka:

8.1. visi tinklo įrenginiai, turintys paprastojo tinklo stebėjimo ir valdymo protokolo (angl. *Simple Network Management Protocol, SNMP*) parinktį, stebimi tinklo priežiūros sistemos, kuri, kilus nesklandumams, automatiškai praneša apie problemą kompiuterių tinklų administratoriui;

8.2. visi ryšių kanalai stebimi tinklo priežiūros sistemos, kuri, esant sutrikimams arba didelei apkrovai, automatiškai praneša apie problemą kompiuterių tinklų administratoriui.

9. Belaidžio tinklo saugumas ir kontrolė:

9.1. leidžiama naudoti tik su Informatikos ir ryšių departamento direktoriumi ar jo įgaliotu asmeniu suderintus belaidžio tinklo įrenginius (belaidės prieigos taškus), atitinkančius techninius kibernetinio saugumo reikalavimus;

9.2. tikrinami prieigai prie informacinių sistemų naudojami belaidžiai įrenginiai, ITT pagalbos grupei pranešama apie neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius;

9.3. naudojamos priemonės, kurios automatiškai apribotų neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius arba informuotų ITT pagalbos grupę;

9.4. suderinus su Informatikos ir ryšių departamentu, belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, kontroliuojamoje zonoje;

9.5. prisijungiant prie belaidžio tinklo, turi būti taikomas informacinės sistemos naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas;

9.6. belaidėje sąsajoje turi būti išjungtas tinklo stebėsenos ir valdymo protokolas (SNMP);

9.7. turi būti išjungti visi nebūtini valdymo protokolai;

9.8. turi būti išjungti nenaudojami duomenų perdavimo TCP (angl. *Transmission Control Protocol*) / UDP (angl. *User Datagram Protocol*) protokolų naudojami prievadai;

9.9. turi būti išjungtas lygiarangis (angl. *peer to peer*) funkcionalumas, leidžiantis belaidžiais įrenginiais tarpusavyje palaikyti ryšį;

9.10. belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu;

9.11. prieš pradedant naudoti belaidę prieigos stotelę ir šifruoti belaidį ryšį, turi būti pakeisti belaidės prieigos stotelėje standartiniai gamintojo slaptažodžiai ir šifravimo raktai;

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

10. informacinių sistemų tvarkytojų tarnybinių stočių patalpų saugumo užtikrinimas:

10.1. įrengta elektroninė perimetro kontrolės sistema; tarnybinių stočių patalpos turi atskirą elektroninę perimetro kontrolės sistemą;

10.2. įrengta tarnybinių stočių patalpų apsaugos signalizacija, kurios signalai, įvykus gaisrui ar įsilaužimui (bandymui įsilaužti) automatizuotu būdu perduodami už patalpų apsaugą atsakingiems asmenims;

10.3. patalpos turi atitikti priešgaisrinės saugos reikalavimus, turi būti gaisro gesinimo priemonės, atliekama gaisro gesinimo priemonių patikra;

10.4. patalpos, kuriose yra tarnybinės stotys, turi būti atskirtos nuo bendro naudojimo patalpų.

11. Informatikos ir ryšių departamento informacinių sistemų tarnybinių stočių patalpose:

11.1. sienos sumūrytos iš plytų ar blokelių, pagamintos iš gelžbetonio, lubos pagamintos iš gelžbetonio;

11.2. durys atsparios laužimui, nedegios, su užraktais;

11.3. į tarnybinių stočių patalpas gali patekti tik Informatikos ir ryšių departamento direktoriaus patvirtintame sąraše išvardinti darbuotojai; valymas, elektros tinklo priežiūra, patalpų remonto ir kiti darbai atliekami tik dalyvaujant darbuotojui, turinčiam leidimą patekti į tarnybinių stočių patalpas;

11.4. tarnybinių stočių patalpos turi alternatyvų elektros energijos tiekimo šaltinį;

11.5. tarnybinių stočių patalpose įrengta gaisro gesinimo dujomis sistema;

11.6. tarnybinių stočių patalpose įrengta oro kondicionavimo, temperatūros ir drėgmės kontrolės įranga;

11.7. tarnybinių stočių patalpų raktai ir atsarginiai raktai saugomi atskirose patalpose.

12. Nešiojamųjų kompiuterių, naudojamų prisijungimui prie informacinių sistemų, naudojimo tvarka:

12.1. prisijungimui prie informacinių sistemų leidžiama naudoti tik tarnybinius nešiojamuosius kompiuterius;

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

12.3. nešiojamąjį kompiuterį naudojant ne darbo vietos patalpoje, patalpa, kurioje jis paliekamas, turi būti užrakinama net ir trumpam jį paliekant; nešiojamąjį kompiuterį paliekant ilgesniam laikui, jis turi būti išjungiamas;

12.4. prie nešiojamųjų kompiuterių draudžiama prijungti kokius nors kitus informacinėms sistemoms nepriklausančius įrenginius, išskyrus nurodytus 12.5 papunktyje;

12.5. prie nešiojamojo kompiuterio gali būti jungiami tik informacinių sistemų naudotojų tarnybinėms funkcijoms atlikti reikalingi įrenginiai, įtraukti į leistinų jungti įrenginių sąrašą, patvirtintą Informatikos ir ryšių departamento direktoriaus arba kito informacinių sistemų tvarkytojo vadovo; pagrindinio administratoriaus parengtas ir Informatikos ir ryšių departamento direktoriaus patvirtintas leistinų jungti įrenginių sąrašas ne rečiau kaip kartą per metus peržiūrimas bei prireikus atnaujinamas;

12.6. turi būti parengti nešiojamųjų kompiuterių operacinių sistemų atvaizdai su saugumo nuostatomis; atvaizde turi būti nustatyti tik veiklai būtini operacinių sistemų komponentai (administravimo paskyros, paslaugos (angl. *Services*), taikomosios programos, tinklo prievadai, atnaujinimai, sisteminės priemonės); atvaizdai turi būti reguliariai peržiūrimi ir atnaujinami, nedelsiant atnaujinami nustačius naujų pažeidžiamumų ar atakų;

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

12.8. nešiojamuosiuose kompiuteriuose turi būti naudojamos vykdomojo kodo (angl. *Executable code*) kontrolės priemonės, automatiškai apribojančios neleistino vykdomojo kodo naudojimą ar informacinių sistemų komponentų administratorius informuojančios apie neleistino vykdomojo kodo naudojimą;

12.9. nešiojamieji kompiuteriai, kuriais naršoma internete, privalo būti apsaugoti nuo judriųjų programų (angl. *Mobile code*) keliamų grėsmių;

12.10. duomenys, perduodami belaidžiu ryšiu tarp nešiojamojo kompiuterio ir informacinės sistemos, turi būti šifruojami taikant VPN technologiją;

12.11. jungiantis prie informacinių sistemų išteklių, turi būti patvirtinamas tapatumas; nešiojamame kompiuteryje ar jo taikomojoje programinėje įrangoje turi būti uždrausta automatiškai išsaugoti slaptažodį;

12.12. nešiojamasis kompiuteris, kuriuo nesinaudojama 15 minučių, turi automatiškai užsirakinti;

12.13. kitos nešiojamųjų kompiuterių apsaugai užtikrinti naudojamos priemonės numatytos Saugos nuostatų 51 punkte.

13. Mobiliųjų įrenginių (išmaniųjų telefonų ir planšetinių kompiuterių, naudojančių Android ar iOS operacines sistemas), naudojamų prisijungti prie informacinių sistemų, saugumas ir kontrolė:

13.1. leidžiama naudoti tik tarnybinius, tinkamai sukonfigūruotus, su įdiegtomis saugos priemonėmis ir įdiegta tarnybinėms funkcijoms atlikti reikalinga programine įranga mobiliuosius įrenginius:

13.1.1. mobiliuosiuose įrenginiuose turi būti įdiegta centralizuoto mobiliųjų įrenginių administravimo programinė įranga;

13.1.2. mobilieji įrenginiai turi būti apsaugoti saugiais slaptažodžiais;

13.1.3. mobiliajame įrenginyje nesant nustatyto slaptažodžio, draudžiama jame saugoti jautrius ir neužšifruotus duomenis; šiuo atveju duomenys turi būti laikomi laikmenose atskirai nuo mobiliojo įrenginio;

13.1.4. esant galimybei, mobilusis įrenginys užrakinamas naudojant PIN kodą, atrakinimo piešinį, slaptažodį ar biometrinius duomenis;

13.2. išnešti iš patalpų mobilieji įrenginiai negali būti palikti be priežiūros; jei įmanoma, informacinių sistemų naudotojas turi laikyti mobilųjį įrenginį prie savęs visą laiką, ypač viešosiose vietose;

13.3. mobilųjį įrenginį naudojant ne darbo vietos patalpoje, patalpa, kurioje jis paliekamas, turi būti užrakinama net ir trumpam jį paliekant; mobilųjį įrenginį paliekant ilgesniam laikui, jis turi būti išjungiamas;

13.4. turi būti tikrinami prieigai prie informacinių sistemų naudojami mobilieji įrenginiai, komponentų administratoriams pranešama apie neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius;

13.5. turi būti naudojamos priemonės, kurios automatiškai apribotų neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius ar kompiuterių tinklų administratorių informuotų apie neleistinos mobiliosios įrangos prijungimą prie informacinės sistemos;

13.6. mobiliuosiuose įrenginiuose privalo būti naudojamos centralizuotai valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, užkardymo ir stebėjimo realiuoju laiku priemonės;

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

13.8. mobiliuosiuose įrenginiuose turi būti naudojamos vykdomojo kodo (angl. *Executable code*) kontrolės priemonės, automatiškai apribojančios neleistino vykdomojo kodo naudojimą ar komponentų administratorius informuojančios apie neleistino vykdomojo kodo naudojimą;

13.9. mobilieji įrenginiai, kuriais naršoma internete, privalo būti apsaugoti nuo judriųjų programų (angl. *Mobile code*) keliamų grėsmių;

13.10. prie mobiliųjų įrenginių draudžiama prijungti kokius nors kitus informacinėms sistemoms nepriklausančius įrenginius, išskyrus nurodytus 13.11 papunktyje;

13.11. prie mobiliųjų įrenginių gali būti jungiami tik informacinių sistemų naudotojų tarnybinėms funkcijoms atlikti reikalingi įrenginiai, įtraukti į leistinų jungti įrenginių sąrašą, patvirtintą Informatikos ir ryšių departamento direktoriaus arba kito informacinių sistemų tvarkytojo vadovo; pagrindinio administratoriaus parengtas ir Informatikos ir ryšių departamento direktoriaus patvirtintas leistinų jungti įrenginių sąrašas ne rečiau kaip kartą per metus peržiūrimas bei prireikus atnaujinamas;

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

13.13. jungiantis prie informacinių sistemų išteklių, turi būti patvirtinamas tapatumas; mobiliajame įrenginyje ar jo taikomojoje programinėje įrangoje turi būti uždrausta automatiškai išsaugoti slaptažodį;

13.14. mobilusis įrenginys, kuriuo nesinaudojama 15 minučių, turi automatiškai užsirakinti;

13.15. mobiliuosiuose įrenginiuose privalo būti įdiegtos priemonės, leisiančios nuotoliniu būdu neatkuriamai ištrinti duomenis;

13.16. turi būti užtikrinta kompiuterinių laikmenų apsauga;

13.17. turi būti šifruojami duomenys tiek mobiliųjų įrenginių laikmenose, tiek išorinėse kompiuterinėse laikmenose.

14. Informacinių sistemų naudojamų svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė:

14.1. atpažinties, tapatumo patvirtinimo ir naudojimosi kontrolės reikalavimai:

14.1.1. draudžiama slaptažodžius saugoti programiniame kode;

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

14.2. turi būti įgyvendinti svetainės kriptografijos reikalavimai:

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

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

14.2.3. turi būti naudojamas TLS (angl. *Transport Layer Security*) standartas, užtikrinantis informacinės sistemos naudotojo ir tarnybinės stoties abipusį tapatumo nustatymą, kad būtų užtikrintas šifruotas ryšys;

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

14.2.5. šifravimui naudojamų raktų poros turi būti generuojamos naudojant algoritmus, atitinkančius kvalifikuoto elektroninio parašo reikalavimus;

14.2.6. generuojamų raktų ilgiai turi būti tinkami kvalifikuotam elektroniniam parašui;

14.2.7. privatieji kriptografiniai raktai ar jų kopijos, saugomi ar laikomi ne kriptografiniame saugumo modulyje, turi būti šifruojami;

14.3. tarnybinės stoties, kurioje yra svetainė, svetainės saugos parametrai turi būti teigiamai įvertinti naudojant Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos rekomenduojamą testavimo priemonę;

14.4. draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai;

14.5. turi būti naudojama svetainės ugniasienė (angl. *Web Application Firewall*); įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius; naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu Informatikos ir ryšių departamento direktoriaus ar jo įgalioto asmens sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio informacinės sistemos veiklai vertinimas (testavimas);

14.6. turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), įterptinių instrukcijų atakų (angl. *Cross-site scripting, XSS*), atkirtimo nuo paslaugos (angl. *Denial of Service, DOS*), paskirstyto atsisakymo aptarnauti (angl. *Distributed Denial of Service, DDOS*) ir kitų, priemonės; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project, OWASP*) interneto svetainėje www.owasp.org;

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

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

14.9. svetainės saugumo priemonės turi gebėti automatiškai uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir panašiai);

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

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

14.12. turi būti įdiegta svetainės turinio nesankcionuoto pakeitimo (angl. *Defacement*) stebėsenos sistema;

14.13. turi būti atliekama pažeidžiamumų paieška, ne rečiau kaip kartą per mėnesį tikrinant svetainės saugumą su skenavimo programine įranga.

15. Siekiant užkirsti kelią jautrių duomenų paviešinimui, turėtų būti naudojamos šifravimo priemonės:

15.1. turi būti šifruojami atskiri failai, katalogai ar visos duomenų laikmenos, jei įrenginys su jautriais duomenimis išnešamas už informacinės sistemos tvarkytojo įstaigos ribų;

15.2. šifravimas turi būti atliktas taip, kad tik šifravimo raktą turintis asmuo galėtų perskaityti ir naudoti duomenis;

15.3. turi būti pasirinktas saugus duomenų šifravimo algoritmas; pastangos, reikalingos įveikti algoritmą, turėtų būti didesnės nei atskleistos informacijos vertė;

15.4. turi būti pasirinktas tinkamas šifro raktas; esant galimybei, jis turi būti sugeneruotas atsitiktinai; šifravimo raktą parinkus kaip slaptažodį, jam turi būti taikomi vidaus reikalų ministro tvirtinamose naudotojų administravimo taisyklėse nustatyti administratorių slaptažodžių naudojimo reikalavimai;

15.5. šifravimo algoritmas (programa), užšifruotas tekstas ir šifro raktai negali būti saugomi toje pačioje vietoje; šifro raktai turi būti laikomi atskirai;

15.6. kitos saugumo priemonės, susijusios su perduodamų duomenų šifravimu, nurodytos Informacijos tvarkymo taisyklių 9.10, 9.11, 13.1.3, 13.12, 14.2.1–14.2.3, 14.2.5, 14.2.7 papunkčiuose.

16. Kitos priemonės, naudojamos užtikrinti informacinių sistemų elektroninės informacijos saugą:

16.1. baigus darbą su informacine sistema, būtina užtikrinti, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungti nuo informacinės sistemos, atjungti saugią sertifikato laikmeną nuo kompiuterinės įrangos, uždaryti programinę įrangą, įjungti ekrano užsklandą su slaptažodžiu, dokumentus padėti į pašaliniams asmenims neprieinamą vietą;

16.2. informacinių sistemų naudotojui neatliekant jokių veiksmų 15 min., visos kompiuterizuotos darbo vietos ir tarnybinės stotys automatiškai užsirakina ir naudotis informacine sistema galima tik pakartojus naudotojo tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

16.3. turi būti įgyvendintos Lietuvos standarte LST EN ISO/IEC 27002 nurodytos saugos priemonės, išskyrus priemones, kurios netaikytinos dėl institucijos veiklos, informacinės sistemos ar naudojamos informacinėje sistemoje techninės įrangos pobūdžio, ir Lietuvos standarte LST EN ISO/IEC 27001 nurodyti reikalavimai informacijos saugumo valdymo sistemai.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

17. Informacinių sistemų elektroninės informacijos įvedimo, keitimo, atnaujinimo ir naikinimo tvarka:

17.1. informacinėse sistemose tvarkomus duomenis įrašyti, keisti, atnaujinti gali tik informacinių sistemų naudotojas pagal suteiktas prieigos prie informacinių sistemų teises;

17.2. informacinių sistemų elektroninė informacija įrašoma, atnaujinama, keičiama ir naikinama vadovaujantis informacinių sistemų nuostatais, Saugos nuostatais ir kitais teisės aktais, reglamentuojančiais informacinių sistemų elektroninės informacijos tvarkymą;

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

17.4. informacinių sistemų naudotojų duomenis įrašyti, keisti, atnaujinti gali tik naudotojų administratorius.

18. Atsarginės elektroninės informacijos kopijos daromos, saugomos, elektroninė informacija atkuriama iš atsarginių kopijų vadovaujantis Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos administruojamų informacinių sistemų ir registrų elektroninės informacijos atsarginių kopijų darymo, saugojimo ir atkūrimo tvarkos aprašu, patvirtintu Informatikos ir ryšių departamento direktoriaus 2017 m. sausio 9 d. įsakymu Nr. 5V-6 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos administruojamų informacinių sistemų ir registrų elektroninės informacijos atsarginių kopijų darymo, saugojimo ir atkūrimo tvarkos aprašo patvirtinimo“.

19. Informacinių sistemų elektroninė informacija kitiems registrams ir informacinėms sistemoms teikiama ir gaunama iš jų tik pasirašius duomenų teikimo sutartis, laikantis šių reikalavimų:

19.1. Informacinių sistemų elektroninė informacija kitiems registrams ir informacinėms sistemoms perduodama vadovaujantis informacinių sistemų nuostatais ir kitais duomenų saugą užtikrinančiais ir reglamentuojančiais teisės aktais;

19.2. duomenų teikėjai informacinėms sistemoms elektroninę informaciją turi teikti teisės aktų nustatytais būdais, apimtimi, reguliarumu ir terminais;

19.3. visi faktai apie apsikeitimus duomenimis fiksuojami ir laikomi elektroninėje duomenų bazėje.

20. Neteisėto duomenų kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) nustatymo tvarka:

20.1. informacinių sistemų naudotojai, pastebėję saugos dokumentų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų

saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai ITT pagalbos grupei telefonu 57777, elektroniniu paštu ittpagalba@vrm.lt arba interneto naršyklės adresu https://ittpagalba.vrm.lt. ITT pagalbos grupė pranešimą nedelsdama perduoda atitinkamų informacinių sistemų administratoriams ir saugos įgaliotiniams;

20.2. informacinių sistemų administratoriai apie saugos pažeidimus informuoja informacinių sistemų pagrindinį saugos įgaliotinį ir imasi visų įmanomų prevencinių veiksmų, susijusių su neteisėtu duomenų naudojimu Kibernetinių incidentų valdymo Vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano nustatyta tvarka.

21. Informacinių sistemų programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

21.1. techninės, programinės ir sisteminės įrangos naujinimui taikoma pokyčių valdymo tvarka, nustatyta Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir informacinių sistemų pokyčių valdymo tvarkos apraše, patvirtintame Lietuvos Respublikos vidaus reikalų ministro 2017 m. lapkričio 10 d. įsakymu Nr. 1V-773 „Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir informacinių sistemų pokyčių valdymo tvarkos aprašo patvirtinimo“;

21.2. informacinių sistemų programinės ir techninės įrangos keitimo ir atnaujinimo tvarką su trečia šalimi, kuriai Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos informacinės sistemos ir (ar) jos infrastuktūros priežiūros funkcijos (toliau – paslaugų teikėjas), priklausomai nuo konkretaus atvejo, derina informacinių sistemų pagrindinis administratorius arba ji aprašoma paslaugų, susijusių su informacinių sistemų programinės ir techninės įrangos keitimu ir atnaujinimu, teikimo sutartyse.

22. Informacinių sistemų pokyčių valdymo tvarka nustatyta Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir informacinių sistemų pokyčių valdymo tvarkos apraše.

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

23. Sutartis su paslaugų teikėjais administruojantys darbuotojai (toliau – sutarčių kuratoriai) organizuoja paslaugų teikėjų prieigos prie programinių, techninių ir kitų informacinių sistemų išteklių suteikimą, teikia šios prieigos poreikius komponentų administratoriams. Komponentų administratoriai pagal kompetenciją atsako už tinkamą ir saugų prieigos prie programinių, techninių ir kitų informacinių sistemų išteklių suteikimą ir panaikinimą paslaugos teikėjui.

24. Atitinkamas komponentų administratorius suteikia paslaugos teikėjui tik tokią prieigą prie informacinių sistemų išteklių, kuri yra būtina norint atlikti arba vykdyti sutartyje nustatytus įsipareigojimus, kurie neprieštarauja įstatymų ir kitų teisės aktų reikalavimams.

25. Sutarčių kuratoriai privalo pasirašytinai supažindinti paslaugos teikėjų darbuotojus su Saugos nuostatais ir kitų saugos dokumentų nuostatomis, susijusiomis su teikiamomis paslaugomis.

Sutarčių kuratoriai privalo prižiūrėti, kaip paslaugos teikėjų darbuotojai laikosi Saugos nuostatų ir kitų nustatytų saugos reikalavimų.

26. Pasibaigus sutarties su paslaugos teikėju galiojimo terminui, paslaugos teikėjui baigus pagal sutartį numatytus darbus, paslaugų teikėjo darbuotojams nutraukus darbo santykius ar atitinkamų funkcijų, kurioms buvo būtina prieiga, vykdymą arba atsiradus kitoms sutartyje ar informacinių sistemų saugos dokumentuose įvardintoms sąlygoms, komponentų administratoriai nedelsdami privalo panaikinti suteiktą prieigą.

27. Reikalavimai, keliami patalpoms, įrangai, informacinių sistemų priežiūrai, duomenų perdavimui tinklais ir kitoms paslaugoms, turi būti ne žemesni nei Informacijos tvarkymo taisyklių II skyriuje nustatyti atitinkami reikalavimai.

_____

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų
ministro 2018 m. d.
įsakymu Nr.

KAI KURIŲ LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų naudotojų administravimo taisyklės (toliau – Naudotojų administravimo taisyklės) reglamentuoja Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Vidaus reikalų ministerija) valdomų bei Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) tvarkomų registrų ir valstybės informacinių sistemų (toliau – informacinės sistemos), nurodytų Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2017 m. gruodžio 22 d. įsakymu Nr. 1V- 883 „Dėl Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų patvirtinimo“ (toliau – Saugos nuostatai) priede, naudotojų ir Informatikos ir ryšių departamento paskirtų administratorių (toliau – administratoriai) įgaliojimus, teises, pareigas, informacinių sistemų naudotojų administravimo principus ir tvarką, jų veiksmų kontrolę.

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 tvarkant informacines sistemas, nurodytas Saugos nuostatų priede.

4. Naudotojų administravimo taisyklės taikomos visiems informacinių sistemų naudotojams, įskaitant privilegijuotus naudotojus.

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

6. Kiekvienas informacinių sistemų 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.

II SKYRIUS
NAUDOTOJŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

7. Sprendimus dėl teisės suteikimo informacinių sistemų tvarkytojui administruoti savo bei jam pavaldžių įstaigų informacinių sistemų naudotojus, atsižvelgiant į Saugos nuostatų 16.4 papunktį, priima Informatikos ir ryšių departamentas per 5 darbo dienas nuo informacinių sistemų tvarkytojo prašymo suteikti tokias teises gavimo.

8. Informacinių sistemų naudotojų registravimą vykdo Informatikos ir ryšių departamentas, išskyrus atvejus, kai šią teisę jis suteikė informacinių sistemų tvarkytojui.

9. Informacinių sistemų naudotojai privalo tvarkyti elektroninę informaciją, vadovaudamiesi informacinių sistemų elektroninės informacijos tvarkymą reglamentuojančiais teisės aktais ir duomenų teikimo sutartimis.

10. Informacinių sistemų naudotojai privalo saugoti tvarkomų 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), Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo, Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo

už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo nustatyta tvarka.

11. Informacinių sistemų naudotojas turi tik tas prieigos prie informacinių sistemų teises, kurios jam suteiktos Naudotojų administravimo taisyklių III skyriuje nustatyta tvarka:

11.1. esant poreikiui tam pačiam asmeniui vykdyti funkcijas, susijusias su veiksmais, galinčiais sukelti didesnę nei įprastą riziką informacinei sistemai, 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;

11.2. nereikalingos ar nenaudojamos informacinių sistemų naudotojų paskyros turi būti blokuojamos nedelsiant ir ištrinamos praėjus duomenų nustatytam saugojimo terminui.

12. Informacinių sistemų naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai komponentų administratoriams, saugos įgaliotiniams arba Informatikos ir ryšių departamento Informacinių technologijų ir telekomunikacijų pagalbos grupei (toliau – ITT pagalbos grupė) telefonu Nr. (8 5) 271 7777 arba elektroniniu paštu ittpagalba@vrm.lt ar registruodami pranešimą interneto naršyklės adresu https://ittpagalba.vrm.lt arba savo institucijos pagalbos tarnybai, jei ji įsteigta.

13. Administratorių prieigos prie informacinių sistemų lygiai:

13.1. Informatikos ir ryšių departamento paskirtas naudotojų administratorius administruoja visų informacinių sistemų naudotojų prieigos teises prie informacinių sistemų, išskyrus informacinių sistemų tvarkytojų paskirtų naudotojų administratorių administruojamus informacinių sistemų naudotojus;

13.2. kitų Informatikos ir ryšių departamento paskirtų administratorių funkcijos ir prieigos prie informacinių sistemų lygiai įvardyti Saugos nuostatuose, pareigybių aprašymuose;

13.3. Informacinių sistemų tvarkytojų paskirti naudotojų administratoriai administruoja informacinių sistemų naudotojus informacinių sistemų tvarkytojo ir jam pavaldžiose įstaigose.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO NAUDOTOJAMS KONTROLĖS TVARKA

14. Informacinių sistemų naudotojų, kuriuos administruoja Informatikos ir ryšių departamentas, įregistravimo tvarka:

14.1. dėl informacinių sistemų naudotojų prieigos (įskaitant privilegijuotą) prie informacinių sistemų suteikimo teikiamas prašymas įregistruoti registro, informacinės sistemos naudotoją ir suteikti

ar panaikinti naudotojo prieigos prie registro, informacinės sistemos teises, kurio forma nustatyta Naudotojų administravimo taisyklių 1 priede (toliau – prašymas), ir pasižadėjimas laikytis Vidaus reikalų ministerijos valdomų registrų ir (ar) valstybės informacinių sistemų elektroninės informacijos saugos reikalavimų, kurio forma nustatyta Naudotojų administravimo taisyklių 2 priede (toliau – pasižadėjimas); prašymas ir pasižadėjimas teikiami Informatikos ir ryšių departamentui raštu arba pasirašyti saugiu elektroniniu parašu elektroninių ryšių priemonėmis ir perduodami naudotojų administratoriui (išskyrus Naudotojų administravimo taisyklių 14.2 papunktyje nustatytus atvejus); pasižadėjimą asmuo pildo tik pirmą kartą teikiant prašymą, išskyrus atvejus, kai prieigos teisės informacinių sistemų naudotojui dėl pažeidimų buvo sustabdytos ar laikinai panaikintos;

14.2. jei teikiamas prašymas suteikti prieigą (įskaitant privilegijuotą) Informatikos ir ryšių departamento valstybės tarnautojui ar darbuotojui, jį pasirašo šio valstybės tarnautojo ar darbuotojo tiesioginis vadovas; jei teikiamas prašymas suteikti privilegijuotą prieigą paslaugų teikėjo darbuotojui, jį pasirašo paslaugų teikėjo vadovas ir vizuoja sutartį su šiuo paslaugų teikėju administruojantis valstybės tarnautojas ar darbuotojas; šiais atvejais prašymas suteikti prieigą (įskaitant privilegijuotą) kartu su pasižadėjimu teikiami Informatikos ir ryšių departamento direktoriui ar jo įgaliotam asmeniui; paslaugų teikėjo darbuotojui prieiga suteikiama tik jam pasirašius pasižadėjimą ir konfidencialumo pasižadėjimą;

14.3. jei naudotojų administratorius ar Naudotojų administravimo taisyklių 14.2 papunktyje nurodytu atveju Informatikos ir ryšių departamento direktorius ar jo įgaliotas asmuo, išnagrinėjęs prašymą, nustato, kad prašyme nurodyti duomenys yra neteisingi, netikslūs ar kad prašyme nurodyta prieigos prie informacinių sistemų teisių apimtis nėra būtina numatytų valstybės tarnautojo ar darbuotojo funkcijų vykdymui, arba kad prašomos tokios prieigos prie informacinių sistemų teisės, kurių įgyvendinimas gali daryti neigiamą įtaką informacinių sistemų, Vidaus reikalų telekomunikacinio tinklo veikimui ar informacinių sistemų duomenų saugai, per 5 darbo dienas nuo prašymo gavimo priima sprendimą prašymo netenkinti ir apie tai raštu informuoja prašymą pateikusį subjektą, nurodydamas atsisakymo registruoti informacinių sistemų naudotoju motyvus;

14.4. jei naudotojų administratorius ar Naudotojų administravimo taisyklių 14.2 papunktyje nurodytu atveju Informatikos ir ryšių departamento direktorius ar jo įgaliotas asmuo patenkina prašymą, naudotojų administratorius informacinės sistemos naudotojui suteikia informacinių sistemų naudotojo prisijungimo vardą ir laikiną slaptažodį ir registruoja jį informacinių sistemų naudotojų administravimo posistemėje; naudotojų administratorius šiuos informacinių sistemų naudotojų prisijungimo duomenis perduoda asmeniškai arba išsiunčia tarnybiniu el. paštu informacinių sistemų naudotojui ne vėliau kaip per 5 darbo dienas nuo prašymo gavimo; informacinių sistemų naudotojas laikomas įregistruotu, kai jam suteikiamas unikalus identifikavimo kodas ir jo duomenys įrašomi į informacinių sistemų naudotojų administravimo posistemę;

14.5. kiekvienas informacinių sistemų naudotojas, jungdamasis prie informacinės sistemos, privalo atlikti tapatumo nustatymo procedūrą, t. y. nurodyti jam suteiktą informacinių sistemų naudotojo prisijungimo vardą ir slaptažodį arba jungtis su kvalifikuotu skaitmeniniu sertifikatu, jei tokį prisijungimo būdą palaiko informacinė sistema;

14.6. kiekvienam informacinių sistemų naudotojui suteikiamas nesikartojantis prisijungimo vardas;

14.7. kiekvienas informacinių sistemų naudotojas privalo naudoti tik jam suteiktą informacinių sistemų naudotojo prisijungimo vardą; naudoti svetimą informacinių sistemų naudotojo prisijungimo vardą draudžiama;

14.8. informacinių sistemų naudotojų slaptažodžiai, praėjus Naudotojų administravimo taisyklių 17 punkte nustatytiems jų keitimo terminams, ar juos pamiršus, turi būti keičiami.

15. Prieigos prie informacinių sistemų teisių (rolių) sąrašą tvirtina Informatikos ir ryšių departamento direktorius.

16. Informacinės sistemos tvarkytojas, jei jam suteikta tokia teisė Naudotojų administravimo taisyklių 7 punkte nustatyta tvarka, informacinės sistemos naudotojus administruoja vadovaudamasis šio informacinės sistemos tvarkytojo nustatyta ir su Informatikos ir ryšių departamentu suderinta tvarka. Informacinės sistemos tvarkytojo paskirtas naudotojų administratorius negali suteikti privilegijuotos prieigos.

17. Reikalavimai informacinių sistemų naudotojų slaptažodžiams, jų galiojimo trukmei, keitimui ir saugojimui:

17.1. slaptažodis informacinių sistemų naudotojui negali būti perduodamas neužšifruotas ar užšifruojamas nepatikimais algoritmais;

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

17.3. pirmojo prisijungimo prie informacinės sistemos metu iš informacinės sistemos naudotojo turi būti reikalaujama, kad jis pakeistų laikiną slaptažodį;

17.4. kilus įtarimui, kad slaptažodis galėjo būti atskleistas, informacinių sistemų naudotojas turi nedelsdamas slaptažodį pakeisti ir apie tai informuoti ITT pagalbos grupę;

17.5. slaptažodis (tame tarpe ir laikinas slaptažodis) keičiamas naudojantis elektronine paslauga https://icdb.vrm.lt/pass/;

17.6. slaptažodžiai turi būti saugomi naudojant maišos funkcijas;

17.7. informacinių sistemų naudotojas slaptažodį turi įsiminti; draudžiama slaptažodį užsirašyti ar pasakyti kitam asmeniui;

17.8. draudžiama informacinių sistemų techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į Naudotojų administravimo taisyklių 17.10.1–17.10.3 papunkčiuose nustatytus reikalavimus atitinkančius slaptažodžius;

17.9. pirmos kategorijos informacinėse sistemose leistinas didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius turi būti nustatytas ne didesnis kaip 3 kartai, kitose informacinėse sistemose – ne didesnis kaip 5 kartai; slaptažodį iš eilės neteisingai įvedus didžiausią leistiną skaičių, informacinė sistema turi užsirakinti ir, jei informacinė sistema palaiko tokį funkcionalumą, neleisti informacinės sistemos naudotojui identifikuotis ne trumpiau nei 15 minučių; pirmos kategorijos informacinės sistemos atveju, apie tai turi būti automatizuotai informuojama ITT pagalbos grupė, jei informacinė sistema palaiko tokį funkcionalumą;

17.10. reikalavimai informacinių sistemų naudotojų slaptažodžiams:

17.10.1. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;

17.10.2. slaptažodį turi sudaryti bent viena didžioji raidė, bent viena mažoji raidė, bent vienas skaičius ir bent vienas specialus simbolis;

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

17.10.4. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius; informacinių sistemų naudotojų teisės sustabdomos, jei slaptažodis nepakeičiamas laiku;

17.10.5. keičiant slaptažodį, informacinė sistema neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

17.11. papildomi reikalavimai privilegijuotų naudotojų slaptažodžiams:

17.11.1. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

17.11.2. keičiant slaptažodį, informacinės sistemos taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.

18. Informacinių sistemų naudotojų prieigos prie informacinių sistemų sustabdymo atvejai:

18.1. kai informacinių sistemų naudotojas nesinaudoja informacine sistema ar informacinėmis sistemomis ilgiau kaip 2 mėnesius;

18.2. nustačius informacinių sistemų elektroninės informacijos konfidencialumo ar vientisumo pažeidimą arba kitų informacinių sistemų elektroninės informacijos saugą ir tvarkymą reglamentuojančių teisės aktų ar informacinių sistemų duomenų teikimo sutarties nustatytų reikalavimų pažeidimą;

18.3. informacinių sistemų naudotojas nušalinamas nuo darbo (pareigų).

19. Informacinių sistemų naudotojo prieiga prie informacinių sistemų nedelsiant panaikinama:

19.1. jei nustoja vykdyti funkcijas, kurių vykdymui buvo suteiktos prieigos prie informacinių sistemų teisės;

19.2. pasibaigus tarnybos (darbo) santykiams;

19.3. pasibaigus paslaugų teikėjo sutartiniams santykiams.

20. Informacinių sistemų naudotojų paskyrų kontrolė:

20.1. suteikti privilegijuotą prieigą leidžiama tik asmenims, įtrauktiems į Informatikos ir ryšių departamento direktoriaus patvirtintą sąrašą asmenų, kuriems suteikta privilegijuota prieiga prie informacinių sistemų ar jų komponentų (toliau – privilegijuotų naudotojų sąrašas); Informatikos ir ryšių departamento direktoriaus įgaliotas asmuo rengia, tvarko ir periodiškai (ne rečiau kaip kartą per metus) peržiūri privilegijuotų naudotojų sąrašą; privilegijuotų naudotojų sąrašas turi būti nedelsiant patikslintas, kai Naudotojų administravimo taisyklių 18 ir 19 punktuose nustatytais atvejais sąraše nurodytiems asmenims sustabdoma ar panaikinama prieiga prie informacinių sistemų;

20.2. turi būti naudojamos automatizuotos privilegijuotų naudotojų ir kitų naudotojų paskyrų kontrolės priemonės, kurios tikrintų faktines privilegijuotų naudotojų ir kitų naudotojų paskyras ir apie paskyras, suteikiančias privilegijuotą prieigą asmenims, neįtrauktiems į privilegijuotų naudotojų sąrašą, paskyras, faktiškai suteikiančias prieigą asmenims, kuriems prieiga turėjo būti panaikinta šių taisyklių nustatyta tvarka, paskyras, kurios negali būti susietos su konkrečiu asmeniu, paskyras, kurių sukūrimas negali būti pagrįstas turima informacija apie šiose taisyklėse nustatytų prieigos suteikimo procedūrų atlikimą, nedelsdamos praneštų pagrindiniam saugos įgaliotiniui ar kitam Informatikos ir ryšių departamento direktoriaus įgaliotam asmeniui. Su šia informacija supažindinamas Informatikos ir ryšių departamento direktorius.

21. Nuotolinio prisijungimo prie informacinių sistemų suteikimo ir panaikinimo tvarką, technines nuotolinių prisijungimų prie informacinių sistemų sąlygas tvirtina Informatikos ir ryšių departamento direktorius.

22. Nuotolinį prisijungimą prie informacinių sistemų naudojančiam informacinių sistemų naudotojui draudžiama savavališkai diegti technines ir programines priemones į nuotoliniam prisijungimui naudojamą informacinių sistemų įrangą bei daryti kitokius jos pakeitimus.

Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų naudotojų administravimo taisyklių
1 priedas

(Prašymo forma)

_____
(įstaigos pavadinimas)

Informatikos ir ryšių departamentui prie
Lietuvos Respublikos vidaus reikalų ministerijos

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

_____ Nr. _____
(data) (registracijos numeris)

_____
(sudarymo vieta)

Vadovaudamasis _____,
(teisinis pagrindas)
prašau suteikti / panaikinti (pabraukti reikalingą variantą) prieigos prie registro (-ų) ar informacinės sistemos (-ų) teises šiam asmeniui:

_____
(valstybės tarnautojo ar darbuotojo asmens kodas, 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.	Registro, informacinės sistemos pavadinimas	Prieigos teisės (rolės)	
		Suteikti	Panaikinti

PASTABOS:
1. Automatizuotu būdu pildomos prašymo formos vaizdinė išraiška gali skirtis; prašymo formos pavyzdį pildymui automatizuotu būdu su aktualiu registrų ir informacinių sistemų bei prieigos prie jų teisių (rolių) sąrašu skelbia Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos savo tinklapyje;
2. Prašyme nurodomi tik tie registrai ir informacinės sistemos, prie kurių prieigą prašoma suteikti ar panaikinti.

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

Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų naudotojų administravimo taisyklių
2 priedas

(Pasižadėjimo forma)

PASIŽADĖJIMAS
LAIKYTIS VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ REGISTRŲ IR (AR) VALSTYBĖS INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMŲ

_____ Nr. _____
(data) (registracijos numeris)

_____
(sudarymo vieta)

Aš, _____
(pareigos, vardas, pavardė, gimimo data)
_____,

1. Patvirtinu, kad esu susipažinęs (-usi) su Vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais, 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 (Bendruoju duomenų apsaugos reglamentu), Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais atsakomybę bei duomenų saugą.

2. Suprantu, kad:

2.1. dirbdamas, atlikdamas pareigybės aprašyme nustatytas funkcijas, tvarkysiu Vidaus reikalų ministerijos valdomų registrų ir (ar) valstybės informacinių sistemų duomenis ar susipažinsiu su šiais duomenimis, įskaitant asmens duomenis, (toliau – duomenys); šie duomenys visuomenės ir atskirų asmenų interesais gali būti atskleisti ar perduoti tik teisės aktų nustatyta tvarka įgaliotiems asmenims ir institucijoms;

2.2. draudžiama perduoti neįgaliotiems asmenimis įstaigoje ar už jos ribų duomenis, informaciją, dokumentus ir (arba) jų kopijas ar kitaip sudaryti sąlygas susipažinti su minėtais duomenimis, informacija, dokumentais, jų kopijomis;

2.3. netinkamas duomenų tvarkymas užtraukia atsakomybę pagal Lietuvos Respublikos įstatymus;

2.4. asmuo, patyręs žalą dėl mano padarytos neteisėtos veikos, įstatymų nustatyta tvarka turi teisę reikalauti atlyginti jam padarytą turtinę ir neturtinę žalą;

2.5. šis pasižadėjimas galios visą mano darbo laiką šioje įstaigoje, perėjus dirbti į kitas pareigas ir nutraukus ar pasibaigus valstybės tarnybos, darbo ar sutartiniams santykiams.

3. Pasižadu ir įsipareigoju:

3.1. saugoti duomenų ir informacijos paslaptį, jei jie neskirti skelbti viešai; įsipareigojimas saugoti paslaptį galioja ir nutraukus su duomenų, informacijos, dokumentų ir (arba) jų kopijų tvarkymu susijusią veiklą;

3.2. tvarkyti duomenis vadovaudamasis Lietuvos Respublikos įstatymais, Vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų elektroninės informacijos saugą reglamentuojančių teisės aktų nuostatomis ir kitais teisės aktais, taip pat pareigybės aprašymu;

3.3. neatskleisti, neperduoti duomenų, informacijos nė vienam asmeniui, kuris nėra įgaliotas gauti šiuos duomenis ar informaciją teisės aktų nustatyta tvarka;

3.4. pranešti Informatikos ir ryšių departamento ITT pagalbos grupei apie bet kokią įtartiną situaciją, kuri gali kelti grėsmę duomenų saugumui.

_____ _____ _____
(pareigos) (parašas) (vardas, pavardė)

PATVIRTINTA
Lietuvos Respublikos vidaus reikalų
ministro 2018 m. d.
įsakymu Nr.

KAI KURIŲ LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo planas (toliau – Planas) reglamentuoja procedūras, atliekamas siekiant tinkamai valdyti Lietuvos Respublikos vidaus reikalų ministerijos (toliau –Vidaus reikalų ministerija) valdomų bei Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas) tvarkomų registrų ir valstybės informacinių sistemų (toliau – informacinės sistemos), nurodytų Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2017 m. gruodžio 22 d. įsakymu Nr. 1V- 883 „Dėl Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų duomenų saugos nuostatų patvirtinimo“ (toliau – Saugos nuostatai) priede, elektroninės informacijos saugos incidentus (toliau – Incidentas).

2. Plane vartojamos sąvokos atitinka sąvokas, apibrėžtas 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).

3. Informacinių sistemų pagrindinio saugos įgaliotinio, kitų informacinių sistemų saugos įgaliotinių, administratorių ir kitų asmenų, atsakingų už informacinių sistemų veiklos atkūrimą, veiksmai yra nurodyti Vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų veiklos atkūrimo detaliajame plane (1 priedas) (toliau – Informacinių sistemų veiklos atkūrimo detalusis planas).

4. Plano vykdymą, įvykus Incidentui, kurio metu gali kilti pavojus informacinių sistemų elektroninei informacijai, informacinių sistemų techninės, programinės įrangos funkcionavimui, inicijuoja Informatikos ir ryšių departamento direktorius ar jo pavaduotojai. Planas yra privalomas

informacinių sistemų valdytojui, informacinių sistemų tvarkytojams, informacinių sistemų saugos įgaliotiniams, informacinių sistemų administratoriams bei informacinių sistemų naudotojams.

5. Finansinių ir kitokių išteklių, numatomų informacinių sistemų veiklai atkurti, paskelbus Incidentą, šaltinius ir pobūdį numato ir pasirenka informacinių sistemų veiklos tęstinumo valdymo grupė.

6. Informacinių sistemų veikla yra laikoma atkurta tuomet, kai visi informacinių sistemų naudotojai vėl gali atlikti savo darbines funkcijas įprastu būdu.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

7. Informacinių sistemų veiklos tęstinumo valdymo grupė (toliau – Valdymo grupė) užtikrina veiklos tęstinumui kylančių grėsmių valdymą ir informacinių sistemų atkūrimo koordinavimą įvykus Incidentui.

8. Valdymo grupę sudaro:

8.1. Informatikos ir ryšių departamento direktoriaus pavaduotojas, koordinuojantis Informatikos ir ryšių departamento Sistemų infrastruktūros administravimo, Telekomunikacijų administravimo, Informacinių technologijų paslaugų skyrių veiklą (Valdymo grupės vadovas);

8.2. Informatikos ir ryšių departamento direktoriaus pavaduotojas, koordinuojantis Informatikos ir ryšių departamento Informacinių sistemų plėtros, Informacijos apdorojimo ir statistikos, Teistumo informacijos tvarkymo skyrių veiklą (Valdymo grupės vadovo pavaduotojas);

8.3. Informatikos ir ryšių departamento Sistemų infrastruktūros administravimo skyriaus vedėjas;

8.4. Informatikos ir ryšių departamento Informacijos saugos skyriaus vedėjas;

8.5. Informatikos ir ryšių departamento Telekomunikacijų administravimo skyriaus vedėjas;

8.6. Informatikos ir ryšių departamento Projektų valdymo skyriaus vedėjas;

8.7. Informatikos ir ryšių departamento paskirtas informacinių sistemų pagrindinis saugos įgaliotinis.

9. Valdymo grupės vadovas turi teisę kaip konsultantus pasitelkti kitus Informatikos ir ryšių departamento darbuotojus bei informacinių sistemų valdytojo, tvarkytojų atstovus, susijusius su informacinių sistemų funkcionavimo užtikrinimu, taip pat pagal sutartis dėl informacinių sistemų funkcionavimo paslaugų teikimo veikiančių juridinių asmenų atstovus.

10. Valdymo grupės funkcijos:

10.1. situacijos analizė ir sprendimų informacinių sistemų veiklos tęstinumo valdymo klausimais priėmimas;

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

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

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

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

10.6. elektroninės informacijos fizinė sauga įvykus Incidentui;

10.7. logistika (žmonių, daiktų, įrangos gabenimas ir jo organizavimas);

10.8. informacinių sistemų veiklos atkūrimo priežiūra ir koordinavimas;

10.9. kitos Valdymo grupei pavestos funkcijos.

11. Įvykus Incidentui, informacinių sistemų veiklą atkuria informacinių sistemų veiklos atkūrimo grupė (toliau – Atkūrimo grupė), kurią sudaro:

11.1. Informatikos ir ryšių departamento Sistemų infrastruktūros administravimo skyriaus vedėjas (Atkūrimo grupės vadovas);

11.1. Informatikos ir ryšių departamento Informacinių technologijų paslaugų skyriaus vedėjas (Atkūrimo grupės vadovo pavaduotojas);

11.2. Informatikos ir ryšių departamento Informacijos apdorojimo ir statistikos skyriaus vedėjas;

11.3. Informatikos ir ryšių departamento Teistumo informacijos tvarkymo skyriaus vedėjas;

11.4. Informatikos ir ryšių departamento Sistemų infrastruktūros administravimo skyriaus patarėjas;

11.5. Informatikos ir ryšių departamento Telekomunikacijų administravimo skyriaus patarėjas;

11.6. Informatikos ir ryšių departamento paskirti asmenys, atsakingi už tarnybinių stočių veikimo, kompiuterių tinklo veikimo, taikomųjų programų tinkamo veikimo, darbo kompiuterių veikimo, informacinių sistemų elektroninės informacijos, duomenų atkūrimą;

11.7. išoriniai ekspertai (jei būtina).

12. Atkūrimo grupės vadovas turi teisę kaip konsultantus pasitelkti kitus Informatikos ir ryšių departamento darbuotojus bei informacinių sistemų valdytojo, tvarkytojų atstovus, susijusius su informacinių sistemų funkcionavimo užtikrinimu, taip pat pagal sutartis dėl informacinių sistemų funkcionavimo paslaugų teikimo veikiančių juridinių asmenų atstovus.

13. Atkūrimo grupės funkcijos:

13.1. tarnybinių stočių veikimo atkūrimo organizavimas;

13.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

13.3. informacinių sistemų elektroninės informacijos atkūrimo organizavimas;

13.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

13.5. darbo kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

13.6. kitos Atkūrimo grupei pavestos funkcijos.

14. Valdymo ir Atkūrimo grupių asmeninę sudėtį įsakymu tvirtina Informatikos ir ryšių departamento direktorius.

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

16. Reaguojant į Incidentus ir juos valdant, turi būti vadovaujamasi veiksmais, išdėstytais Informacinių sistemų veiklos atkūrimo detaliajame plane. Jei Incidentas susijęs su kibernetiniu saugumu, taip pat turi būti vadovaujamasi Kibernetinių incidentų valdymo vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano, patvirtinto Lietuvos Respublikos vidaus reikalų ministro 2017 m. rugsėjo 20 d. įsakymu Nr. 1V-651 „Dėl Kibernetinių incidentų valdymo vidaus reikalų ministerijos valdomose ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“, (toliau – Kibernetinių incidentų valdymo planas) nuostatomis.

17. Turi būti nedelsiant imamasi visų priemonių, būtinų informacinių sistemų veiklai atkurti, pavyzdžiui, incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga keičiama turima rezervine arba testavimui skirta informacinių sistemų aplinkos įranga, vėliau įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka, įsigijimo sąnaudos padengiamos iš Lietuvos Respublikos valstybės biudžeto ir kitų finansavimo šaltinių.

18. Atsarginių patalpų, naudojamų informacinių sistemų veiklai atkurti įvykus Incidentui, reikalavimai:

18.1. patekimas į patalpas turi būti registruojamas žurnale;

18.2. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

18.3. patalpos turi atitikti priešgaisrinės saugos reikalavimus, jose turi būti įrengtos gaisro gesinimo priemonės;

18.4. patalpų durys turi būti šarvuotos ir apsaugotos bent dviem skirtingos konstrukcijos spynomis;

18.5. patalpose turi būti įrengtas rezervinis elektros energijos šaltinis, užtikrinantis įrangos veikimą ne trumpiau kaip 10 minučių, taip pat elektros generatorius nepertraukiam informacinių sistemų veikimui užtikrinti. sutrikus elektros energijos tiekimui;

18.6. patalpoje turi nuolat veikti oro temperatūros ir drėgmės reguliavimo įranga (oro kondicionavimo sistema).

19. Incidento atveju informacinių sistemų veiklai atkurti naudojamos pagrindinėms patalpoms, kuriose veikia informacinės sistemos, keliamus reikalavimus atitinkančios atsarginės patalpos, esančios Žirmūnų g. 1D, Vilniuje.

20. Valdymo ir Atkūrimo grupės tarpusavyje bendrauja el. paštu ar telefonu. Ne rečiau negu kartą per metus organizuojamas šių dviejų grupių susitikimas, kuriame aptariama esama situacija ir suderinami galimi jos pagerinimo būdai.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

21. Informatikos ir ryšių departamentas parengia šiuos dokumentus:

21.1. informacinių sistemų informacinių technologijų įrangos sąrašus su šios įrangos parametrais;

21.2. patalpų brėžinius ir šiose patalpose esančios įrangos bei komunikacijų sąrašą (jame pažymint tarnybines stotis, kompiuterių tinklo ir telefonų tinklo mazgus, kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietas, elektros įvedimo pastate vietas);

21.3. kompiuterių tinklo fizinio ar loginio sujungimo schemas.

22. Plano 21.1–21.3 papunkčiuose nurodytų dokumentų kopijos saugomos Informatikos ir ryšių departamento Informacinių technologijų ir telekomunikacijų pagalbos grupėje (toliau – ITT pagalbos grupė), informacinių sistemų techninės ir programinės įrangos konfigūracijos duomenys tvarkomi Vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų Informacinių technologijų paslaugų valdymo posistemėje.

23. Informacinių sistemų administratorius pavaduojančių asmenų minimalus kompetencijos ar žinių lygis negali būti žemesnis už Informatikos ir ryšių departamento paskirtiems informacinių sistemų administratoriams keliamų reikalavimų lygį.

24. Minimalaus funkcionalumo informacinių technologijų įrangos institucijos poreikius atitinkančiai informacinės sistemos veiklai užtikrinti Incidento metu specifikacija turi būti lygiavertė arba geresnė nei pagrindinė informacinės sistemos techninės ir programinės įrangos specifikacija.

25. Duomenų teikimo, techninės ir programinės įrangos priežiūros sutarčių duomenys tvarkomi Vidaus reikalų ministerijos pavedimų valdymo sistemoje, pasiekiamoje adresu https://pavedimai.vrm.lt/projects/ird-duomenu-tiekimo-sutartys/dmsf. Šių sutarčių suvestiniai duomenys ir kontaktiniai duomenys asmenų, atsakingų už sutarčių vykdymą, saugomi ITT pagalbos grupėje.

26. Informacinių sistemų atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos kitose patalpose, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota.

27. Informatikos ir ryšių departamento paskirtas informacinių sistemų pagrindinis saugos įgaliotinis saugo ir periodiškai atnaujina Valdymo grupės ir Atkūrimo grupės narių sąrašą ir jų kontaktinius duomenis.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

28. Plano veiksmingumo išbandymo būdą ir datą nurodo Informatikos ir ryšių departamento direktorius informacinių sistemų pagrindinio saugos įgaliotinio teikimu.

29. Planas turi būti išbandomas ne rečiau kaip kartą per metus. Plano veiksmingumas išbandomas Incidento teorinio modeliavimo, simuliacinio žaidimo ar kitu būdu. Jei Incidentas susijęs su kibernetiniu saugumu, išbandymo metu turi būti vadovaujamasi Kibernetinių incidentų valdymo plano nuostatomis.

30. Pagal bandymų rezultatus, teikiamus Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos administruojamų informacinių sistemų ir registrų elektroninės informacijos atsarginių kopijų darymo, saugojimo ir atkūrimo tvarkos aprašo, patvirtinto Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus 2017 m. sausio 7 d. įsakymu Nr. 5V-6 „Dėl Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos administruojamų informacinių sistemų ir registrų elektroninės informacijos atsarginių kopijų darymo, saugojimo ir atkūrimo tvarkos aprašo patvirtinimo“, nustatyta tvarka Informatikos ir ryšių departamento paskirtam informacinių sistemų pagrindiniam saugos įgaliotiniui, jis parengia informacinių sistemų veiklos tęstinumo valdymo plano veiksmingumo išbandymo ataskaitą (toliau – Ataskaita) (2 priedas), kurioje yra apibendrinami atliktų bandymų rezultatai, akcentuojami pastebėti trūkumai ir pasiūlomos šių trūkumų šalinimo priemonės. Gali būti parengiama bendra Plano ir Kibernetinių incidentų valdymo plano išbandymo Ataskaita. Ataskaita pateikiama Informatikos ir ryšių departamento direktoriui ir informacinių sistemų valdytojui.

31. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo plano
1 priedas

VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
1. Gamtinės sąlygos (klimatinių sąlygų pakitimai)	1.1. galimos žalos informacinėms sistemoms įvertinimas, priemonių plano užkirsti kelią elektroninės informacijos saugos incidentui ar jo plėtrai (toliau – saugos incidentas) sudarymas ir įgyvendinimas;	1.1.1. žalos įvertinimas, priemonių plano saugos incidento pasekmėms likviduoti sudarymas ir įgyvendinimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas
	1.2. informacinių sistemų veiklos atkūrimo veiksmus atliekančių darbuotojų paskyrimas, jų budėjimo grafiko nustatymas ir jų informavimas apie tai;	1.2.1. darbų grafiko saugos incidento pasekmėms likviduoti sudarymas; 1.2.2. saugos incidento pasekmių likvidavimo darbams atlikti darbuotojų sąrašo sudarymas ir jų informavimas apie tai;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas
	1.3. meteorologinės informacijos sekimas;	1.3.1. saugos incidento pasekmių likvidavimo darbus atliekančių darbuotojų informavimas apie esamą situaciją;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	1.4. informacinių sistemų naudotojams rekomenduojamo elgesio saugos incidento metu skelbimas žodžiu arba ryšio priemonėmis;	1.4.1. saugos incidento pasekmių likvidavimo darbus atliekančių darbuotojų instruktavimas apie elgseną saugos incidento vietoje;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
	1.5. saugios vietos nustatymas ir nurodymas informacinių sistemų naudotojams eiti į saugią vietą;	1.5.1. informacinių sistemų naudotojų informavimas apie būtinumą pereiti į kitas saugias patalpas;	Veiklos tęstinumo valdymo grupės vadovas
	1.6. informacinių sistemų naudotojų informavimas apie darbo sustabdymą dėl nepalankių sąlygų;	1.6.1. informacinių sistemų naudotojų informavimas apie esamą situaciją ir numatomas darbo sąlygas;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	1.7. pasiruošimas suteikti nukentėjusiems informacinių sistemų naudotojams pirmąją pagalbą;	1.7.1. pirmos pagalbos suteikimas nukentėjusiems informacinių sistemų naudotojams, nukentėjusių gabenimo į gydymo įstaigą organizavimas;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	1.8. pavojingų vietų ženklinimas, informacinių lentelių pakabinimas;	1.8.1. informacinių sistemų naudotojų informavimas, saugos incidento pasekmes likviduojančių darbuotojų instruktavimas;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	1.9. alternatyvių energijos tiekimo šaltinių panaudojimas;	1.9.1. energijos tiekimo tarnybų rekomendacijų vykdymas;	Veiklos atkūrimo grupės vadovas
	1.10. alternatyvaus ryšio organizavimas;	1.10.1. kreipimasis į ryšio paslaugos teikėjus;	Veiklos atkūrimo grupės vadovas
	1.11. pagrindinės informacinių sistemų techninės ir programinės įrangos, duomenų galimam pavojui išvengti / likviduoti paruošimas;	1.11.1. informacinių sistemų tarnybinių stočių, kitos techninės įrangos išjungimas;	Veiklos atkūrimo grupės vadovo paskirtas administratorius

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
2. Potvynis	2.1. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4 papunkčiuose, atlikimas;	2.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2 1.3.1, 1.4.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo Veiklos atkūrimo grupės vadovas Veiklos atkūrimo grupės vadovo paskirtas administratorius
	2.2. potvynio prognozės sekimas;	2.2.1. Saugos incidento pasekmes likviduojančių darbuotojų instruktavimas	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	2.3. veiksmų, nurodytų šio priedo 1.5–1.11 papunkčiuose, atlikimas;	2.3.1. informacinių sistemų naudotojų informavimas apie būtinumą pereiti į kitas saugias patalpas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
		2.3.2. informacinių sistemų naudotojų informavimas apie esamą situaciją ir numatomas darbo sąlygas;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
		2.3.3. pirmos pagalbos suteikimas nukentėjusiems informacinių sistemų naudotojams, nukentėjusių gabenimo į gydymo įstaigą organizavimas;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
		2.3.4. informacinių sistemų naudotojų informavimas, saugos incidento pasekmes likviduojančių darbuotojų instruktavimas;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
		2.3.5. energijos tiekimo tarnybų rekomendacijų vykdymas;	Veiklos atkūrimo grupės vadovas

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
		2.3.6. kreipimasis į ryšio paslaugos teikėjus;	Veiklos atkūrimo grupės vadovas
		2.3.7. informacinių sistemų tarnybinių stočių, kitos techninės įrangos išjungimas;	Veiklos atkūrimo grupės vadovo paskirtas administratorius
3. Pavojingos medžiagos	3.1. pavojingų medžiagų šalinimo tarnybos informavimas;	3.1.1. pavojingų medžiagų šalinimo tarnybos paklausimas dėl leidimo dirbti saugos incidento zonoje, rekomendacijų darbui gavimas ir informacinių sistemų naudotojų informavimas apie rekomenduojamus darbo būdus;	Veiklos tęstinumo valdymo grupės vadovas
	3.2. priešgaisrinės apsaugos ir gelbėjimo tarnybos informavimas;	3.2.1. priešgaisrinės apsaugos ir gelbėjimo tarnybos paklausimas dėl leidimo dirbti saugos incidento vietoje;	Veiklos tęstinumo valdymo grupės vadovas
	3.3. esant priešgaisrinės apsaugos ir gelbėjimo tarnybos rekomendacijai, informacinių sistemų naudotojų evakuacija;	3.3.1. evakuacijos organizavimas, jei gauta priešgaisrinės apsaugos ir gelbėjimo tarnybos rekomendacija;	Veiklos tęstinumo valdymo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	3.4. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 papunkčiuose, atlikimas;	3.4.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo Veiklos atkūrimo grupės vadovas Veiklos atkūrimo grupės vadovo paskirtas administratorius

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
4. Gaisras	4.1. esant būtinumui, informacinių sistemų naudotojų evakuacija;	4.1.1. evakuacijos organizavimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	4.2. priešgaisrinės apsaugos ir gelbėjimo tarnybos informavimas;	4.2.1. priešgaisrinės ir gelbėjimo tarnybos paklausimas dėl leidimo dirbti saugos incidento zonoje, rekomendacijų darbui gavimas, informacinių sistemų naudotojų informavimas apie rekomenduojamus darbo būdus;	Veiklos tęstinumo valdymo grupės vadovas
	4.3. gaisro gesinimas ankstyvoje stadijoje, nekeliant pavojaus informacinių sistemų naudotojų gyvybei;	4.3.1. priešgaisrinės ir gelbėjimo tarnybos nurodymų vykdymas;	Veiklos tęstinumo valdymo grupė
	4.4. komunalinių komunikacijų, galinčių sukelti papildomą nenumatytą situaciją, išjungimas;	4.4.1. priešgaisrinės ir gelbėjimo tarnybos rekomendacijų vykdymas;	Veiklos tęstinumo valdymo grupė
	4.5. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 papunkčiuose, atlikimas;	4.5.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo Veiklos atkūrimo grupės vadovo paskirtas administratorius

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
5. Patalpų, kuriose yra informacinių sistemų tarnybinės stotys ir svarbiausia komutacinė įranga (toliau – patalpos) užgrobimas	5.1. teisėsaugos tarnybų informavimas;	5.1.1. teisėsaugos tarnybų informavimas apie saugos incidentą;	Veiklos tęstinumo valdymo grupės vadovas
	5.2. esant teisėsaugos tarnybų rekomendacijai, visų konkrečioje situacijoje nereikalingų informacinių sistemų naudotojų evakavimas, įspėjant teisėsaugos tarnybas;	5.2.1. informacinių sistemų naudotojų informavimas apie evakavimą, jei yra teisėsaugos tarnybų rekomendacija;	Veiklos tęstinumo valdymo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	5.3. esant būtinumui, informacinių sistemų techninės įrangos išjungimas ir patalpų užrakinimas;	5.3.1. informacinių sistemų tarnybinių stočių, kitos techninės įrangos išjungimas, patalpų užrakinimas, jei yra galimybė;	Veiklos atkūrimo grupės vadovas
	5.4. esant būtinumui, likusių informacinių sistemų naudotojų evakavimas;	5.4.1. informacinių sistemų naudotojų informavimas apie evakavimą, jei yra teisėsaugos tarnybų rekomendacija;	Veiklos tęstinumo valdymo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	5.5. teisėsaugos pareigūnų nurodymų vykdymas;	5.5.1. informacinių sistemų naudotojų informavimas apie teisėsaugos tarnybų nurodymus;	Veiklos tęstinumo valdymo grupė
	5.6. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 papunkčiuose, atlikimas;	5.6.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
			Veiklos atkūrimo grupės vadovo paskirtas administratorius
6. Patalpų sugadinimas	6.1. avarinių ar teisėsaugos tarnybų informavimas, atsižvelgiant į iškilusio pavojaus pobūdį;	6.1.1. atitinkamos tarnybos paklausimas dėl leidimo dirbti pavojaus zonoje, rekomendacijų darbui gavimas, informacinių sistemų naudotojų informavimas apie rekomenduojamus darbo būdus;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	6.2. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4–1.11 papunkčiuose, atlikimas;	6.2.1. veiksmų, nurodytų šios priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1–1.11.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo Veiklos atkūrimo grupės vadovo paskirtas administratorius
	6.3. esant reikalui, atsarginių patalpų informacinių sistemų veiklai užtikrinti ir darbo vietoms išdėstyti suradimas;	6.3.1. darbo organizavimas ir koordinavimas atsarginėse informacinių sistemų patalpose;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	6.4. komunalinių komunikacijų, galinčių sukelti papildomą saugos incidentą, išjungimas;	6.4.1. pažeistų patalpų rekonstrukcijos, atstatymo darbų, komunalinių komunikacijų išjungimo organizavimas ir / ar informacinių sistemų perkėlimas į naujas patalpas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
7. Elektros energijos tiekimo sutrikimai	7.1. elektros energijos tiekimo sistemos veiklos patikrinimas;	7.1.1. pažeisto vietos elektros tinklo, užtikrinančio informacinių sistemų veiklą, atkūrimo organizavimas;	Veiklos atkūrimo grupės vadovas
	7.2. esant būtinumui, tarnybinių stočių ir kitos techninės įrangos, jautrios elektros energijos tiekimo sutrikimams, išjungimas;	7.2.1. elektros energijos tiekimo informacinių sistemų tarnybinėms stotims ir kitai techninei įrangai išjungimas;	Veiklos atkūrimo grupės vadovas Veiklos atkūrimo grupės vadovo paskirtas administratorius
	7.3. kreipimasis į savo elektros energijos tiekimo tarnybą dėl sutrikimo pašalinimo trukmės prognozės;	7.3.1. rekomendacijų iš elektros energijos tiekimo tarnybos gavimas;	Veiklos atkūrimo grupės vadovas
	7.4. sutrikimo pašalinimo trukmės prognozės skelbimas informacinių sistemų naudotojams;	7.4.1. informacinių sistemų naudotojų informavimas apie esamą situaciją bei numatomas darbo sąlygas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	7.5. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4, 1.10, 6.3 papunkčiuose, atlikimas;	7.5.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1, 1.10.1, 6.3.1 papunkčiuose, vykdymas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo Veiklos atkūrimo grupės vadovo paskirtas administratorius
8. Vandentiekio ir šildymo sistemos sutrikimai	8.1. vandentiekio ar šilumos tinklų avarinių tarnybų informavimas, atsižvelgus į sutrikimo pobūdį;	8.1.1. atitinkamos tarnybos informavimas apie sutrikimus, rekomendacijų darbui gavimas, informacinių sistemų naudotojų	Veiklos atkūrimo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
		informavimas apie rekomenduojamus darbo būdus;	
	8.2. sutrikimo pašalinimo prognozės skelbimas informacinių sistemų naudotojams;	8.2.1. informacinių sistemų naudotojų informavimas apie esamą situaciją bei numatomas darbo sąlygas;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	8.3. veiksmų, nurodytų šio priedo 1.1, 1.2, 4.4, 6.3 papunkčiuose, atlikimas;	8.3.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 4.4.1, 6.3.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo Veiklos atkūrimo grupės vadovo paskirtas administratorius
9. Ryšio sutrikimai	9.1. ryšio sutrikimo priežasčių nustatymas;	9.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo Veiklos atkūrimo grupės vadovo paskirtas administratorius
	9.2. telefono ir / ar interneto ryšio paslaugų teikėjų informavimas, atsižvelgus į sutrikimo pobūdį, paklausimo dėl jo pašalinimo trukmės prognozės pateikimas;	9.2.1. kreipimasis į telefono ir / ar interneto paslaugų teikėjus;	Veiklos atkūrimo grupės vadovas Telekomunikacijų administravimo skyriaus vedėjas

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
	9.3. sutrikimo pašalinimo prognozės skelbimas informacinių sistemų naudotojams;	9.3.1. informacinių sistemų naudotojų informavimas apie esamą situaciją ir numatomas darbo sąlygas;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
	9.4. alternatyvaus ryšio organizavimas;	9.4.1. neatkūrus ryšio per prognozuotą laiką, ryšio per kitus ryšio paslaugų teikėjus organizavimas;	Veiklos atkūrimo grupės vadovas Telekomunikacijų administravimo skyriaus vedėjas
10. Informacinių sistemų tarnybinių stočių ar komutacinės įrangos sugadinimas (gedimas), sunaikinimas, praradimas	10.1. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4, 1.6 papunkčiuose, atlikimas;	10.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1, 1.6.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo Veiklos atkūrimo grupės vadovo įgaliotas administratorius
	10.2. rezervinės informacinių sistemų techninės įrangos naudojimas;	10.2.1. esant būtinumui, kreipimasis į teisėsaugos tarnybas dėl informacinių sistemų techninės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas;	Veiklos atkūrimo grupės vadovas
		10.2.2. esamos techninės įrangos išteklių perskirstymas informacinių sistemų veiklai užtikrinti;	Veiklos tęstinumo grupės vadovas
		10.2.3. esant būtinumui, kreipimasis į techninės įrangos tiekėjus dėl sugadintos	Veiklos atkūrimo grupės vadovas

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
		įrangos remonto ar dėl naujos techninės įrangos įsigijimo;	
		10.2.4. pranešimas draudimo įstaigai apie įvykį, dėl kurio nukentėjo apdrausti daiktai;	Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo
11. Informacinių sistemų programinės įrangos sugadinimas, praradimas	11.1. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4 papunkčiuose, atlikimas;	11.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo Veiklos atkūrimo grupės vadovo paskirtas administratorius
	11.2. informacinių sistemų programinės įrangos atkūrimas iš atsarginių kopijų;	11.2.1. esant būtinumui, kreipimasis į teisėsaugos tarnybas dėl programinės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas;	Veiklos tęstinumo valdymo grupės vadovas
		11.2.2. sugadintos ar prarastos programinės įrangos atkūrimas iš programinės įrangos kopijų;	Veiklos atkūrimo grupės vadovas Veiklos atkūrimo grupės vadovo paskirtas administratorius
12. Informacinių sistemų duomenų pakeitimas,	12.1. veiksmų, nurodytų šio priedo 1.1, 1.2, 1.4, 1.6 papunkčiuose, atlikimas.	12.1.1. veiksmų, nurodytų šio priedo 1.1.1, 1.2.1, 1.2.2, 1.4.1, 1.6.1 papunkčiuose, atlikimas;	Veiklos tęstinumo valdymo grupės vadovas Veiklos atkūrimo grupės vadovas

Elektroninės informacijos saugos incidentas	Veiksmai esant elektroninės informacijos saugos incidentui	Informacinių sistemų veiklos atkūrimo veiksmai	Informacinių sistemų veiklos atkūrimo veiksmų atsakingi vykdytojai
sunaikinimas, atskleidimas			Veiklos tęstinumo valdymo grupės vadovo paskirtas asmuo Veiklos atkūrimo grupės vadovo paskirtas administratorius
		12.1.2. įvykus neteisėtam informacinių sistemų duomenų pakeitimui, sunaikinimui ar atskleidimui, kreipimasis į teisėsaugos tarnybas ir jų nurodymų vykdymas;	Veiklos tęstinumo valdymo grupės vadovas
		12.1.3. informacinėms sistemoms nustojus funkcionuoti dėl duomenų pakeitimo ar sunaikinimo, duomenų atkūrimas iš duomenų kopijų;	Veiklos atkūrimo grupės vadovas Veiklos atkūrimo grupės vadovo paskirtas administratorius
		12.1.4. nesant galimybių atkurti pakeistų ar sunaikintų duomenų iš duomenų kopijų, informacinių sistemų duomenų gavėjų informavimas dėl būtinumo sugadintus ar prarastus duomenis iš naujo įrašyti į duomenų bazes.	Veiklos tęstinumo valdymo grupės vadovas

Kai kurių Lietuvos Respublikos vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo plano
2 priedas

(Vidaus reikalų ministerijos valdomų registrų ir valstybės informacinių sistemų veiklos tęstinumo valdymo plano išbandymo ataskaitos forma)

VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ REGISTRŲ IR VALSTYBĖS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO ATASKAITA

_____ Nr. _____

Plano išbandymas (pratybos) vyko:
_____

Plano išbandyme dalyvavo Veiklos tęstinumo valdymo grupės nariai:
1. _____
2. _____
3. _____

Plano išbandymo scenarijus:
_____
_____
_____

Plano išbandymo eiga:
_____
_____
_____

Rasti trūkumai:
_____
_____
_____

Pasiūlymai dėl trūkumų šalinimo, Plano tikslinimo:
_____
_____
_____

Veiklos tęstinumo valdymo grupės vadovo ir ataskaitą parengusio asmens parašai:

_____ _____
(vardas, pavardė) (parašas)

_____ _____
(vardas, pavardė) (parašas)

_____