Suvestinė redakcija nuo 2021-04-30

Įsakymas paskelbtas: TAR 2020-09-11, i. k. 2020-19123

LIETUVOS RESPUBLIKOS SUSISIEKIMO MINISTRAS

ĮSAKYMAS DĖL NACIONALINĖS ELEKTRONINIŲ SIUNTŲ PRISTATYMO, NAUDOJANT PAŠTO TINKLĄ, INFORMACINĖS SISTEMOS SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ PATVIRTINIMO

2020 m. rugsėjo 11 d. Nr. 3-519
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 punktu, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 6 punktu:

1. T v i r t i n u pridedamus Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos saugos politiką įgyvendinančius dokumentus:

1.1. Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos saugaus elektroninės informacijos tvarkymo taisykles;

1.2. Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos veiklos tęstinumo valdymo planą;

1.3. Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos naudotojų administravimo taisykles.

2. P a v e d u Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos saugos įgaliotiniui pateikti patvirtintų Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

Susisiekimo ministras Jaroslav Narkevič

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2020 m. rugpjūčio 19 d. raštu Nr. (4.1 E) 6K-526

PATVIRTINTA
Lietuvos Respublikos susisiekimo
ministro 2020 m. rugsėjo 11 d.
įsakymu Nr. 3-519

NACIONALINĖS ELEKTRONINIŲ SIUNTŲ PRISTATYMO, NAUDOJANT PAŠTO TINKLĄ, INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato techninių ir kitų saugos priemonių aprašymą, saugų elektroninės informacijos tvarkymą, reikalavimus, keliamus Nacionalinei elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinei sistemai (toliau – E. siuntų pristatymo IS) funkcionuoti reikalingoms paslaugoms ir jų teikėjams.

2. Taisyklės privalomos E. siuntų pristatymo IS išoriniams naudotojams, E. siuntų pristatymo IS administratoriams, E. siuntų pristatymo IS saugos įgaliotiniui (-iams) ir asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą (kibernetinio saugumo vadovui).

3. Taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu ir Saugos dokumentų turinio gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Aprašas), ir Lietuvos Respublikos krašto apsaugos ministro tvirtinamais Techniniais informacinių sistemų elektroninės informacijos saugos reikalavimais.

4. Taisyklėse vartojamos sąvokos atitinka sąvokas, vartojamas 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“.

5. Remiantis Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos duomenų saugos nuostatų, patvirtintų Lietuvos Respublikos susisiekimo ministro 2017 m. sausio 9 d. įsakymu Nr. 3-9 „Dėl Nacionalinės elektroninių siuntų pristatymo,

naudojant pašto tinklą, informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – Saugos nuostatai), 22 punktu, E. siuntų pristatymo IS tvarkoma elektroninė informacija yra priskiriama vidutinės svarbos informacijos kategorijai, o E. siuntų pristatymo IS yra priskiriama trečiajai kategorijai.

6. E. siuntų pristatymo IS tvarkoma Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2015 m. rugpjūčio 26 d. nutarimu Nr. 914 „Dėl Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos nuostatų patvirtinimo“ (toliau – E. siuntų pristatymo IS nuostatai), III skyriuje išvardinta elektroninė informacija. Už jos tvarkymą atsakingi E. siuntų pristatymo IS naudotojai ir E. siuntų pristatymo IS administratoriai.

II SKYRIUS
E. SIUNTŲ PRISTATYMO IS TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

7. E. siuntų pristatymo IS techninės ir kompiuterinės įrangos saugos priemonės:

7.1. tarnybinėse stotyse ir E. siuntų pristatymo IS vidinių naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės; šios priemonės automatiškai turi informuoti E. siuntų pristatymo IS administratorius apie tai, kuriems E. siuntų pristatymo IS posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas. E. siuntų pristatymo IS komponentai be kenksmingosios programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu rizikos vertinimo metu yra patvirtinama, kad šių komponentų rizika yra priimtina;

7.2. E. siuntų pristatymo IS techninė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų. Techninę priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai;

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

7.4. paslaugų tarnybinės stotys ir svarbiausi elektroninės informacijos perdavimo tinklo mazgai turi įtampos filtrą ir rezervinį elektros energijos tiekimo šaltinį. Rezervinis elektros energijos tiekimo šaltinis užtikrina E. siuntų pristatymo IS pagrindinių tarnybinių stočių veikimą ne trumpiau kaip 1 val.;

7.5. E. siuntų pristatymo IS veikimo stebėjimo priemonės turi perspėti E. siuntų pristatymo IS administratorius, kai pagrindinėje E. siuntų pristatymo IS kompiuterinėje įrangoje iki nustatytos pavojingos ribos sumažėja laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja, sutrinka kitų E. siuntų pristatymo IS komponentų įprastas veikimas;

7.6. turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų E. siuntų pristatymo IS įeinantį ir išeinantį duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų;

7.7. pagrindinėse E. siuntų pristatymo IS tarnybinėse stotyse turi būti įjungtos saugasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį duomenų srautą, išskyrus susijusį su E. siuntų pristatymo IS funkcionalumu ir administravimu;

7.8. įsilaužimo aptikimo techninių sprendinių įgyvendinimas, konfigūracija ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo E. siuntų pristatymo IS techninės įrangos (kartu nurodant tam tikras datas (įgyvendinimo, atnaujinimo ir pan.), atsakingus asmenis, taikymo periodus ir pan.).

8. Sisteminės ir taikomosios E. siuntų pristatymo IS programinės įrangos saugos priemonės:

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

8.2. E. siuntų pristatymo IS darbui naudojama tik legali sisteminė ir taikomoji programinė įranga;

8.3. E. siuntų pristatymo IS vidinių naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga. E. siuntų pristatymo IS saugos įgaliotinis turi parengti, su E. siuntų pristatymo IS tvarkytojo – VĮ Registrų centro (toliau – E. siuntų pristatymo IS tvarkytojas) vadovu suderinti ir ne rečiau kaip kartą per metus peržiūrėti ir prireikus atnaujinti leistinos programinės įrangos sąrašą;

8.4. E. siuntų pristatymo IS tarnybinėse stotyse neturi veikti sisteminė ir taikomoji programinė įranga, kuri yra nesusijusi su E. siuntų pristatymo IS tvarkymu, E. siuntų pristatymo IS naudotojų ir pačios įrangos administravimu;

8.5. turi būti operatyviai testuojami ir įdiegiami E. siuntų pristatymo IS tarnybinių stočių ir E. siuntų pristatymo IS vidinių naudotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai. E. siuntų pristatymo IS administratoriai reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie neįdiegtus gamintojų rekomenduojamus E. siuntų pristatymo IS posistemių, funkciškai savarankiškų sudedamųjų dalių, E. siuntų pristatymo IS vidinių naudotojų darbo vietų kompiuterinės įrangos atnaujinimus ir susijusius saugos pažeidžiamumų svarbos lygius;

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

8.7. programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka E. siuntų pristatymo IS administratoriai arba kiti E. siuntų pristatymo IS valdytojo ar tvarkytojo vadovo įgalioti asmenys;

8.8. programinė įranga prižiūrima laikantis gamintojo rekomendacijų. Programinės įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai;

8.9. programinės įrangos testavimas atliekamas naudojant atskirą testavimo aplinką;

8.10. per metus turi būti užtikrintas E. siuntų pristatymo IS prieinamumas ne mažiau kaip 96 proc. laiko darbo metu darbo dienomis.

9. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

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

9.2. ugniasienės įvykių žurnalai (angl. *Logs*) reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai persvarstomos ir atnaujinamos E. siuntų pristatymo IS administratorių;

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

9.4. viešaisiais ryšių tinklais perduodamos E. siuntų pristatymo IS elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. *Virtual Private Network*), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas priemones;

9.5. tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešajame ryšių tinkle naršančių E. siuntų pristatymo IS naudotojų kompiuterinę įrangą nuo kenksmingo kodo.

10. E. siuntų pristatymo IS patalpų saugos priemonės:

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

10.2. patalpos, kuriose yra E. siuntų pristatymo IS tarnybinės stotys, turi būti atskirtos nuo bendrojo naudojimo patalpų. Į šias patalpas patekti gali tik E. siuntų pristatymo IS tvarkytojo įgalioti asmenys, kitus asmenis turi lydėti E. siuntų pristatymo IS administratoriai;

10.3. jei E. siuntų pristatymo IS tarnybinių stočių patalpose esančios įrangos bendras galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga;

10.4. prieiga prie patalpų, kuriose yra E. siuntų pristatymo IS tarnybinės stotys, ir patalpų, kuriose saugomos atsarginės kopijos, turi būti kontroliuojama (registruojami įeinančių ir išeinančių iš patalpų apsilankymai, kontroliuojamas patekimas į patalpas Taisyklių 10.2 papunktyje nustatyta tvarka).

11. Prisiregistravimo prie E. siuntų pristatymo IS ir išsiregistravimo iš jos duomenys (prisijungimo vardas, data, laikas) automatiškai fiksuojami E. siuntų pristatymo IS elektroniniuose veiksmų žurnaluose (toliau – veiksmų žurnalai), kurie prieinami tik atitinkamam E. siuntų pristatymo IS administratoriui. Veiksmų žurnalai yra saugomi E. siuntų pristatymo IS duomenų bazėje ir jų apsaugai nuo netyčinio arba neteisėto jų duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų yra taikomos tos pačios saugos priemonės, kaip ir E. siuntų pristatymo IS elektroninei informacijai. Už veiksmų žurnalų tvarkymą atsakingas E. siuntų pristatymo IS administratorius.

12. E. siuntų pristatymo IS turi būti įrašomi ir ne trumpiau nei vienus metus saugomi duomenys apie E. siuntų pristatymo IS tarnybinių stočių, E. siuntų pristatymo IS taikomosios programinės įrangos ir kitų E. siuntų pristatymo IS komponentų įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis E. siuntų pristatymo IS tarnybinėse stotyse, E. siuntų pristatymo IS taikomojoje programinėje įrangoje, visus E. siuntų pristatymo IS naudotojų vykdomus veiksmus (elektroninės informacijos įvedimas, peržiūra, keitimas, atnaujinimas, naikinimas ir kiti elektroninės informacijos tvarkymo veiksmai), kitus elektroninės informacijos saugai svarbius įvykius, nurodant E. siuntų pristatymo IS naudotojo ir E. siuntų pristatymo IS administratoriaus identifikatorių ir elektroninės informacijos saugai svarbaus įvykio ar vykdyto veiksmo datą ir laiką, įvykio ar veiksmo rezultatą, E. siuntų pristatymo IS naudotojo, E. siuntų pristatymo IS administratoriaus ir (arba) E. siuntų pristatymo IS įrenginio, susijusio su įvykiu, duomenis; šie duomenys turi būti saugomi ne toje pačioje E. siuntų pristatymo IS, kurioje jie įrašomi, taip pat jie turi būti analizuojami ne rečiau kaip kartą per savaitę E. siuntų pristatymo IS administratoriaus. Turi būti įrašomas audito funkcijos įjungimas ir išjungimas, audito įrašų trynimas, kūrimas ar keitimas. Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas.

13. E. siuntų pristatymo IS naudotojų ir E. siuntų pristatymo IS administratorių tapatybei nustatyti ir prieigai prie elektroninės informacijos kontroliuoti būtina naudoti prisijungimo vardų, slaptažodžių ir teisių sistemą.

14. Pagrindinės E. siuntų pristatymo IS kompiuterinės įrangos techninė būklė turi būti nuolat stebima. Pagrindinės kompiuterinės įrangos gedimai turi būti registruojami. Už gedimų

registravimą atsakingi E. siuntų pristatymo IS administratoriai.

15. E. siuntų pristatymo IS naudotojui neatliekant jokių veiksmų E. siuntų pristatymo IS taikomoji programinė įranga turi užsirakinti, kad toliau naudotis E. siuntų pristatymo IS būtų galima tik pakartotinai patvirtinus savo tapatybę. Terminas, per kurį E. siuntų pristatymo IS naudotojui neatliekant jokių veiksmų E. siuntų pristatymo IS užsirakina, negali būti ilgesnis nei 15 minučių.

III SKYRIUS
SAUGUS E. SIUNTŲ PRISTATYMO IS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

16. Šių Taisyklių 5 punkte nurodytą tvarkomą elektroninę informaciją įvesti, keisti, atnaujinti gali tik E. siuntų pristatymo IS išoriniai naudotojai ir E. siuntų pristatymo IS administratoriai pagal nustatytas prieigos teises.

17. E. siuntų pristatymo IS posistemės naudoja įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones.

18. E. siuntų pristatymo IS išoriniams naudotojams ar E. siuntų pristatymo IS administratoriams, atliekant veiksmus su E. siuntų pristatymo IS elektronine informacija, automatiškai veiksmų žurnale registruojamas darbo laikas, prisijungimo vardas ir atliekami veiksmai. Šie duomenys skirti elektroninės informacijos vientisumo pažeidimams nustatyti.

19. Baigus darbą ar E. siuntų pristatymo IS naudotojui pasitraukus iš darbo vietos turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo E. siuntų pristatymo IS, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai ar jų kopijos darbo vietoje turi būti padedami į pašaliniams asmenims neprieinamą vietą.

20. Elektroninė informacija naikinama E. siuntų pristatymo IS nuostatų VIII ir IX skyriuose nustatyta tvarka.

21. E. siuntų pristatymo IS elektroninės informacijos kopijų rengimas:

21.1. E. siuntų pristatymo IS elektroninės informacijos kopijos daromos ne rečiau kaip kartą per savaitę;

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

21.3. atsarginės laikmenos su E. siuntų pristatymo IS programinės įrangos kopijomis turi būti laikomos nedegioje spintoje, kitose patalpose arba kitame pastate, nei yra E. siuntų pristatymo IS tarnybinės stotys;

21.4. E. siuntų pristatymo IS elektroninės informacijos kopijos saugomos kitose patalpose, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate taip, kad prireikus jas būtų galima atkurti;

21.5. duomenys apie E. siuntų pristatymo IS elektroninės informacijos kopijų darymą turi būti fiksuojami kopijų darymo įvykių žurnale;

21.6. sunaikintos ar sugadintos E. siuntų pristatymo IS elektroninės informacijos atkūrimą kontroliuoja E. siuntų pristatymo IS administratoriai.

22. E. siuntų pristatymo IS elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) nustatymo tvarka:

22.1. E. siuntų pristatymo IS administratoriai privalo ne rečiau nei kartą per mėnesį peržiūrėti visus E. siuntų pristatymo IS veiksmų žurnaluose registruojamus įrašus, siekdami patikrinti, ar nėra vykdoma neteisėta veikla;

22.2. kilus įtarimui, kad su E. siuntų pristatymo IS ar jos elektronine informacija yra vykdoma neteisėta veikla, E. siuntų pristatymo IS vidiniai naudotojai privalo nedelsdami informuoti E. siuntų pristatymo IS tvarkytojo informacinių technologijų pagalbos tarnybą, kuri inicijuoja neteisėtos veiklos tyrimą ir priskiria už tyrimą atsakingus asmenis, o E. siuntų pristatymo IS išoriniai naudotojai privalo nedelsdami apie tai pranešti E. siuntų pristatymo IS tvarkytojui jo interneto svetainėje nurodytais kontaktais. Į pranešimus apie neteisėtas veiklas turi būti reaguojama nedelsiant ir imamasi visų įmanomų veiksmų, reikalingų užkirsti kelią neteisėtai veiklai.

23. Programinės ir techninės E. siuntų pristatymo IS įrangos keitimo ir atnaujinimo tvarka (toliau – Pokyčių valdymo tvarka):

23.1. pokyčiai identifikuojami analizuojant vidinę ir išorinę E. siuntų pristatymo IS valdytojo ir E. siuntų pristatymo IS tvarkytojo veiklos aplinką ir poreikius, kuriuos formuoja socialiniai, teisiniai, ekonominiai, technologiniai aspektai ir tendencijos, esama padėtis (E. siuntų pristatymo IS sąranka, pažeidžiamumai, atitiktis teisės aktų ir standartų reikalavimams ir panašiai);

23.2. pokyčiai, atsižvelgiant į jų svarbą, aktualumą ir poreikį, skirstomi į kategorijas pagal pokyčio tipą (administracinis, organizacinis, funkcinis, programinis ar techninis);

23.3. pokyčius turi teisę inicijuoti E. siuntų pristatymo IS duomenų valdymo įgaliotinis, E. siuntų pristatymo IS saugos įgaliotinis ar E. siuntų pristatymo IS administratorius (-iai), o įgyvendinti – E. siuntų pristatymo IS administratorius (-iai). Atlikdamas (-i) E. siuntų pristatymo IS sąrankos pakeitimus, E. siuntų pristatymo IS administratorius (-iai) turi laikytis Pokyčių valdymo tvarkos;

23.4. prioritetas turi būti skiriamas skubiems ir plėtros (vystymo) pokyčiams. Pokyčių prioritetas nustatomas pokyčių įtakos vertinimo metu;

23.5. funkcinių, programinių ir techninių pokyčių įtaką pagal kompetenciją vertina E. siuntų pristatymo IS tvarkytojo paslaugų valdymo direktoriaus pavaldumui priklausantys struktūriniai padaliniai. Pokyčių įtakai įvertinti gali būti sudaroma darbo grupė. Šią darbo grupę gali sudaryti E. siuntų pristatymo IS valdytojo ir E. siuntų pristatymo IS tvarkytojo kompetentingi valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, prireikus – nepriklausomi ekspertai;

23.6. pokyčių įtakos vertinimo metu turi būti įvertinama pokyčių nauda ir pagrįstumas, pokyčių įgyvendinamumas ir alternatyvūs sprendimai, pokyčiams atlikti reikalingos sąnaudos, taip pat informacinių sistemų veiklos sutrikdymo ar sustabdymo rizika, elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo pažeidimo rizika;

23.7. galimybių studija turi būti rengiama, kai pokyčių įtakos vertinimo metu nustatoma, kad informacinėms sistemoms kurti ar modernizuoti planuojama viršyti Lietuvos Respublikos Vyriausybės ar jos įgaliotos institucijos patvirtintą lėšų dydį;

23.8. visi E. siuntų pristatymo IS pokyčiai, susiję su programinės ir (arba) techninės įrangos keitimu ir (arba) atnaujinimu, galintys sutrikdyti ar sustabdyti E. siuntų pristatymo IS darbą, įgyvendinami tik raštiškai suderinus su E. siuntų pristatymo IS valdytoju ar E. siuntų pristatymo IS duomenų valdymo įgaliotiniu;

23.9. prieš atliekant E. siuntų pristatymo IS programinės ir (arba) techninės įrangos keitimą ir (arba) atnaujinimą, kurio metu gali būti pažeistas E. siuntų pristatymo IS elektroninės informacijos vientisumas, prieinamumas ir (ar) konfidencialumas, pokyčiai turi būti patikrinti bandomojoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos E. siuntų pristatymo IS;

23.10. atlikus testavimą ir konstatavus keičiamos ir (arba) atnaujinamos E. siuntų pristatymo IS programinės ir (arba) techninės įrangos sėkmingą veikimą, E. siuntų pristatymo IS

administratoriai pradeda rengti keičiamos ir (arba) atnaujinamos programinės ir (arba) techninės įrangos keitimo ir (arba) atnaujinimo planą;

23.11. E. siuntų pristatymo IS administratorius (-iai) privalo patikrinti (peržiūrėti) E. siuntų pristatymo IS sąranką ir informacinės sistemos būsenos rodiklius reguliariai, ne rečiau kaip kartą per metus ir (arba) po informacinės sistemos pokyčio. E. siuntų pristatymo IS sąrankos aprašai turi būti nuolat atnaujinami ir rodyti esamą informacinės sistemos sąrankos būklę.

24. E. siuntų pristatymo IS naudojamų svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumo ir kontrolės priemonės:

24.1. turi būti įgyvendinti atpažinties, tapatumo patvirtinimo ir naudojimosi E. siuntų pristatymo IS saugumo ir kontrolės reikalavimai, nustatyti Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos naudotojų administravimo taisyklėse;

24.2. draudžiama slaptažodžius saugoti programiniame kode;

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

24.4. turi būti įgyvendinti svetainės kriptografijos reikalavimai;

24.5. svetainės administravimo darbai turi būti atliekami ne trumpesniu kaip 128 bitų raktu;

24.6. šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2 048 bitų;

24.7. turi būti naudojamas TLS (angl. *Transport Layer Security*) standartas;

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

24.9. kriptografiniai raktai ir algoritmai turi būti nustatomi, atsižvelgiant į Lietuvos ir tarptautinius standartus, Aprašo reikalavimus, krašto apsaugos ministro tvirtinamus Techninius informacinių sistemų elektroninės informacijos saugos reikalavimus;

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

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

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

24.13. turi būti vykdomas E. siuntų pristatymo IS naudotojų ir E. siuntų pristatymo IS administratorių atliekamų veiksmų auditas ir naudojami kontrolės reikalavimai;

24.14. tarnybinė stotis, kurioje yra svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus HTTP (angl. *HyperText Transfer Protocol*) protokolo metodus;

24.15. turi būti uždrausta naršyti svetainės kataloguose (angl. *Directory Browsing*).

25. Nešiojamiesiems kompiuteriams ir kitiems mobiliesiems įrenginiams (toliau visi kartu – mobilieji įrenginiai) taikomi tokie patys elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai, kaip ir stacionariesiems kompiuteriams. Papildomos mobiliųjų įrenginių saugumo priemonės:

25.1. leidžiama naudoti mobiliuosius įrenginius, tik atitinkančius elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus, nustatytus Saugos nuostatuose ir E. siuntų pristatymo IS saugos politikos įgyvendinamuosiuose dokumentuose;

25.2. turi būti užtikrinta kompiuterinių laikmenų apsauga. Nevieša informacija, laikoma mobiliuosiuose įrenginiuose, turi būti užšifruota;

25.3. E. siuntų pristatymo IS valdytojas turi turėti teises valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą;

25.4. turi būti tikrinami E. siuntų pristatymo IS naudojami mobilieji įrenginiai, E. siuntų pristatymo IS saugos įgaliotiniui pranešama apie neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius;

25.5. turi būti įdiegiamos operacinės sistemos ir kiti naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

25.6. duomenys, perduodami tarp mobiliojo įrenginio ir E. siuntų pristatymo IS, turi būti šifruojami taikant virtualaus privataus tinklo (angl. VPN) technologiją;

25.7. jungiantis prie E. siuntų pristatymo IS, turi būti patvirtinamas tapatumas. Mobiliajame įrenginyje ar jo taikomojoje programinėje įrangoje turi būti uždrausta išsaugoti slaptažodį.

IV SKYRIUS
REIKALAVIMAI, KELIAMI E. SIUNTŲ PRISTATYMUI IS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

26. E. siuntų pristatymo IS tvarkytojas:

26.1. atsako už prieigos prie programinių, techninių ir kitų išteklių, reikalingų paslaugos teikėjui, teikiančiam E. siuntų pristatymo IS priežiūros paslaugą, suteikimo ir panaikinimo organizavimą;

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

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

27. E. siuntų pristatymo IS administratorius (-iai) supažindina E. siuntų pristatymo IS priežiūros paslaugų teikėją su suteiktos prieigos prie E. siuntų pristatymo IS saugos reikalavimais ir sąlygomis.

28. Pasibaigus sutarties su E. siuntų pristatymo IS priežiūros paslaugos teikėju galiojimo terminui, E. siuntų pristatymo IS tvarkytojas nedelsdamas organizuoja suteiktos prieigos prie E. siuntų pristatymo IS panaikinimą.

29. Perkant paslaugas, darbus ar įrangą, susijusius su E. siuntų pristatymo IS, jų projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi būti nustatoma, kad teikėjas užtikrina atitiktį Apraše nustatytiems reikalavimams. Perkamos paslaugos, darbai ar įranga, susiję su E. siuntų pristatymo IS, turi atitikti teisės aktų ir standartų, kuriais vadovaujamasi užtikrinant E. siuntų pristatymo IS elektroninės informacijos saugą ir kibernetinį saugumą, reikalavimus, kurie iš anksto nustatomi paslaugų teikimo, darbų atlikimo ar įrangos tiekimo pirkimo dokumentuose.

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

31. Teikėjas, vykdydamas sutartinius įsipareigojimus, turi įgyvendinti tinkamas organizacines ir technines priemones, skirtas informacinėms sistemoms ir jose tvarkomai elektroninei informacijai apsaugoti nuo netyčinio ar neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jos.

32. E. siuntų pristatymo IS tvarkytojas su interneto paslaugų teikėju (-ais) turi būti sudaręs sutartis dėl apsaugos nuo E. siuntų pristatymo IS tvarkytojo elektroninių paslaugų

trikdymo taikymo (angl. *Denial of Service*), reagavimo į kibernetinius incidentus įprastomis darbo valandomis, nepertraukiamo interneto paslaugos teikimo ir interneto paslaugos sutrikimų registravimo įprastomis darbo valandomis.

33. Už paslaugų teikimo kontrolę ir saugos priemonių auditą atsakingas E. siuntų pristatymo IS tvarkytojas. Iškilus poreikiui, siekiant įsitikinti, ar tinkamai vykdoma sutartis, laikomasi elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų, informacinių sistemų tvarkytojas turi teisę atlikti paslaugos teikėjo teikiamų paslaugų stebėseną ir auditą, suteikti galimybę atlikti auditą trečiosioms šalims.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

34. Asmenys, pažeidę Taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

PATVIRTINTA
Lietuvos Respublikos susisiekimo
ministro 2020 m. rugsėjo 11 d.
įsakymu Nr. 3-519

NACIONALINĖS ELEKTRONINIŲ SIUNTŲ PRISTATYMO, NAUDOJANT PAŠTO TINKLĄ, INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos veiklos tęstinumo valdymo planas (toliau – Planas) nustato Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos (toliau – E. siuntų pristatymo IS) veiklos tęstinumo organizacines, aprašomąsias ir Plano veiksmingumo išbandymo nuostatas.

2. Plano paskirtis – užtikrinti nepertraukiamą E. siuntų pristatymo IS funkcionavimą.

3. Plane vartojamos sąvokos atitinka sąvokas, vartojamas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo 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 – Aprašas).

4. Planas parengtas vadovaujantis Aprašu, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu ir Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintais Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

5. Planas parengtas E. siuntų pristatymo IS tvarkytojo patalpoms, esančioms V. Kudirkos g. 18, Vilniuje. E. siuntų pristatymo IS komponentų, jeigu jie yra E. siuntų pristatymo IS prieglobos paslaugų teikėjų patalpose, veiklos tęstinumo valdymą ir veiklos atkūrimą reglamentuoja šių paslaugų teikėjų veiklos tęstinumo valdymą reglamentuojantys dokumentai.

6. Planas įsigalioja įvykus elektroninės informacijos saugos ar kibernetiniam incidentui, dėl kurio E. siuntų pristatymo IS tvarkytojai negali teikti E. siuntų pristatymo IS elektroninių paslaugų daliai arba visiems E. siuntų pristatymo IS naudotojams ir būtina atkurti įprastą E. siuntų pristatymo IS veiklą E. siuntų pristatymo IS tvarkytojo patalpose arba atsarginėse patalpose. Plano vykdymą inicijuoja E. siuntų pristatymo IS veiklos tęstinumo valdymo grupės vadovas. Plano nuostatos taip pat taikomos po stichinės nelaimės, avarijos ar kitų ekstremalių situacijų, kai būtina atkurti įprastą E. siuntų pristatymo IS veiklą.

7. E. siuntų pristatymo IS saugos įgaliotinio, asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą (toliau – kibernetinio saugumo vadovas), E. siuntų pristatymo IS administratorių, E. siuntų pristatymo IS išorinių naudotojų funkcijos, įgaliojimai ir veiksmai:

7.1. E. siuntų pristatymo IS saugos įgaliotinis:

7.1.1. bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, elektroninės informacijos saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka E. siuntų pristatymo IS elektroninės informacijos saugos darbo grupės;

7.1.2. duoda privalomus vykdyti nurodymus ir pavedimus E. siuntų pristatymo IS valdytojo ir E. siuntų pristatymo IS tvarkytojo darbuotojams, jeigu tai būtina elektroninės informacijos saugos politikai įgyvendinti;

7.1.3. koordinuoja elektroninės informacijos saugos incidentų tyrimą;

7.2. kibernetinio saugumo vadovas:

7.2.1. bendradarbiauja su kompetentingomis institucijomis, tiriančiomis kibernetinius incidentus, neteisėtas veikas, susijusias su kibernetiniais incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka E. siuntų pristatymo IS kibernetinio saugumo darbo grupė;

7.2.2. koordinuoja kibernetinių incidentų tyrimą;

7.2.3. duoda privalomus vykdyti nurodymus ir pavedimus E. siuntų pristatymo IS valdytojo ir E. siuntų pristatymo IS tvarkytojo darbuotojams, jeigu tai būtina kibernetinio saugumo politikai įgyvendinti;

7.3. E. siuntų pristatymo IS administratorius (-iai):

7.3.1. organizuoja E. siuntų pristatymo IS elektroninio ryšio įrangos funkcionavimo atkūrimą;

7.3.2. organizuoja E. siuntų pristatymo IS duomenų perdavimo tinklo funkcionavimo atkūrimą;

7.3.3. atkuria E. siuntų pristatymo IS tarnybinių stočių veiklą;

7.3.4. organizuoja E. siuntų pristatymo IS duomenų bazės funkcionavimo atkūrimą;

7.3.5. organizuoja E. siuntų pristatymo IS veiklai atkurti reikalingos įrangos įsigijimą;

7.3.6. organizuoja atsargines patalpas, naudojamas E. siuntų pristatymo IS veiklai atkurti;

7.3.7. organizuoja E. siuntų pristatymo IS elektroninės informacijos atkūrimą;

7.3.8. informuoja E. siuntų pristatymo IS išorinius naudotojus apie veiklos sutrikimus ir jų atkūrimo laiką;

7.3.9. vertina E. siuntų pristatymo IS galimą ir padarytą žalą.

8. E. siuntų pristatymo IS veiklos atkūrimas finansuojamas naudojant Lietuvos Respublikos valstybės biudžeto asignavimus (įskaitant Europos Sąjungos fondų lėšas), kurie šiam tikslui skirti Lietuvos Respublikos susisiekimo ministerijai.

9. Planas yra privalomas E. siuntų pristatymo IS valdytojui, E. siuntų pristatymo IS tvarkytojams, E. siuntų pristatymo IS saugos įgaliotiniui, E. siuntų pristatymo IS administratoriams, kibernetinio saugumo vadovui ir E. siuntų pristatymo IS išoriniams naudotojams.

10. E. siuntų pristatymo IS veikla laikoma atkurta, jeigu yra atkuriamas elektroninės informacijos saugos ar kibernetinio incidento (toliau – saugos incidentas) metu sutrikdytas E. siuntų pristatymo IS veikimas, užtikrintas jos duomenų prieinamumas, konfidencialumas ir vientisumas, o E. siuntų pristatymo IS naudotojai gali tvarkyti E. siuntų pristatymo IS elektroninę informaciją. E. siuntų pristatymo IS veikla turi būti atkurta per kuo trumpesnį terminą, kuris neturi būti ilgesnis kaip 16 valandų.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

11. E. siuntų pristatymo IS veiklos tęstinumo valdymo grupę (toliau – VTVG) sudaro:

11.1. E. siuntų pristatymo IS tvarkytojo – valstybės įmonės Registrų centro (toliau – Registrų centras) paslaugų valdymo direktorius (VTVG vadovas);

11.2. VTVG vadovo pavaduotojas – Registrų centro Informacinių technologijų centro direktorius;

11.3. VTVG nariai:

11.3.1. Registrų centro Bendrųjų IS departamento vadovas;

11.3.2. Registrų centro Prevencijos departamento vadovas;

11.3.3. Registrų centro finansų ir administravimo direktorius;

11.3.4. Registrų centro Komunikacijos skyriaus vadovas;

11.3.5. Registrų centro saugos įgaliotinis;

11.3.6. Registrų centro duomenų apsaugos pareigūnas;

11.3.7. Lietuvos Respublikos susisiekimo ministerijos atstovas;

11.3.8. E. siuntų pristatymo IS prieglobos paslaugų teikėjo atstovas, jeigu yra naudojamasi šiomis paslaugomis.

12. VTVG funkcijos:

12.1. situacijos analizė ir sprendimų E. siuntų pristatymo IS veiklos tęstinumo valdymo klausimais priėmimas;

12.2. bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais E. siuntų pristatymo IS veiklos tęstinumo valdymo klausimais;

12.3. bendravimas su kitų institucijų, informacinių sistemų prieglobos paslaugų teikėjų ir kitų organizacijų, susijusių su E. siuntų pristatymo IS, veiklos tęstinumo valdymo grupėmis;

12.4. bendravimas su teisėsaugos ir kitomis institucijomis, institucijų valstybės tarnautojais arba darbuotojais, dirbančiais pagal darbo sutartį, kitomis interesų grupėmis;

12.5. finansinių ir kitų išteklių, reikalingų E. siuntų pristatymo IS veiklai atkurti, įvykus saugos incidentui, naudojimo kontrolė;

12.6. E. siuntų pristatymo IS elektroninės informacijos fizinė sauga, įvykus saugos incidentui;

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

13. E. siuntų pristatymo IS veiklos atkūrimo grupę (toliau – VAG) sudaro:

13.1. Registrų centro IT infrastruktūros departamento vadovas (VAG vadovas);

13.2. VAG vadovo pavaduotojai:

13.2.1. Registrų centro IS valdymo departamento vadovas;

13.2.2. Registrų centro IT infrastruktūros departamento IS aplikacijų priežiūros skyriaus vadovas;

13.3. VAG nariai:

13.3.1. Registrų centro IT infrastruktūros departamento Tarnybinių stočių skyriaus vadovas;

13.3.2. Registrų centro IT infrastruktūros departamento Kompiuterių tinklų priežiūros skyriaus vadovas;

13.3.3. Registrų centro Aptarnavimo departamento vadovas;

13.3.4. Registrų centro Kibernetinės saugos skyriaus vadovas;

13.3.5. Registrų centro Turto valdymo skyriaus vadovas;

13.3.6. E. siuntų pristatymo IS administratoriai;

13.3.7. E. siuntų pristatymo IS priežiūros paslaugų teikėjų atstovai, jei E. siuntų pristatymo IS techninės ir programinės įrangos priežiūros funkcijos perduotos informacinių sistemų priežiūros paslaugų teikėjams Valstybės informacinių išteklių valdymo įstatyme nustatytomis sąlygomis ir tvarka;

13.4. E. siuntų pristatymo IS prieglobos paslaugų teikėjo atstovas.

14. VAG funkcijos:

14.1. E. siuntų pristatymo IS veiklos atkūrimas (E. siuntų pristatymo IS administratoriai), priežiūra ir koordinavimas;

14.2. E. siuntų pristatymo IS tarnybinių stočių veikimo atkūrimas (E. siuntų pristatymo IS administratoriai) ir organizavimas;

14.3. kompiuterių tinklų veikimo atkūrimas (E. siuntų pristatymo IS administratoriai) ir organizavimas;

14.4. E. siuntų pristatymo IS elektroninės informacijos atkūrimas (E. siuntų pristatymo IS administratoriai) ir organizavimas;

14.5. E. siuntų pristatymo IS programinės įrangos tinkamo veikimo atkūrimas (E. siuntų pristatymo IS administratoriai) ir organizavimas.

15. VTVG organizuoja susirinkimą, įvykus esminiams E. siuntų pristatymo IS pokyčiams.

16. VTVG, atlikusi situacijos analizę, susisiekia su VAG ir informuoja apie priimtus sprendimus dėl E. siuntų pristatymo IS veiklos atkūrimo.

17. Tarpusavyje VTVG ir VAG nariai bendrauja asmeniškai, elektroniniu paštu arba mobiliaisiais telefonais.

18. Veiklos atkūrimo detalieji planai pateikiami šio Plano priede.

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

20. VAG vadovas nuolat informuoja VTVG grupės narius apie E. siuntų pristatymo IS veiklos atkūrimo eigą.

21. VTVG ir VAG nariai rengia susitikimus, įvykus esminiams E. siuntų pristatymo IS pokyčiams.

22. Atsarginės patalpos, naudojamos E. siuntų pristatymo IS veiklai atkurti, turi atitikti visus reikalavimus, keliamus pagrindinėms E. siuntų pristatymo IS tarnybinių stočių patalpoms, nurodytus Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių II skyriuje. Atsarginės patalpos, pritaikytos E. siuntų pristatymo IS veiklai atkurti įvykus saugos incidentui, yra Registrų centro patalpos, esančios Tilto g. 17, Vilniuje.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

23. E. siuntų pristatymo IS veiklos tęstinumui užtikrinti turi būti parengti ir saugomi šie dokumentai:

23.1. dokumentas, kuriame nurodyti informacinių technologijų įrangos parametrai ir už šios įrangos priežiūrą atsakingas (-i) E. siuntų pristatymo IS administratorius (-iai), minimalus informacinės sistemos veiklai atkurti, nesant E. siuntų pristatymo IS administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą, reikiamos kompetencijos ar žinių lygis;

23.2. dokumentas, kuriame nurodyta minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos institucijos poreikius atitinkančiai informacinės sistemos veiklai užtikrinti įvykus saugos incidentui, specifikacija;

23.3. dokumentas, kuriame nurodyti kiekvieno pastato, kuriame yra E. siuntų pristatymo IS įranga, aukšto patalpų brėžiniai ir juose pažymėta:

23.3.1. tarnybinės stotys;

23.3.2. kompiuterių tinklų ir telefonų tinklo mazgai;

23.3.3. kompiuterių tinklų ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos;

23.3.4. elektros įvedimo pastate vietos;

23.4. dokumentas, kuriame nurodytos kompiuterių tinklų fizinio ir loginio sujungimo schemos;

23.5. dokumentas, kuriame nurodytos elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys, atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigos;

23.6. dokumentas, kuriame nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

23.7. dokumentas, kuriame nurodytas VTVG ir VAG narių sąrašas su kontaktiniais duomenimis, leidžiančiais susisiekti su šiais asmenimis bet kuriuo metu.

24. Už 23 punkte nurodytų dokumentų saugojimą atsakingi E. siuntų pristatymo IS administratoriai.

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

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

26. Plano veiksmingumo išbandymą inicijuoja E. siuntų pristatymo IS saugos įgaliotinis. Už Plano veiksmingumo išbandymo organizavimą atsakingas Registrų centro Informacinių technologijų centro direktorius.

27. Plano veiksmingumas išbandomas ne rečiau kaip kartą per metus.

28. Išbandžius Plano veiksmingumą, VAG parengia Plano veiksmingumo išbandymo ataskaitą (toliau – ataskaita) ir pateikia ją VTVG. Plano kito išbandymo data nurodoma ataskaitoje.

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

_____

Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos veiklos tęstinumo valdymo plano priedas

NACIONALINĖS ELEKTRONINIŲ SIUNTŲ PRISTATYMO, NAUDOJANT PAŠTO TINKLĄ, INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

1. Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos veiklos atkūrimo detaliajame plane nurodomi veiksmai, reikalingi Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos (toliau – E. siuntų pristatymo IS) veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, jų vykdymo eiliškumas, terminai ir atsakingi vykdytojai.

2. Įsigaliojus E. siuntų pristatymo IS veiklos tęstinumo valdymo planui, E. siuntų pristatymo IS veiklos tęstinumo valdymo grupė (toliau – VTVG) informuoja E. siuntų pristatymo IS išorinius naudotojus, kitus suinteresuotus asmenis apie E. siuntų pristatymo IS veikimo sutrikimus. Informacija teikiama E. siuntų pristatymo IS tvarkytojo – VĮ Registrų centro interneto svetainėje,
E. siuntų pristatymo IS taikomosiose programose, kitomis priemonėmis (pvz., raštu, elektroniniu paštu ir panašiai).

3. Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos veiklos atkūrimo grupė (toliau – VAG) E. siuntų pristatymo IS veiklą atkuria pagal šiuos E. siuntų pristatymo IS funkcijų prioritetus:

3.1. tarnybinių stočių veikimo atkūrimas:

3.1.1. duomenų bazės veikimo atkūrimas;

3.1.2. taikomųjų programų veikimo atkūrimas;

3.2. kompiuterių tinklų veikimo atkūrimas;

3.3. elektroninės informacijos atkūrimas;

3.4. taikomųjų programų veikimo atkūrimas;

3.5. interneto ryšio atkūrimas;

3.6. kompiuterinių darbo vietų veikimo atkūrimas.

4. E. siuntų pristatymo IS veiklos atkūrimo veiksmai, atsižvelgiant į kibernetinio ar elektroninės informacijos saugos incidento tipą ir mastą, veiklos atkūrimo veiksmų pobūdį, turi būti atlikti per kuo trumpesnį terminą, kuris neturi būti ilgesnis kaip 16 valandų. E. siuntų pristatymo IS veiklos atkūrimo veiksmai nurodyti toliau pateiktoje lentelėje:

Situacija	Pirminiai veiksmai	Veiklos atkūrimo veiksmai	Atsakingi vykdytojai
1. Manipuliacija elektronine informacija (pvz., elektroninės informacijos, įskaitant E. siuntų pristatymo IS	1.1. Incidento analizė.	1.1.1. Nustatomas atakos šaltinis, kibernetinio ar elektroninės informacijos saugos incidento padariniai, identifikuojama pakeista, sunaikinta ar kitaip neteisėtai tvarkyta elektroninė informacija. 1.1.2. Stabdomas pažeistos	VAG vadovas

Situacija	Pirminiai veiksmai	Veiklos atkūrimo veiksmai	Atsakingi vykdytojai
programinę įrangą, pakeitimas kita elektronine informacija, elektroninės informacijos iškraipymas, ištrynimas ar kitoks neteisėtas jos naudojimas).		elektroninės informacijos teikimas. 1.1.3. Nustatomos elektroninės informacijos vientisumo pažeidimo, neteisėto tvarkymo priežastys. 1.1.4. Informuojamos kompetentingos institucijos, kitos suinteresuotos šalys.	
	1.2. Veiksmų plano sudarymas.	1.2.1. Sudaromas veiksmų planas manipuliacijos elektronine informacija padariniams likviduoti, E. siuntų pristatymo IS veiklai atkurti ir E. siuntų pristatymo IS apsaugoti.	VTVG vadovas, VAG vadovas
	1.3. Padarinių likvidavimas ir veiklos atkūrimas.	1.3.1. Imamasi veiksmų neteisėtai veikai sustabdyti. 1.3.2. Likviduojami kibernetinio ar elektroninės informacijos saugos incidento padariniai, atkuriamas E. siuntų pristatymo IS veikimas, diegiamos E. siuntų pristatymo IS apsaugos priemonės. 1.3.3. Jeigu E. siuntų pristatymo IS veiklos atkūrimo metu elektroninė informacija atkuriama iš atsarginių kopijų, tikrinama, ar atkurta elektroninė informacija yra teisinga. 1.3.4. Jeigu nėra galimybės tinkamai atkurti elektroninę informaciją iš atsarginių kopijų, E. siuntų pristatymo IS duomenų teikėjų prašoma pateikti elektroninę informaciją iš naujo. 1.3.5. Atkuriamas elektroninės informacijos paslaugų teikimas. 1.3.6. Prireikus veikla atkuriama atsarginėse patalpose.	VAG vadovas
2. Ryšio sutrikimas.	2.1. Ryšio sutrikimo priežasties nustatymas.	2.1.1. Aiškinamasi ryšio sutrikimo priežastis. Jeigu nustatoma, kad ryšys sutriko ne dėl įrangos gedimo, kreipiamasi į ryšio paslaugų teikėją dėl ryšio sutrikimo pašalinimo.	VAG vadovas
	2.2. Ryšio tarnybų informavimas, paklausimo dėl sutrikimo trukmės ir	2.2.1. Priemonių sutrikimams pašalinti nustatymas.	VAG vadovas

Situacija	Pirminiai veiksmai	Veiklos atkūrimo veiksmai	Atsakingi vykdytojai
	pašalinimo prognozės.		
	2.3. Ryšio sutrikimo pašalinimas.	2.3.1. Priemonių įgyvendinimas.	VAG vadovas
3. Kritinės techninės įrangos gedimas, praradimas (pvz., techninis serverio, duomenų saugyklos, tinklo paskirstymo komponento, tinklo sietuvo, tinklo sąsajos, oro kondicionavimo įrangos gedimas, šios įrangos vagystė arba sugadinimas).	3.1. Incidento analizė.	3.1.1. Nustatomas techninės įrangos gedimas, sugadinta ar prarasta techninė įranga.	VAG vadovas
		3.1.2. Nustatomi ir įvertinami įvykio padariniai, žala.	VTVG vadovas
	3.2. Veiksmų plano sudarymas.	3.2.1. Sudaromas veiksmų planas ir, atsižvelgiant į techninės įrangos gedimo, sugadinimo ar praradimo mastą, pasirenkamas optimalus veiklos atkūrimo scenarijus. Galimi veiklos atkūrimo scenarijai: 3.2.1.1. naudoti kitos turimos techninės įrangos išteklius; 3.2.1.2. kreiptis į techninės įrangos garantinių paslaugų teikėją; 3.2.1.3. užsakyti reikalingą techninę įrangą pagal įrangos tiekimo sutartis; 3.2.1.4. vykdyti viešąjį techninės įrangos pirkimą; 3.2.1.5. atkurti veiklą atsarginėse patalpose (naudoti atsarginėse patalpose esančią infrastruktūrą arba šiose patalpose įrengti reikiamą įrangą). 3.2.2. Prireikus numatomas finansinių ir kitokių išteklių poreikis E. siuntų pristatymo IS veiklai atkurti.	VTVG vadovas
	3.3. Padarinių likvidavimas ir veiklos atkūrimas.	3.3.1. E. siuntų pristatymo IS veikla atkuriama pagrindinėse patalpose arba atsarginėse patalpose pagal pasirinktą veiklos atkūrimo scenarijų.	VAG vadovas
4. Stichinė nelaimė, avarija, patalpų praradimas, pažeidimas (pvz., žemės drebėjimas,	4.1. Standartinių veiksmų vykdymas.	4.1.1. Veiksmų, nustatytų E. siuntų pristatymo IS valdytojo, E. siuntų pristatymo IS tvarkytojo valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis (toliau visi kartu – darbuotojai), saugos ir sveikatos	Darbuotojai, kiti asmenys

Situacija	Pirminiai veiksmai	Veiklos atkūrimo veiksmai	Atsakingi vykdytojai
potvynis, gaisras, sprogimas, teroristinis išpuolis, didelio kiekio pavojingųjų medžiagų išsiveržimas į aplinką).		įvadinėse instrukcijose, vykdymas.	
5. Patalpų užgrobimas.	5.1. Teisėsaugos institucijų informavimas.	5.1.1. Apie neteisėtą įsibrovimą į patalpas informuojamos teisėsaugos institucijos. 5.1.2. Galimybių evakuoti darbuotojus nagrinėjimas, jei yra teisėsaugos institucijos nurodymas.	VTVG vadovas
	5.2. Darbuotojų evakavimas, jei yra teisėsaugos institucijų rekomendacija.	5.2.1. Draudimas įeiti į patalpas bet kuriems asmenims, jei yra teisėsaugos institucijos nurodymai. 5.2.2. Darbuotojų informavimas apie evakavimą.	VTVG vadovas
	5.3. Patalpų užrakinimas, jei yra galimybė.	5.3.1. Teisėsaugos institucijų nurodymų vykdymas.	VTVG vadovas
	5.4. Teisėsaugos institucijų kitų nurodymų vykdymas, jei yra rekomendacija.	5.4.1. Darbuotojų informavimas apie nurodymų vykdymą.	VAG vadovas
	5.5. Veiksmai atlaisvinus užgrobtas patalpas.	5.5.1. Padarytos žalos įvertinimas. 5.5.2. Padarytos žalos likvidavimo priemonių plano sudarymas, paskelbimas, darbuotojų instruktavimas ir plano vykdymas.	VTVG vadovas, VAG vadovas
6. Komunalinių paslaugų teikimo sutrikimai (nutrūksta elektros energijos, šildymo, vandens tiekimas).	6.1. Incidento analizė.	6.1.1. Pagal kompetenciją nustatomos galimos komunalinių paslaugų teikimo sutrikimo priežastys. 6.1.2. Informuojami komunalinių paslaugų teikėjai.	Registrų centro Turto valdymo skyriaus vadovas
	6.2. Veiksmų plano sudarymas.	6.2.1. Sudaromas veiksmų planas paslaugų teikimo sutrikimams pašalinti.	VTVG vadovas

Situacija	Pirminiai veiksmai	Veiklos atkūrimo veiksmai	Atsakingi vykdytojai
	6.3. Padarinių likvidavimas ir veiklos atkūrimas.	6.3.1. Organizuojamas komunalinių paslaugų teikimo sutrikimų pagal veiksmų planą šalinimas.	VAG vadovas
7. Darbuotojų praradimas (pvz., nėra darbuotojų, galinčių vykdyti svarbius įstaigos veiklos procesus).	7.1. Incidento analizė.	7.1.1. Nustatoma, kokie žmogiškieji ištekliai, būtini svarbiems procesams vykdyti, yra prarasti. 7.1.2. Nustatoma, kokios kompetencijos darbuotojų reikia svarbiems procesas vykdyti.	Registrų centro Žmogiškųjų išteklių valdymo departamento vadovas
	7.2. Veiklos atkūrimas.	7.2.1. Trūkstamas personalas pakeičiamas pakaitiniais darbuotojais. Prireikus apmokomi esami darbuotojai. 7.2.2. Vykdoma naujų darbuotojų paieška ir atliekamos įdarbinimo procedūros.	Žmogiškųjų išteklių valdymo departamento vadovas

_____

PATVIRTINTA
Lietuvos Respublikos susisiekimo
ministro 2020 m. rugsėjo 11 d.
įsakymu Nr. 3-519

NACIONALINĖS ELEKTRONINIŲ SIUNTŲ PRISTATYMO, NAUDOJANT PAŠTO TINKLĄ, INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos naudotojų administravimo taisyklės (toliau – Taisyklės) nustato Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos (toliau – E. siuntų pristatymo IS) naudotojų įgaliojimus, teises, pareigas ir kontrolės tvarką.

2. Taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu ir Saugos dokumentų turinio gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

3. Taisyklėse vartojamos sąvokos atitinka sąvokas, vartojamas 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“, taip pat Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos nuostatuose, patvirtintuose Lietuvos Respublikos Vyriausybės 2015 m. rugpjūčio 26 d. nutarimu Nr. 914 „Dėl Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos nuostatų patvirtinimo“, taip pat kituose susijusiuose Lietuvos Respublikos įstatymuose ir teisės aktuose.

4. Taisyklės taikomos visiems E. siuntų pristatymo IS išoriniams naudotojams, E. siuntų pristatymo IS administratoriams, E. siuntų pristatymo IS saugos įgaliotiniui (-iams) ir asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą (toliau – kibernetinio saugumo vadovas).

5. E. siuntų pristatymo IS naudotojams prieiga prie E. siuntų pristatymo IS elektroninės informacijos suteikiama vadovaujantis šiais principais:

5.1. E. siuntų pristatymo IS naudotojų prieiga prie elektroninės informacijos grindžiama būtinumo žinoti principu, kuris reiškia, kad E. siuntų pristatymo IS naudotojams suteikiama prieiga tik prie tos E. siuntų pristatymo IS elektroninės informacijos, kuri reikalinga vykdant tiesiogines jų darbo (tarnybos) funkcijas. Tvarkyti E. siuntų pristatymo IS elektroninę informaciją gali tik tie

E. siuntų pristatymo IS naudotojai, kuriems Taisyklių III skyriuje nustatyta tvarka suteiktos prieigos prie E. siuntų pristatymo IS elektroninės informacijos teisės ir priemonės (pvz., identifikavimo priemonės, slaptažodžiai ar kitos autentifikavimo priemonės ir pan.);

5.2. kiekvienas E. siuntų pristatymo IS naudotojas turi būti E. siuntų pristatymo IS unikaliai identifikuojamas (asmens kodas negali būti naudojamas kaip naudotojo identifikatorius);

5.3. E. siuntų pristatymo IS naudotojų prieigos prie E. siuntų pristatymo IS elektroninės informacijos lygis grindžiamas mažiausios privilegijos principu, kuris reiškia, kad turi būti suteikiamos tik minimalios E. siuntų pristatymo IS naudotojų tiesioginėms darbo (tarnybos) funkcijoms vykdyti reikalingos prieigos teisės ir organizacinėmis bei techninėmis priemonėmis užtikrinama minimalių prieigos teisių naudojimo kontrolė (pvz., privilegijuotos prieigos teisės neturi būti naudojamos veiklai, kuriai atlikti pakanka žemesnio lygio prieigos teisių, ir pan.);

5.4. pareigų atskyrimo principas, kuris reiškia, kad E. siuntų pristatymo IS išoriniam naudotojui negali būti pavesta atlikti ar kontroliuoti visų pagrindinių E. siuntų pristatymo IS elektroninės informacijos tvarkymo ar E. siuntų pristatymo IS priežiūros funkcijų (pvz., E. siuntų pristatymo IS išoriniams naudotojams negali būti suteikiamos E. siuntų pristatymo IS administratoriaus teisės, E. siuntų pristatymo IS priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą E. siuntų pristatymo IS administratoriaus paskyrą, kuria naudojantis negalima atlikti kasdienių E. siuntų pristatymo IS išorinio naudotojo funkcijų ir pan.).

II SKYRIUS
E. SIUNTŲ PRISTATYMO IS IŠORINIŲ NAUDOTOJŲ IR E. SIUNTŲ PRISTATYMO IS ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. E. siuntų pristatymo IS išoriniai naudotojai ir E. siuntų pristatymo IS administratoriai privalo rūpintis E. siuntų pristatymo IS ir joje tvarkomos elektroninės informacijos sauga ir kibernetiniu saugumu, tvarkyti elektroninę informaciją vadovaudamiesi E. siuntų pristatymo IS veiklą reglamentuojančiais teisės aktais ir sutartyse nustatytais reikalavimais ir sąlygomis, savo veiksmais nepažeisti elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo.

7. E. siuntų pristatymo IS administratoriai, pastebėję Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos duomenų saugos nuostatuose, patvirtintuose Lietuvos Respublikos susisiekimo ministro 2017 m. sausio 9 d. įsakymu Nr. 3-9 „Dėl Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos duomenų saugos nuostatų patvirtinimo“, ir E. siuntų pristatymo IS saugos politikos įgyvendinamuosiuose dokumentuose (toliau visi kartu – saugos dokumentai) nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos ir (ar) kibernetinio saugumo užtikrinimo priemones, privalo nedelsdami kreiptis į E. siuntų pristatymo IS tvarkytojo – VĮ Registrų centro (toliau – E. siuntų pristatymo IS tvarkytojas) informacinių technologijų pagalbos tarnybą (toliau – informacinių technologijų pagalbos tarnyba).

8. E. siuntų pristatymo IS išoriniai naudotojai, pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos ir (ar) kibernetinio saugumo užtikrinimo priemones, privalo nedelsdami apie tai pranešti E. siuntų pristatymo IS tvarkytojui jo interneto svetainėje nurodytais kontaktais.

9. Jeigu E. siuntų pristatymo IS saugos įgaliotinis nebuvo informuotas apie Taisyklių 7 ir 8 punktuose nurodytus pažeidimus, apie tai jį informuoja informacinių technologijų pagalbos tarnyba. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią E. siuntų pristatymo IS saugą, E. siuntų pristatymo IS saugos įgaliotinis apie tai turi pranešti E. siuntų pristatymo IS valdytojo

vadovui ir kompetentingoms institucijoms, tiriančioms elektroninių ryšių tinklų, elektroninės informacijos saugos incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais.

10. Informacinių technologijų pagalbos tarnyba informuoja ir kibernetinio saugumo vadovą apie Taisyklių 7 ir 8 punktuose nurodytus pažeidimus, susijusius su E. siuntų pristatymo IS kibernetiniu saugumu, jei jis apie tai nebuvo informuotas. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią E. siuntų pristatymo IS kibernetinį saugumą, kibernetinio saugumo vadovas apie tai turi pranešti E. siuntų pristatymo IS valdytojo vadovui ir kompetentingoms institucijoms, tiriančioms kibernetinius incidentus, neteisėtas veikas, susijusias su kibernetiniais incidentais.

11. Kiekvienas E. siuntų pristatymo IS išorinis naudotojas, jungdamasis prie E. siuntų pristatymo IS, privalo atlikti tapatumo nustatymo procedūrą, t. y. patvirtinti tapatybę naudojantis Valstybės informacinių išteklių sąveikumo platformos (toliau – VIISP) priemonėmis arba esant atitinkamam E. siuntų pristatymo IS tvarkytojo ir paslaugų gavėjo rašytiniam susitarimui, per paslaugų gavėjo naudojamą dokumentų valdymo sistemą (ar kitą informacinę sistemą), užtikrinant patikimą tokios dokumentų valdymo sistemos identifikavimą, autentifikaciją ir autorizaciją. VIISP priemonių saugumo (slaptažodžių, jų galiojimo trukmės, keitimo ir saugojimo) reikalavimus nustato VIISP priemonių paslaugų teikėjai.

12. E. siuntų pristatymo IS naudotojai gali naudotis tik tomis E. siuntų pristatymo IS dalimis ir jose apdorojama elektronine informacija, prie kurios prieiga jiems yra nustatyta pagal E. siuntų pristatymo IS naudotojo tipus.

13. E. siuntų pristatymo IS išoriniai naudotojai ir E. siuntų pristatymo IS administratoriai, tvarkantys E. siuntų pristatymo IS elektroninę informaciją, privalo laikytis saugos dokumentuose ir kituose teisės aktuose nustatytų reikalavimų.

14. E. siuntų pristatymo IS išoriniai naudotojai ir E. siuntų pristatymo IS administratoriai privalo užtikrinti E. siuntų pristatymo IS ir joje esančios elektroninės informacijos saugą pagal kompetenciją.

15. Serverių administratoriui ir E. siuntų pristatymo IS administratoriams suteikiama visiška prieiga prie jų funkcijoms atlikti reikalingų E. siuntų pristatymo IS, E. siuntų pristatymo IS išorinių naudotojų duomenų ir visų E. siuntų pristatymo IS dalių valdymo parametrų bei teisė juos skaityti, redaguoti, atnaujinti, kopijuoti ar naikinti, kai tai reikalinga šios sistemos veikimui užtikrinti.

III SKYRIUS
SAUGAUS DUOMENŲ TEIKIMO E. SIUNTŲ PRISTATYMO IS NAUDOTOJAMS KONTROLĖS TVARKA

16. E. siuntų pristatymo IS išorinių naudotojų registravimo ir išregistravimo tvarka:

16.1. E. siuntų pristatymo IS išoriniu naudotoju tampama, kai prisijungiama prie E. siuntų pristatymo IS ir patvirtinama, kad šis naudotojas sutinka su Elektroninio pristatymo paslaugų teikimo Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos priemonėmis taisyklėmis.

16.2. Juridinio asmens elektroninio pristatymo dėžutės savininku tampa asmuo, kuris Juridinių asmenų registre yra įregistruotas juridinio asmens vadovu.

16.3. E. siuntų pristatymo IS naudotojų administratorius įregistruoja E. siuntų pristatymo IS išorinius naudotojus – įgaliotuosius paslaugų gavėjo atstovus, tik gavęs juridinio asmens raštą, kuriame nurodomas įgaliojantis asmuo (juridinio asmens vadovas) ir asmuo, įgaliotas tvarkyti E. siuntų pristatymo IS elektroninio pristatymo dėžutės informaciją. E. siuntų pristatymo IS naudotojų

administratorius turi periodiškai, bet ne rečiau kaip kartą per 3 mėnesius tikrinti, ar nėra nepatvirtintų šiame papunktyje nurodytų E. siuntų pristatymo IS išorinių naudotojų paskyrų, taip pat E. siuntų pristatymo IS vidinių naudotojų – E. siuntų pristatymo IS tvarkytojo darbuotojų paskyrų, ir apie nepatvirtintas paskyras pranešti E. siuntų pristatymo IS tvarkytojo IT pagalbos tarnybai. E. siuntų pristatymo IS išorinius naudotojus – įgaliotuosius paslaugų gavėjo atstovus išregistruoja elektroninio pristatymo dėžutės savininkas.

Papunkčio pakeitimai:
Nr. 3-238, 2021-04-29, paskelbta TAR 2021-04-29, i. k. 2021-09011

16.4. E. siuntų pristatymo IS išorinis naudotojas – elektroninio pristatymo dėžutės savininkas, įgaliotasis paslaugų gavėjo atstovas ar elektroninio pristatymo dėžutės administratorius gali paskirti kitą E. siuntų pristatymo IS išorinį naudotoją – autorizuotą elektroninio pristatymo dėžutės asmenį. E. siuntų pristatymo IS išorinis naudotojas – elektroninio pristatymo dėžutės savininkas turi periodiškai, bet ne rečiau kaip kartą per 3 mėnesius tikrinti, ar nėra nepatvirtintų šame papunktyje nurodytų E. siuntų pristatymo IS išorinių naudotojų paskyrų, ir jas pašalinti.

Papunkčio pakeitimai:
Nr. 3-238, 2021-04-29, paskelbta TAR 2021-04-29, i. k. 2021-09011

16.5. E. siuntų pristatymo IS išorinių naudotojų teisė tvarkyti elektroninę informaciją turi būti panaikinama:

16.5.1. netekus teisės tvarkyti ar administruoti E. siuntų pristatymo IS elektroninę informaciją;

16.5.2. pastebėjus neteisėtą prisijungimo prie E. siuntų pristatymo IS elektroninės informacijos naudojimą;

16.5.3. praradus patikimumą ar įtarus prisijungimo prie E. siuntų pristatymo IS elektroninės informacijos atskleidimą.

16.6. Apie prieigos teisių dirbti su E. siuntų pristatymo IS elektronine informacija panaikinimą E. siuntų pristatymo IS išorinio naudotojo – įgaliotojo paslaugų gavėjo atstovo – juridinio asmens vadovas arba jo įgaliotas asmuo elektroniniu laišku informuoja E. siuntų pristatymo IS naudotojų administratorių paskutinę E. siuntų pristatymo IS išorinio naudotojo – įgaliotojo paslaugų gavėjo atstovo darbo dieną. E. siuntų pristatymo IS naudotojų administratorius, iš juridinio asmens vadovo arba jo įgalioto asmens gavęs rašytinį prašymą apriboti E. siuntų pristatymo IS išorinio naudotojo – įgaliotojo paslaugų gavėjo atstovo prieigos teises, nedelsdamas sustabdo šio E. siuntų pristatymo IS išorinio naudotojo prieigą prie E. siuntų pristatymo IS.

17. E. siuntų pristatymo IS administratorių registravimo ir išregistravimo tvarka:

17.1. E. siuntų pristatymo IS administratoriams prieigos teises suteikia, pakeičia, sustabdo ar panaikina, unikalius prisijungimo E. siuntų pristatymo IS vardus ir pirminius prisijungimo slaptažodžius perduoda E. siuntų pristatymo IS naudotojų administratorius, gavęs E. siuntų pristatymo IS administratoriaus tiesioginio vadovo rašytinį prašymą;

17.2. teisė administruoti E. siuntų pristatymo IS gali būti suteikiama tik įsitikinus, kad E. siuntų pristatymo IS administratorius yra pasirašęs pasižadėjimą saugoti duomenų ir informacijos paslaptį ir pasirašytinai susipažinęs su saugos dokumentais;

17.3. E. siuntų pristatymo IS naudotojų administratorius E. siuntų pristatymo IS administratorių prieigos teises sustabdo nedelsdamas, gavęs už žmogiškųjų išteklių valdymą atsakingo E. siuntų pristatymo IS tvarkytojo struktūrinio padalinio arba kito kompetentingo darbuotojo pateiktą informaciją apie tai, kad teisės aktų nustatytais atvejais E. siuntų pristatymo IS administratorius nušalinamas nuo darbo (pareigų), neatitinka teisės aktuose nustatytų E. siuntų pristatymo IS administratoriaus kvalifikacinių reikalavimų, praranda patikimumą, yra nėštumo ir gimdymo (motinystės) ar vaiko priežiūros atostogose;

17.4. E. siuntų pristatymo IS naudotojų administratorius E. siuntų pristatymo IS administratorių prieigos teises panaikina, gavęs už žmogiškųjų išteklių valdymą atsakingo E. siuntų pristatymo IS tvarkytojo struktūrinio padalinio arba kito kompetentingo darbuotojo pateiktą informaciją apie E. siuntų pristatymo IS administratoriaus darbo (tarnybos) santykių pasibaigimą. E. siuntų pristatymo IS naudotojų administratorius prieigos teises turi panaikinti ne vėliau kaip paskutinę E. siuntų pristatymo IS administratoriaus tarnybos (darbo) dieną, tačiau ne vėliau kaip iki darbo (tarnybos) dienos pabaigos. Priverstinio darbo (tarnybos) santykių nutraukimo atveju ir kitais atvejais, kai yra rizika, kad E. siuntų pristatymo IS administratorius gali atlikti tyčinius veiksmus (pakeisti ar sunaikinti elektroninę informaciją, sutrikdyti elektroninės informacijos perdavimą informacinių technologijų duomenų perdavimo tinklais, pažeisti E. siuntų pristatymo IS saugumą, įvykdyti vagystę ir kita), prieigos teisės turi būti panaikintos nedelsiant;

17.5. tiesioginiai E. siuntų pristatymo IS administratorių vadovai ne rečiau kaip kartą per metus arba keičiantis E. siuntų pristatymo IS administratoriaus pareigoms ar funkcijoms turi peržiūrėti šiems darbuotojams suteiktas teises, įvertinti jų atitiktį vykdomoms funkcijoms. Tiesioginiai E. siuntų pristatymo IS administratorių vadovai turi parengti rašytinį prašymą dėl prieigos teisių E. siuntų pristatymo IS administratoriui pakeitimo, jeigu suteiktos prieigos teisės neatitinka vykdomų funkcijų.

18. E. siuntų pristatymo IS administratorių slaptažodžių, jų sudarymo, galiojimo trukmės ir keitimo bendrieji reikalavimai:

18.1.1. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

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

18.1.3. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;

18.1.4. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pvz., vardas, pavardė, gimimo data, šeimos narių vardai, prisijungimo vardas, gyvenamosios vietos adresas ar jo sudedamosios dalys, telefono numeris ir kita);

18.1.5. draudžiama slaptažodžius atskleisti tretiesiems asmenims;

18.1.6. kilus įtarimui dėl slaptažodžio konfidencialumo pažeidimo, slaptažodis turi būti nedelsiant pakeistas;

18.1.7. E. siuntų pristatymo IS dalys, atliekančios nuotolinio prisijungimo tapatybės nustatymą, turi neleisti išsaugoti slaptažodžių;

18.1.8. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais;

18.1.9. keičiant slaptažodį E. siuntų pristatymo IS dalys neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių tais atvejais, kai E. siuntų pristatymo IS komponentai palaiko tokį funkcionalumą;

18.1.10. draudžiama informacinių sistemų techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti nedelsiant pakeisti ir atitikti informacinių sistemų administratorių slaptažodžiams taikomus reikalavimus.

18.1.11. didžiausias leistinas mėginimų įvesti slaptažodį skaičius turi būti ne didesnis kaip 5 kartai. Viršijus leistiną mėginimų įvesti slaptažodį skaičių, paskyra turi užsirakinti ir neleisti identifikuotis ne trumpiau kaip 15 minučių.

Papildyta papunkčiu:
Nr. 3-238, 2021-04-29, paskelbta TAR 2021-04-29, i. k. 2021-09011

19. E. siuntų pristatymo IS administratorių paskyrų kontrolės priemonės:

19.1. turi būti patvirtinti asmenų, kuriems suteiktos E. siuntų pristatymo IS administratoriaus teisės prisijungti prie E. siuntų pristatymo IS, sąrašai, periodiškai peržiūrimi E. siuntų pristatymo IS saugos administratoriaus. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais

E. siuntų pristatymo IS administratorius nušalinamas nuo darbo (pareigų);

19.2. turi būti periodiškai tikrinama, ar nėra nepatvirtintų E. siuntų pristatymo IS administratorių paskyrų, ir apie nepatvirtintas paskyras pranešama E. siuntų pristatymo IS saugos administratoriui. Apie nepatvirtintas E. siuntų pristatymo IS administratorių paskyras turi būti pranešama nedelsiant;

19.3. nereikalingos ar nenaudojamos E. siuntų pristatymo IS administratorių paskyros turi būti blokuojamos nedelsiant ir ištrinamos praėjus audito duomenų saugojimo terminui, nustatytam Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

20. Nuotolinis prisijungimas prie E. siuntų pristatymo IS turi būti vykdomas protokolu, skirtu elektroninei informacijai šifruoti.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

21. Asmenys, pažeidę Taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.

Pakeitimai:

1.
Lietuvos Respublikos susisiekimo ministerija, Įsakymas
Nr. 3-238, 2021-04-29, paskelbta TAR 2021-04-29, i. k. 2021-09011
Dėl Lietuvos Respublikos susisiekimo ministro 2020 m. rugsėjo 11 d. įsakymo Nr. 3-519 „Dėl Nacionalinės elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinės sistemos saugos politiką įgyvendinančių dokumentų patvirtinimo“ pakeitimo