Suvestinė redakcija nuo 2023-03-01

Įsakymas paskelbtas: TAR 2021-10-15, i. k. 2021-21589

LIETUVOS RESPUBLIKOS TEISINGUMO MINISTRAS

ĮSAKYMAS
DĖL LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJOS INFORMACINIŲ SISTEMŲ SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ PATVIRTINIMO

2021 m. spalio 14 d. Nr. 1R-350
Vilnius

Įgyvendindama 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 punktus, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 5.3 papunktį,

t v i r t i n u pridedamus:

1. Lietuvos Respublikos teisingumo ministerijos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisykles.

2. Lietuvos Respublikos teisingumo ministerijos informacinių sistemų naudotojų administravimo taisykles.

3. Lietuvos Respublikos teisingumo ministerijos informacinių sistemų veiklos tęstinumo valdymo planą.

Teisingumo ministrė Evelina Dobrovolska

SUDERINTA

Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2021-08-02 raštu Nr. (4.1 E) 6K-598

PATVIRTINTA
Lietuvos Respublikos teisingumo ministro
2021 m. spalio 14 d. įsakymu Nr. 1R-350

LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJOS INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos teisingumo ministerijos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato Lietuvos Respublikos teisingumo ministerijos eksploatuojamų informacinių sistemų (toliau – informacinės sistemos) technines ir kitas saugos priemones, saugaus elektroninės informacijos tvarkymo principus ir reikalavimus saugiam informacinių sistemų funkcionavimui užtikrinti.

2. Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos 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“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, ir kituose teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą.

3. Informacinėse sistemose tvarkoma elektroninė informacija nurodyta Lietuvos Respublikos teisingumo ministro patvirtintuose šių informacinių sistemų nuostatuose (aprašuose), elektroninės informacijos svarbos kategorija nurodyta teisingumo ministro patvirtintuose Teisingumo ministerijos informacinių sistemų duomenų saugos nuostatuose (toliau – Saugos nuostatai).

4. Už informacinių sistemų elektroninės informacijos tvarkymą atsakingi Teisingumo ministerijos valstybės tarnautojai ar darbuotojai, dirbantys pagal darbo sutartis, kuriems teisingumo ministro patvirtintų Teisingumo ministerijos informacinių sistemų naudotojų administravimo taisyklių nustatyta tvarka suteikta informacinių sistemų duomenų tvarkymo teisė.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

5. Informacinių sistemų kompiuterinės įrangos saugos užtikrinimo priemonės:

5.1. Visose informacinių sistemų tarnybinėse stotyse ir kompiuterizuotose darbo vietose įdiegta ir reguliariai atnaujinama virusų ir kenkimo kodo aptikimo bei šalinimo programinė įranga, skirta kompiuteriams ir išorinėms laikmenoms tikrinti.

5.2. Kvalifikuoti specialistai, laikydamiesi gamintojo rekomendacijų, atlieka informacinių sistemų kompiuterinės įrangos priežiūrą ir gedimų šalinimą.

5.3. Kompiuterinėje įrangoje naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga, kurios sąrašas peržiūrimas kartą per metus ir prireikus atnaujinamas.

5.4. Patalpose, kuriose yra techninė įranga, užtikrintos gamintojo nustatytos techninės įrangos veikimo sąlygos, įranga prižiūrima ir eksploatuojama pagal gamintojo rekomendacijas.

5.5. Informacinių sistemų kompiuterinės įrangos diegimą, keitimą ir gedimų šalinimą atlieka informacinių sistemų valdytojo vadovo įgalioti kvalifikuoti Teisingumo ministerijos darbuotojai arba informacinių technologijų paslaugas pagal sutartį teikiančios įmonės specialistai.

5.6. Iš kompiuterinės įrangos, perduotos remontui ar techninei priežiūrai, turi būti pašalinta visa riboto naudojimo elektroninė informacija.

5.7. Pagrindinė informacinių sistemų kompiuterinė įranga turi turėti įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį kompiuterinės įrangos veikimą ir apsaugantį nuo elektros srovės svyravimų.

5.8. Kompiuterinė aparatinė įranga turi būti apsaugota nuo neteisėtos prieigos, jos sugadinimo ar neteisėto poveikio.

6. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

6.1. Naudojama tik legali, autorizuota ir saugi sisteminė ir taikomoji programinė įranga.

6.2. Programinės įrangos priežiūrą ir gedimų šalinimą atlieka kvalifikuoti specialistai.

6.3. Programinės įrangos konfigūravimas yra apsaugotas slaptažodžiu.

6.4. Informacinių sistemų naudotojų ir administratorių kompiuterinėje įrangoje turi būti naudojama tik darbo funkcijoms atlikti reikalinga programinė įranga (informacinių sistemų komponentų administratoriai ne rečiau kaip kartą per metus peržiūri ir prireikus atnaujina leistinos programinės įrangos sąrašą).

6.5. Informacinių sistemų tarnybinėse stotyse ir naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, stebėjimo realiu laiku priemonės. Šios priemonės automatiškai turi informuoti informacinių sistemų komponentų administratorių apie tai, kurių informacinių sistemų posistemių, funkciškai savarankiškų sudedamųjų dalių kenkimo programinės įrangos aptikimo priemonių atsinaujinimo laikas yra pradelstas. Informacinių sistemų komponentai be kenkimo programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu vertinant riziką patvirtinama, kad šių komponentų rizika yra priimtina.

6.6. Turi būti operatyviai testuojami ir įdiegiami informacinių sistemų tarnybinių stočių ir naudotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos programinės įrangos gamintojų rekomenduojami atnaujinimai. Informacinių sistemų komponentų administratoriai reguliariai, bet ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie informacinių sistemų posistemiams, funkciškai savarankiškoms sudedamosioms dalims, naudotojų darbo vietų kompiuterinei įrangai neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumų svarbos lygius.

6.7. Informacinių sistemų sisteminės ir taikomosios programinės įrangos apsaugai nuo virusų ir kitų kenkimo programų naudojama specializuota, nuolat automatiškai atnaujinama antivirusinė programinė įranga.

6.8. Taikomos programinės priemonės naudotojų ir administratorių tapatybei ir jų veiksmams nustatyti.

6.9. Informacinių sistemų naudotojų ir administratorių slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai nustatyti teisingumo ministro patvirtintose Teisingumo ministerijos informacinių sistemų naudotojų administravimo taisyklėse.

7. Duomenų perdavimo tinklais saugos 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 naudojant užkardas. Pagrindinėse informacinių sistemų tarnybinėse stotyse turi būti įjungtos užkardos, sukonfigūruotos praleisti tik su informacinių sistemų funkcionalumu ir administravimu susijusį duomenų srautą.

7.2. Užkardos žurnalai (angl. *Logs*) turi būti reguliariai analizuojami, o užkardos saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos.

7.3. Informacinių sistemų elektroninės informacijos perdavimo tinklas yra segmentuotas pagal informacinių sistemų sudedamųjų dalių atliekamas funkcijas ir turi priskirtus IP adresų intervalus:

7.3.1. Paslaugų tarnybinių stočių tinklas turi būti skirtas taikomųjų programų tarnybinėms stotims.

7.3.2. Informacinių sistemų kompiuterizuotų darbo vietų tinklai turi būti skirti nutolusių informacinių sistemų naudotojų kompiuterinėms darbo vietoms ir kompiuterinei įrangai.

7.3.3. Informacinių sistemų kūrimo, tobulinimo ir testavimo tinklas turi būti skirtas naudojamoms tarnybinėms stotims ir duomenų bazių testavimo tarnybinėms stotims testuoti.

7.3.4. Administratorių tinklas turi būti skirtas darbuotojų, turinčių informacinių sistemų ir (ar) tarnybinių stočių administratoriaus teises, kompiuterizuotoms darbo vietoms.

7.3.5. Informacinių sistemų elektroninės informacijos perdavimo tinklo priežiūros ir saugumo potinklis turi būti skirtas tinklo stebėjimo, priežiūros, antivirusinių sistemų tarnybinėms stotims.

7.4. Nutolę informacinių sistemų naudotojai turi perduoti informaciją naudodami saugias ryšio linijas.

7.5. Informacinėms sistemoms turi būti taikomas elektroninės informacijos perdavimo tinklo trijų lygių saugumas – išorinio perdavimo tinklo, taikomųjų programų, duomenų bazių, kiekvieną iš lygių atskiriant užkarda.

7.6. Jungimasis prie informacinių sistemų iš viešųjų telekomunikacinių tinklų turi būti griežtai kontroliuojamas ir atliekamas tik per tarpines tarnybines stotis.

7.7. Keitimasis informacija su kitais registrais ir informacinėmis sistemomis galimas tik naudojant saugius šifruotus ryšio kanalus (VPN, SSL) ir (ar) tarpines tarnybines stotis.

7.8. Informacinių sistemų tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešajame ryšių tinkle naršančių informacinių sistemų naudotojų kompiuterinę įrangą nuo kenkimo kodo.

8. Elektroninės informacijos perdavimo tinklais saugos užtikrinimo priemonės:

8.1. Siekiant užtikrinti informacinėse sistemose saugomos ir apdorojamos elektroninės informacijos konfidencialumą ir vientisumą, šios informacijos teikimas bei priėmimas turi būti vykdomi naudojant saugų valstybinį duomenų perdavimo tinklą, šifravimą ir kitas saugos užtikrinimo priemones.

8.2. Informacinių sistemų naudotojų tapatybei nustatyti ir tiesioginei prieigai prie informacinių sistemų elektroninės informacijos kontroliuoti turi būti naudojama prisijungimo vardų, slaptažodžių ir naudotojų prieigos teisių sistema.

8.3. Prisijungimo prie informacinių sistemų vardai ir pirminiai slaptažodžiai turi būti žinomi tik informacinių sistemų komponentų administratoriams, kurie juos suteikia konkrečiam informacinių sistemų naudotojui ar administratoriui.

8.4. Informacinių sistemų tarnybinės stotys nuo interneto grėsmių turi būti apsaugotos užkardomis.

8.5. Mobiliųjų įrenginių, naudojamų prisijungti prie informacinių sistemų, sauga ir kontrolė:

8.5.1. Leidžiama naudoti tik leistinus mobiliuosius įrenginius, atitinkančius informacinių sistemų valdytojo nustatytus saugos reikalavimus.

8.5.2. Turi būti tikrinami naudojami mobilieji įrenginiai. Už mobiliųjų įrenginių tikrinimą yra atsakingi informacinių sistemų saugos administratoriai, kurie praneša asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą Teisingumo ministerijoje (toliau – asmuo, atsakingas už kibernetinį saugumą), apie neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius.

8.5.3. Turi būti įdiegiamos operacinės sistemos ir kiti naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai.

8.5.4. Jungiantis prie informacinių sistemų, turi būti patvirtinamas tapatumas.

8.5.5. Turi būti užtikrinta kompiuterinių laikmenų apsauga.

8.6. Belaidžio tinklo sauga ir kontrolė:

8.6.1. Leidžiama naudoti tik su informacinių sistemų saugos administratoriais suderintus belaidžio tinklo įrenginius, atitinkančius techninius kibernetinio saugumo reikalavimus.

8.6.2. Jei eksploatuojami belaidžiai įrenginiai, asmeniui, atsakingam už kibernetinį saugumą, elektroninėmis ryšio priemonėmis pranešama apie neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius.

8.6.3. Belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, kontroliuojamoje zonoje.

8.6.4. Prisijungiant prie belaidžio tinklo, turi būti taikomas naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas.

8.6.5. Turi būti uždrausta belaidėje sąsajoje naudoti SNMP (angl. *Simple Network Management Protocol*) protokolą.

8.6.6. Turi būti uždrausti visi nebūtini valdymo protokolai.

8.6.7. Turi būti išjungti nenaudojami TCP (angl. *Transmission Control Protocol*) / UDP (angl. *User Datagram Protocol*) prievadai.

8.6.8. Turi būti uždraustas lygiarangių (angl. *peer to peer*) funkcionalumas, neleidžiantis belaidžiais įrenginiais tarpusavyje palaikyti ryšio.

8.6.9. Belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu.

8.6.10. Prieš pradedant šifruoti belaidį ryšį, belaidės prieigos stotelėje turi būti pakeisti standartiniai gamintojo raktai.

9. Patalpų ir aplinkos saugos užtikrinimo priemonės:

9.1. Pastate, kuriame yra informacinių sistemų tarnybinių stočių patalpos, turi būti apsaugos darbuotojas.

9.2. Informacinių sistemų tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas. Šios patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų, į šias patalpas gali patekti tik įgalioti asmenys, o kiti asmenys į jas gali patekti tik lydimi įgalioto asmens.

9.3. Tarnybinių stočių patalpose turi būti įrengtos priešgaisrinės signalizacijos ir automatinės gaisro gesinimo sistemos, turi būti ugnies gesintuvai ir speciali gesinimo įranga, įrengti gaisro ir įsilaužimo davikliai, nustatoma įeinančių į patalpas ir išeinančių iš jų asmenų tapatybė. Gaisro ir įsilaužimo davikliai turi būti prijungti prie pastato signalizacijos ir apsaugos tarnybų stebėjimo pulto.

9.4. Tarnybinių stočių patalpose turi būti įrengtos nedegios, metalinės ir visada rakinamos durys, visos išorinės durys ir langai tarnybinių stočių patalpose turi būti apsaugoti taip, kad niekas į jas nepatektų.

9.5. Patalpos turi atitikti priešgaisrinės saugos reikalavimus, jose turi būti gaisro gesinimo priemonės ir periodiškai atliekama gaisro gesinimo priemonių patikra.

9.6. Jei informacinių sistemų tarnybinių stočių patalpose esančios įrangos bendras galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga.

9.7. Ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo ar pažeidimo.

9.8. Papildoma informacinių sistemų naudojamų interneto svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, sauga ir kontrolė:

9.8.1. Atliekant svetainės administravimo darbus, ryšys turi būti šifruojamas naudojant ne trumpesnį kaip 128 bitų raktą.

9.8.2. Kriptografiniai raktai ir algoritmai turi būti valdomi pagal informacinių sistemų valdytojo reikalavimus.

9.8.3. Draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių) pasibaigus susijungimo sesijai.

9.8.4. Tarnybinė stotis, kurioje yra svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus HTTP metodus.

9.8.5. Turi būti uždrausta naršyti svetainės aplankuose (angl. *Directory browsing*).

10. Kitos elektroninės informacijos saugos užtikrinimo priemonės:

10.1. Informacinėse sistemose turi būti įrašomi ir 6 mėn. saugomi duomenys apie informacinių sistemų tarnybinių stočių, taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinių sistemų tarnybinėse stotyse, taikomojoje programinėje įrangoje, visus informacinių sistemų naudotojų vykdomus veiksmus, kitus elektroninės informacijos saugai svarbius įvykius, nurodant informacinių sistemų naudotojo identifikatorių ir elektroninės informacijos saugai svarbaus įvykio ar vykdyto veiksmo laiką. Šie duomenys turi būti saugomi ne toje pačioje informacinėje sistemoje, kurioje jie įrašomi, taip pat jie turi būti analizuojami ne rečiau kaip kartą per savaitę.

10.2. Turi būti užtikrintas informacinių sistemų prieinamumas ne mažiau kaip 70 proc. laiko darbo metu darbo dienomis per metus.

10.3. Turi būti užtikrintas ne ilgesnis nei 24 val. informacinių sistemų neveikimo laikotarpis.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

11. Saugaus elektroninės informacijos įrašymo, keitimo, atnaujinimo ir naikinimo užtikrinimo tvarka:

11.1. Informacinių sistemų duomenis įrašyti, keisti, atnaujinti ir naikinti gali tik tokią teisę turintys informacinių sistemų naudotojai.

11.2. Informacinių sistemos duomenys įvedami, atnaujinami, keičiami ir naikinami vadovaujantis informacinių sistemų nuostatais (aprašais), Saugos nuostatais ir kitais teisės aktais, reglamentuojančiais informacinių sistemų elektroninės informacijos tvarkymą.

11.3. Baigus darbą ar pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: turi būti atsijungiama nuo informacinių sistemų, įjungiama ekrano užsklanda su slaptažodžiu.

11.4. Informacinių sistemų naudotojams neatliekant jokių veiksmų informacinėse sistemose ilgiau nei 15 min., informacinių sistemų taikomoji programinė įranga turi užsirakinti, kad toliau naudotis informacinėmis sistemomis galima būtų tik pakartotinai patvirtinus savo tapatybę. Šis reikalavimas netaikomas, jeigu, atlikus informacinių sistemų rizikos vertinimą, nustatomos kitos nustatytą riziką atitinkančios techninės kibernetinio saugumo priemonės.

12. Informacinių sistemų naudotojų ir administratorių veiksmų registravimo tvarka:

12.1. Informacinių sistemų naudotojų ir administratorių veiksmai su informacinių sistemų duomenimis automatiniu būdu turi būti įrašomi informacinių sistemų duomenų bazės įvykių žurnale, apsaugotame nuo neteisėto jame esančių duomenų panaudojimo, pakeitimo, iškraipymo ir sunaikinimo.

12.2. Duomenų bazės įvykių žurnalo duomenys prieinami informacinių sistemų administratoriams.

13. Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka:

13.1. Saugos nuostatų nustatyta tvarka turi būti daromos atsarginės elektroninės informacijos kopijos (toliau – kopijos), kurios turi būti saugomos kitose patalpose, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate.

13.2. Kopijos laikomos kitose patalpose, nei yra informacinių sistemų tarnybinės stotys.

13.3. Už informacinėse sistemose tvarkomų duomenų kopijų darymą yra atsakingi informacinių sistemų komponentų administratoriai.

13.4. Kopijos daromos automatiškai kiekvieną dieną. Visų duomenų kopija daroma kartą per 24 val.

13.5. Elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų siekiant neteisėtai atkurti elektroninę informaciją.

13.6. Prarasti, iškraipyti, sunaikinti informacinėse sistemose tvarkomi duomenys atkuriami iš kopijų.

13.7. Ne rečiau kaip vieną kartą per metus atliekami elektroninės informacijos atkūrimo iš kopijų bandymai.

14. Saugaus elektroninės informacijos perkėlimo ir teikimo susijusioms informacinėms sistemoms, elektroninės informacijos gavimo iš jų užtikrinimo tvarka:

14.1. Už iš valstybės registrų bei kitų susijusių informacinių sistemų teikiamų duomenų atnaujinimą informacinėse sistemose yra atsakingas informacinių sistemų komponentų administratorius.

14.2. Informacinių sistemų elektroninė informacija teikiama tik teisės aktuose nustatytais atvejais.

14.3. Duomenų mainai su kitomis informacinėmis sistemomis ar valstybės registrais vykdomi pagal su šių informacinių sistemų (registrų) valdytojais ar tvarkytojais sudarytose duomenų teikimo sutartyse nustatytas sąlygas.

14.4. Informacinių sistemų elektroninė informacija, įskaitant asmens duomenis, vadovaujantis Valstybės informacinių išteklių valdymo įstatymu ir 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 (Bendrasis duomenų apsaugos reglamentas), teikiama ir gaunama:

14.4.1. leidžiamosios kreipties būdu internetu;

14.4.2. automatiniu būdu elektroninių ryšių tinklais;

14.4.3. kitais informacinių sistemų nuostatuose (aprašuose) nustatytais būdais ir formomis.

15. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

15.1. Informacinių sistemų saugos administratorius, užtikrindamas informacinių sistemų duomenų vientisumą, privalo naudoti visas įmanomas programines ir administracines priemones, skirtas informacinėse sistemose tvarkomai elektroninei informacijai nuo neteisėtų veiksmų apsaugoti.

15.2. Informacinių sistemų duomenų saugos pažeidimo, neleistinos arba nusikalstamos veikos požymių, neveikiančios arba netinkamai veikiančios duomenų saugą užtikrinančios priemonės registravimas apibrėžtas teisingumo ministro tvirtinamose Teisingumo ministerijos informacinių sistemų naudotojų administravimo taisyklėse.

15.3. Informacinių sistemų naudotojas, įtaręs, kad su informacinių sistemų duomenimis buvo atlikti neteisėti veiksmai, apie tai turi pranešti informacinių sistemų saugos įgaliotiniui ir informacinių sistemų saugos administratoriui.

15.4. Saugos įgaliotinis, gavęs pranešimą apie vykdomus neteisėtus veiksmus su informacinėse sistemose tvarkoma elektronine informacija, inicijuoja elektroninės informacijos saugos incidento valdymo procedūras, detalizuotas Informacinių sistemų veiklos tęstinumo plane.

16. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

16.1. Kiekvienų metų ketvirtąjį ketvirtį informacinių sistemų komponentų administratorius rengia ateinančių metų programinės ir techninės įrangos keitimo ir atnaujinimo darbų planą.

16.2. Atnaujinama ar keičiama programinė ir techninė įranga turi būti testuojama.

16.3. Turi būti įvertinamas informacinių sistemų programinės ir techninės įrangos keitimo ir atnaujinimo poveikis informacinių sistemų saugai.

16.4. Su informacija apie planuojamus atlikti programinės ir techninės įrangos atnaujinimus ar keitimus informacinių sistemų komponentų administratorius turi supažindinti saugos įgaliotinį, visus naudotojus, paslaugų teikėjus.

17. Informacinių sistemų pokyčių valdymo tvarka:

17.1. Pokyčius turi teisę inicijuoti saugos įgaliotinis, informacinių sistemų komponentų administratorius ir informacinių sistemų naudotojas, o įgyvendinti – informacinių sistemų komponentų administratorius. Visi pokyčiai, galintys sutrikdyti ar sustabdyti informacinių sistemų darbą, turi būti suderinti su informacinių sistemų valdytojo vadovu ar jo įgaliotu asmeniu.

17.2. Informacinių sistemų komponentų administratorius užtikrina, kad pokyčiai būtų sparčiai identifikuojami ir suskirstomi į kategorijas, įvertina jų įtaką informacinėms sistemoms ir nustato prioritetus.

17.3. Pokyčiai, galintys turėti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti testavimo aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri yra atskirta nuo eksploatuojamų informacinių sistemų.

17.4. Prieš atlikdamas esminius pokyčius, kurių metu galimi informacinių sistemų veikimo sutrikimai, informacinių sistemų administratorius privalo ne vėliau kaip prieš vieną darbo dieną iki planuojamų pokyčių vykdymo pradžios informuoti (elektroniniu paštu ar kitomis priemonėmis) informacinių sistemų naudotojus apie tokių darbų pradžią ir galimus sutrikimus.

17.5. Atlikęs informacinių sistemų pokyčių testavimą arba jeigu dėl programinių ir (ar) techninių priežasčių nebuvo galima jo atlikti, informacinių sistemų administratorius gali pradėti inicijuoti ir įgyvendinti pokyčius.

17.6. Visi pokyčiai turi būti registruojami informacinių sistemų pokyčių žurnale, kurio forma patvirtinta šių Taisyklių priede.

17.7. Informacinių sistemų valdytojo vadovas užtikrina pokyčių valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas, atsižvelgdamas į pokyčių svarbą, aktualumą, poreikį, įtakos vertinimą, pokyčių prioritetų nustatymo procesus.

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINIŲ SISTEMŲ FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

18. Perkant paslaugas, darbus ar įrangą, susijusius su informacinėmis sistemomis, pirkimo dokumentuose iš anksto nustatoma, kad paslaugų teikėjas turi užtikrinti atitiktį kibernetinio saugumo reikalavimams, nustatytiems Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

19. Reikalavimai, keliami informacinių sistemų funkcionavimui reikalingoms paslaugoms ir jų tiekėjams, nustatomi paslaugų teikimo sutartyse.

20. Paslaugų teikėjams, kurie teikia paslaugas, susijusias su informacinių sistemų funkcionalumo užtikrinimu, yra suteikiama tokia prieiga prie informacinių sistemų, kuri yra būtina norint įvykdyti paslaugų teikimo sutartyje nustatytus įsipareigojimus ir kuri neprieštarauja įstatymų ir kitų teisės aktų reikalavimams.

21. Paslaugų teikimo sutartyse, susijusiose su informacinių sistemų funkcionalumo užtikrinimu, turi būti nurodyta:

21.1. paslaugų teikėjų prieigos prie informacinių sistemų lygiai ir sąlygos;

21.2. reikalavimai, keliami paslaugų teikėjų patalpoms, įrangai, informacinių sistemų priežiūrai, duomenų perdavimui tinklais ir kitoms paslaugoms.

22. Pasibaigus sutarties su paslaugų teikėjais galiojimo terminui ar atsiradus paslaugų teikimo sutartyje ar saugos politikos įgyvendinamuosiuose dokumentuose įvardytų kitų sąlygų, informacinių sistemų administratorius nedelsdamas privalo panaikinti paslaugų teikėjams suteiktą prieigą.

23. Už programinių, techninių ir kitų prieigos prie informacinės sistemos išteklių priemonių organizavimą, suteikimą paslaugų teikėjui ir panaikinimą atsakingas informacinių sistemų komponentų administratorius.

_____

Lietuvos Respublikos teisingumo ministerijos
informacinių sistemų saugaus elektroninės
informacijos tvarkymo taisyklių
priedas

(Informacinių sistemų pokyčių žurnalo forma)

INFORMACINIŲ SISTEMŲ POKYČIŲ ŽURNALAS

Eil. Nr.	**Data**	**Virtuali mašina ar kita kompiuterių tinklo įranga (pavadinimas, IP adresas)**	**Informacinių sistemų pokyčio aprašymas**	**Informacinių sistemų pokytį atlikęs darbuotojas (vardas, pavardė)**	**Pastabos**
1.					
2.					
3.					
4.					
5.					
6.					
7.					

_____

PATVIRTINTA
Lietuvos Respublikos teisingumo ministro
2021 m. spalio 14 d. įsakymu Nr. 1R-350

LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJOS INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos teisingumo ministerijos informacinių sistemų naudotojų administravimo taisyklės (toliau – Taisyklės) nustato Lietuvos Respublikos teisingumo ministerijos eksploatuojamų informacinių sistemų (toliau – informacinės sistemos) naudotojų, komponentų ar saugos administratorių (toliau kartu – administratoriai) įgaliojimus, teises ir pareigas, saugaus elektroninės informacijos teikimo informacinių sistemų naudotojams kontrolės tvarką.

2. Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos 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“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, ir kituose teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą.

3. Taisyklių tikslas – sudaryti tinkamas sąlygas saugiai tvarkyti elektroninę informaciją automatiniu būdu.

4. Taisyklės taikomos informacinių sistemų valdytojui, administratoriams, naudotojams, asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą Teisingumo ministerijoje (toliau – asmuo, atsakingas už kibernetinį saugumą), ir saugos įgaliotiniui.

5. Naudotojams prieiga prie informacinių sistemų elektroninės informacijos suteikiama vadovaujantis šiais prieinamumo prie elektroninės informacijos principais:

5.1. Prieigos prie informacinių sistemų teisė naudotojams suteikiama tik tuo atveju, jei jiems pavesta tvarkyti informacinių sistemų elektroninę informaciją arba jiems numatytoms funkcijoms vykdyti būtina naudotis informacinių sistemų elektronine informacija.

5.2. Naudotojams negali būti suteikiamos informacinių sistemų saugos administratoriaus teisės.

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

5.4. Prieiga prie informacinėse sistemose saugomos elektroninės informacijos ir teisė ją keisti suteikiama tik identifikavus naudotoją ir patvirtinus jo tapatybę slaptažodžiu.

5.5. Kiekvienas naudotojas turi būti unikaliai identifikuojamas (asmens kodas negali būti naudojamas naudotojui identifikuoti).

II SKYRIUS
NAUDOTOJŲ IR INFORMACINIŲ SISTEMŲ ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. Naudotojai rinkdami, tvarkydami, perduodami, saugodami, naikindami ar kitaip naudodami elektroninę informaciją gali naudotis tik tais informacinių sistemų posistemiais ir juose tvarkoma elektronine informacija, prie kurios prieigą jiems suteikė informacinių sistemų naudotojų administratoriai.

7. Naudotojai, vadovaudamiesi Taisyklėse apibrėžtais reikalavimais, privalo užtikrinti jų naudojamo informacinių sistemų posistemio ir jame tvarkomos elektroninės informacijos konfidencialumą, vientisumą ir pasiekiamumą.

8. Naudotojai negali keisti jiems suteiktų prieigos prie duomenų ir priskirtos naudotojų grupės teisių.

9. Su asmens duomenimis galima atlikti tik tuos veiksmus ir tik tais tikslais, kuriais naudotojui yra suteiktos teisės. Naudotojai asmens duomenis gali tvarkyti tik su vykdomomis funkcijomis ir pavedimais (užduotimis) susijusiais tikslais.

10. Administratorių prieigos prie informacinių sistemų lygiai ir juose taikomi saugos reikalavimai nustatomi atsižvelgiant į administratorių atliekamas funkcijas:

10.1. Informacinių sistemų naudotojų administratoriams suteikiama prieiga prie informacinių sistemų naudotojų prieigos teisių valdymo sistemų.

10.2. Informacinių sistemų komponentų administratoriams pagal kompetenciją suteikiama prieiga prie kompiuterių, operacinių sistemų, duomenų bazių ir jų valdymo sistemų, taikomųjų programų sistemų, užkardų, įsilaužimų aptikimo ir prevencijos sistemų, elektroninės informacijos perdavimo tinklų, duomenų saugyklų, bylų serverių ir kitos techninės ir programinės įrangos bei jų sąrankos.

10.3. Informacinių sistemų saugos administratoriams suteikiama prieiga prie informacinių sistemų pažeidžiamumų skenavimo, informacinių sistemų stebėsenos ir saugos atitikties nustatymo ir įvertinimo, saugos informacijos ir įvykių stebėjimo, apsaugos nuo elektroninės informacijos nutekinimo priemonių, kitos saugos užtikrinimo įrangos ir kitų priemonių, kuriomis atliekamas informacinių sistemų pažeidžiamų vietų nustatymas, saugos reikalavimų atitikties nustatymas ir stebėsena. Informacinių sistemų saugos administratoriai turi teisę gauti prieigą ir prie kitų informacinių sistemų komponentų, jeigu tai būtina jų funkcijoms, susijusioms su saugos reikalavimų atitikties nustatymu ir stebėsena, atlikti.

11. Informacinių sistemų komponentų ir saugos administratoriai informacinių sistemų komponentus gali pasiekti naudodamiesi tiesiogine, vietinio tinklo arba nuotoline prieiga. Informacinių sistemų administratorių prieiga ir jos lygiai kontroliuojami per fizinius (įeigos kontrolės sistemos, barjerai ir kita) ir loginius (užkardos, domeno valdikliai ir kita) prieigos taškus. Kontrolės priemonės turi būti taikomos visuose informacinių sistemų sandaros sluoksniuose (kompiuterių tinklas, platformos ar operacinės sistemos, duomenų bazės ir taikomųjų programų sistemos).

12. Naudotojų ir informacinių sistemų administratorių veiksmai, įvykus elektroninės informacijos saugos (kibernetiniam) incidentui, nustatomi Lietuvos Respublikos teisingumo ministro tvirtinamame Teisingumo ministerijos informacinių sistemų veiklos tęstinumo valdymo plane.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO INFORMACINIŲ SISTEMŲ NAUDOTOJAMS KONTROLĖS TVARKA

13. Teisingumo ministerijos darbuotojui, atsakingam už personalo administravimą, pateikus informacinių sistemų naudotojų administratoriui informaciją apie darbuotojo priėmimą į darbą, administratorius per tris darbo dienas sukuria naudotojo kompiuterinę kortelę. Atsižvelgiant į darbuotojo pareigybę, suteikiamos prieigos prie elektroninės informacijos teisės.

14. Teisingumo ministerijos darbuotojui, atsakingam už personalo administravimą, pateikus informacinių sistemų naudotojų administratoriui informaciją apie pasikeitusias darbuotojo funkcijas, administratorius nedelsdamas, bet ne vėliau kaip per vieną darbo dieną, turi peržiūrėti darbuotojo prieigos prie informacinių sistemų elektroninės informacijos teises. Naudotojui turi būti paliekamos teisės, būtinos pareigybės aprašyme nustatytoms funkcijoms ir (ar) gautiems pavedimams (užduotims) vykdyti.

15. Informacinių sistemų naudotojų administratorius, gavęs iš Teisingumo ministerijos darbuotojo, atsakingo už personalo administravimą, informaciją apie darbuotojo atleidimą iš darbo, darbuotojo atleidimo dieną deaktyvuoja naudotojo kompiuterinę kortelę ir panaikina prieigos prie elektroninės informacijos teises.

16. Naudotojų prieiga prie informacinių sistemų duomenų realizuojama tik per naudotojų identifikavimo ir slaptažodžių sistemą.

17. Kiekvienam naudotojui suteikiamas naudotojo vardas ir slaptažodis.

18. Reikalavimai, keliami prisijungimo prie visų kategorijų informacinių sistemų slaptažodžiams:

18.1. Slaptažodis turi būti sudarytas iš tam tikro skaičiaus simbolių, tarp kurių privalo būti bent po vieną simbolį iš šių trijų kategorijų: didžiosios raidės, mažosios raidės, skaitmenys ir specialieji simboliai.

18.2. Slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pvz., gimimo data, šeimos narių vardai ir pan.).

18.3. Draudžiama slaptažodžius atskleisti tretiesiems asmenims.

18.4. Informacinių sistemų dalys, atliekančios nutolusio prisijungimo autentifikavimą, turi drausti automatiškai išsaugoti slaptažodžius.

18.5. Didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius turi būti ne didesnis nei 5 kartai. Neteisingai įvedus didžiausią leistiną slaptažodžių skaičių, informacinė sistema turi užsirakinti ir neleisti informacinės sistemos naudotojui identifikuotis ne trumpiau nei 15 minučių.

18.6. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais. Saugos įgaliotinio sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jei:

18.6.1. informacinės sistemos naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio;

18.6.2. nėra techninių galimybių informacinės sistemos naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

19. Papildomi naudotojų slaptažodžių reikalavimai:

19.1. Slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius.

19.2. Slaptažodį turi sudaryti ne mažiau kaip 8 simboliai.

19.3. Keičiant slaptažodį informacinė sistema neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių.

19.4. Informacinės sistemos naudotojui pirmą kartą jungiantis prie informacinės sistemos turi būti prašoma pakeisti slaptažodį.

20. Papildomi informacinių sistemų administratorių slaptažodžių reikalavimai:

20.1. Slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius.

20.2. Slaptažodį turi sudaryti ne mažiau kaip 12 simbolių.

20.3. Keičiant slaptažodį informacinės sistemos taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.

21. Naudotojo teisė dirbti su konkrečia elektronine informacija turi būti sustabdoma, kai naudotojas nesinaudoja atitinkama informacine sistema ilgiau kaip 3 mėnesius. Nutrūkus darbo, sutartiniams ar kitiems santykiams, naudotojo teisė naudotis informacinėmis sistemomis turi būti nedelsiant panaikinama.

22. Draudžiama informacinių sistemų techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti pagal Taisyklėse nustatytus reikalavimus.

23. Jei naudotojas abejoja informacinėse sistemose įdiegtų saugumo priemonių patikimumu, jis nedelsdamas privalo kreiptis į informacinių sistemų administratorių vadovą, kad būtų įvertintos turimos saugumo priemonės ir, jei reikia, inicijuotas papildomų priemonių įsigijimas ir (ar) įdiegimas.

24. Nuotolinis prisijungimas prie informacinių sistemų administravimo modulio galimas tik naudojant VPN technologijas.

25. Informacinių sistemų administratoriaus teisė dirbti su konkrečia elektronine informacija turi būti sustabdoma, jeigu informacinių sistemų administratorius nesinaudoja atitinkama informacine sistema ilgiau kaip 2 mėnesius. Informacinių sistemų administratoriaus teisė naudotis informacinėmis sistemomis turi būti nedelsiant panaikinama nutrūkus darbo, sutartiniams ar kitiems santykiams arba kai informacinių sistemų administratorius praranda patikimumą.

26. Informacinių sistemų komponentų administratorius ne rečiau kaip kartą per mėnesį tikrina, ar nėra nepatvirtintų administratorių ar naudotojų paskyrų tose informacinėse sistemose,

kurios turi paskyrų patvirtinimo funkciją, ir praneša asmeniui, atsakingam už kibernetinį saugumą, apie nepatvirtintas paskyras.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

27. Administratorius, pastebėjęs Taisyklių nuostatų pažeidimų ar veiksmų, galinčių turėti įtakos informacinių sistemų elektroninės informacijos saugai, gali apriboti naudotojo teisę dirbti su konkrečia elektronine informacija ir sustabdyti visas naudotojui suteiktas prieigos prie informacinių sistemų teises, kol minėti pažeidimai ar veiksmai bus pašalinti.

_____

PATVIRTINTA
Lietuvos Respublikos teisingumo ministro
2021 m. spalio 14 d. įsakymu Nr. 1R-350

LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos teisingumo ministerijos informacinių sistemų veiklos tęstinumo valdymo planas (toliau – Valdymo planas) nustato Lietuvos Respublikos teisingumo ministerijos eksploatuojamų informacinių sistemų (toliau – informacinės sistemos) naudotojų, informacinių sistemų administratorių, saugos įgaliotinio ir asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą Teisingumo ministerijoje (toliau – asmuo, atsakingas už kibernetinį saugumą), veiksmus įvykus elektroninės informacijos saugos incidentui ar kibernetiniam incidentui (toliau – elektroninės informacijos saugos incidentas), kilus pavojui informacinių sistemų duomenims, techninės ir programinės įrangos funkcionavimui.

2. Valdymo plane vartojamos sąvokos apibrėžtos 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“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, ir kituose teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą.

3. Valdymo plano tikslas – užtikrinti informacinių sistemų veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui, kilus pavojui informacinių sistemų duomenims, techninės ir programinės įrangos funkcionavimui.

4. Valdymo planas taikomas įvykus elektroninės informacijos saugos incidentui ir yra privalomas informacinių sistemų saugos įgaliotiniui, informacinių sistemų administratoriams, naudotojams ir asmeniui, atsakingam už kibernetinį saugumą.

5. Kilus kibernetinių incidentų, jų nustatymas, informavimas apie kibernetinius incidentus, kibernetinių incidentų tyrimas ir kibernetinių incidentų analizė, baigus kibernetinių incidentų tyrimą, vykdomi Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nacionalinis kibernetinių incidentų valdymo planas), nustatyta tvarka, o Valdymo plano nuostatos taikomos tiek, kiek kibernetinių incidentų valdymo nereglamentuoja Nacionalinis kibernetinių incidentų valdymo planas.

6. Saugos įgaliotinis atsako už Valdymo plano įgyvendinimo organizavimą ir kontrolę.

7. Naudotojai, informacinių sistemų administratoriai, asmuo, atsakingas už kibernetinį saugumą, yra atsakingi už Valdymo plano įgyvendinimą.

8. Elektroninės informacijos saugos incidento metu patirti nuostoliai padengiami teisės aktų nustatyta tvarka.

9. Informacinių sistemų veikla atkuriama vadovaujantis šiomis nuostatomis:

9.1. Informacinių sistemų veikla atkuriama pagal šios sistemos atliekamų funkcijų prioritetus, stabdant visą neesminę veiklą.

9.2. Naudotojai pagal galimybes privalo užtikrinti, kad būtų vykdomi informacinių sistemų saugos politikos įgyvendinamuosiuose dokumentuose nustatyti reikalavimai.

10. Kriterijai, pagal kuriuos nustatoma, kad informacinių sistemų veikla yra atkurta, yra šie:

10.1. Informacinių sistemų duomenys yra prieinami naudotojams.

10.2. Tvarkant informacinių sistemų duomenis užtikrinamas jų konfidencialumas ir vientisumas.

10.3. Užtikrinama tarnybinių stočių administravimo techninės, sisteminės programinės ir taikomosios programinės įrangos veikla ir teikiamos kokybiškos paslaugos.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

11. Elektroninės informacijos saugos incidentams valdyti ir informacinių sistemų veiklai atkurti sudaromos dvi grupės: Informacinių sistemų veiklos tęstinumo valdymo grupė (toliau – Veiklos tęstinumo valdymo grupė) ir Informacinių sistemų veiklos atkūrimo grupė (toliau – Veiklos atkūrimo grupė).

12. Veiklos tęstinumo valdymo grupės tikslai – tirti saugos incidentus, ieškoti priemonių ir būdų sukeltiems padariniams ir žalai likviduoti, užtikrinti informacinių sistemų veiklos tęstinumą.

13. Veiklos tęstinumo valdymo grupės sudėtis:

13.1. vadovas – Turto valdymo ir aprūpinimo skyriaus vedėjas;

13.2. vadovo pavaduotojas – Veiklos valdymo skyriaus vedėjas;

13.3. asmuo, atsakingas už kibernetinį saugumą;

13.4. darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą;

13.5. duomenų apsaugos pareigūnas;

13.6. Teisinio atstovavimo grupės darbuotojas;

13.7. darbuotojas, atsakingas už personalo administravimą;

13.8. darbuotojas, atsakingas už komunikaciją.

14. Veiklos tęstinumo valdymo grupė atlieka šias funkcijas:

14.1. analizuoja elektroninės informacijos saugos incidentų priežastis ir priima sprendimus informacinių sistemų veiklos tęstinumo valdymo klausimais;

14.2. bendradarbiauja su teisėsaugos ir kitų institucijų darbuotojais, pagal kompetenciją teikia informaciją informacinių sistemų naudotojams;

14.3. nustato finansinių ir kitų išteklių poreikį informacinių sistemų veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, ir vykdo jų naudojimo kontrolę;

14.4. užtikrina informacinių sistemų duomenų fizinę saugą, įvykus elektroninės informacijos saugos incidentui;

14.5. organizuoja logistiką (žmonių, daiktų, įrangos pervežimą);

14.6. prižiūri ir koordinuoja informacinių sistemų veiklos atkūrimo procesus;

14.7. atlieka kitas Veiklos tęstinumo valdymo grupei pavestas funkcijas.

15. Veiklos atkūrimo grupės tikslas – likviduoti saugos incidentus.

16. Veiklos atkūrimo grupės sudėtis:

16.1. vadovas – Turto valdymo ir aprūpinimo skyriaus vedėjas;

16.2. vadovo pavaduotojas – informacinių sistemų komponentų administratorius;

16.3. darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą.

17. Veiklos atkūrimo grupė atlieka šias funkcijas:

17.1. organizuoja tarnybinių stočių administravimo techninės, sisteminės programinės ir taikomosios programinės įrangos veiklos atkūrimo darbus (informacinių sistemų komponentų administratorius);

17.2. organizuoja informacinių sistemų elektroninės informacijos atkūrimo darbus (informacinių sistemų komponentų administratorius);

17.3. organizuoja kompiuterizuotų darbo vietų veiklos atkūrimo ir prijungimo prie kompiuterių tinklo darbus (informacinių sistemų komponentų administratorius);

17.5. atlieka kitas Veiklos atkūrimo grupei pavestas funkcijas (informacinių sistemų komponentų administratorius ir darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą).

18. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės sudėtį tvirtina informacinių sistemų valdytojo vadovas arba jo įgaliotas asmuo.

19. Įvykus elektroninės informacijos saugos incidentui Teisingumo ministerijoje, atliekami šie veiksmai:

19.1. Informacinių sistemų administratoriai ar kiti saugos incidentą nustatę asmenys nedelsdami informuoja apie elektroninės informacijos saugos incidentą saugos įgaliotinį, asmenį, atsakingą už kibernetinį saugumą, ir Veiklos tęstinumo valdymo grupės vadovą. Jei įvyko asmens duomenų saugos pažeidimas, apie šį incidentą ir saugos priemones, kurių imtasi siekiant apsaugoti asmens duomenis, nedelsiant informuojamas Teisingumo ministerijos duomenų apsaugos pareigūnas.

19.2. Informacinių sistemų administratoriai nedelsdami informuoja apie elektroninės informacijos saugos incidentą informacinės sistemos naudotojus.

19.3. Naudotojai, informacinių sistemų administratoriai, asmuo, atsakingas už kibernetinį saugumą, nedelsdami įgyvendina Lietuvos Respublikos teisingumo ministerijos vidaus administravimo informacinių sistemų veiklos atkūrimo detaliajame plane (1 priedas) numatytas priemones. Asmuo, atsakingas už kibernetinį saugumą, informacinių sistemų administratoriai, o jų nurodymu – ir naudotojai atlieka kitus neatidėliotinus veiksmus, skirtus saugos incidento plėtrai sustabdyti ir jo tyrimui būtinai informacijai surinkti.

19.4. Veiklos tęstinumo valdymo grupės vadovas nedelsdamas privalo, o tais atvejais, kai elektroninės informacijos saugos incidentas yra susijęs tik su vienu fiziniu asmeniu, turi teisę organizuoti Veiklos tęstinumo valdymo grupės susirinkimą.

19.5. Veiklos tęstinumo valdymo grupė, atlikusi incidento analizę, susisiekia su Veiklos atkūrimo grupe ir informuoja apie esamą padėtį ir priimtus sprendimus dėl veiklos atkūrimo.

19.6. Veiklos atkūrimo grupė įgyvendina Veiklos tęstinumo valdymo grupės priimtus sprendimus dėl veiklos atkūrimo, nustato konkrečius informacinių sistemų atkūrimo darbus ir paskiria asmenis, kurie turi atlikti šiuos darbus, bei nustato terminus, per kuriuos turi būti atlikti veiklos atkūrimo darbai.

19.7. Veiklos atkūrimo grupės paskirti asmenys atlieka informacinių sistemų atkūrimo darbus ir apie tai nedelsdami informuoja Veiklos atkūrimo grupės vadovą, o jis apie atliktus darbus informuoja Veiklos tęstinumo valdymo grupės vadovą. Veiklos tęstinumo valdymo grupės vadovas nuolat informuoja kitus šios grupės narius apie informacinių sistemų veiklos atkūrimo eigą.

19.8. Veiklos tęstinumo valdymo grupės vadovas arba jo įgaliotas grupės narys ne vėliau kaip per 2 darbo dienas nuo saugos incidento pašalinimo darbų atlikimo dienos Dokumentų valdymo bendrojoje informacinėje sistemoje užregistruoja elektroninės informacijos saugos incidentą, užpildydamas Valdymo plano 2 priede patvirtintą formą, ir aprašo įvykį: nurodo jo pradžią, pabaigą, elektroninės informacijos saugos incidento šalinimo darbus atlikusio (-ių) darbuotojo (-ų) vardą (-us), pavardę (-es), elektroninės informacijos saugos incidento poveikio mažinimo priemones. Elektroninės informacijos saugos incidentų registravimo žurnale turi pasirašyti saugos įgaliotinis ir elektroninės informacijos saugos incidento šalinimo darbus atlikęs (-ę) darbuotojas (-ai).

Papunkčio pakeitimai:
Nr. 1R-66, 2023-02-21, paskelbta TAR 2023-02-21, i. k. 2023-03047

20. Veiklos tęstinumo valdymo grupės vadovas organizuoja žalos informacinių sistemų duomenims, techninei ir programinei įrangai vertinimą, koordinuoja informacinių sistemų veiklai atkurti reikalingos techninės, sisteminės ir taikomosios programinės įrangos įsigijimo procesą.

21. Elektroninės informacijos saugos incidentui paveikus ne Teisingumo ministerijos valdomas informacines sistemas, Veiklos tęstinumo valdymo grupės vadovas informuoja elektroninės informacijos saugos incidento poveikį patyrusius ar galinčius patirti paslaugų teikėjus ir (ar) kitas institucijas ir vykdo jų teisėtus nurodymus bei atsižvelgia į jų pateiktas rekomendacijas.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

22. Parengtų ir saugomų dokumentų sąrašas:

22.1. informacinių sistemų kompiuterinės ir programinės įrangos ir šios įrangos parametrų sąrašas (dokumentas, kuriame nurodyti informacinių technologijų įrangos parametrai, minimalus informacinės sistemos veiklai atkurti, nesant informacinių sistemų administratoriaus, reikiamos kompetencijos ar žinių lygis);

22.2. informacinių sistemų minimalus funkcijų sąrašas (dokumentas, kuriame nurodyta minimalaus informacinių technologijų įrangos funkcijų, skirtų informacinės sistemos veiklai užtikrinti įvykus elektroninės informacijos saugos incidentui, sąrašas);

22.3. informacinių sistemų techninė dokumentacija (dokumentas, kuriame nurodyti Teisingumo ministerijos patalpų brėžiniai ir juose pažymėti kompiuterių tinklo mazgai, elektros įvedimo vietos);

22.4. kompiuterių tinklo fizinio ir loginio sujungimo schemos;

22.5. programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis žurnalas, kuriame nurodoma programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

22.6. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis.

23. Už dokumentų, nurodytų Valdymo plano 22.1–22.6 papunkčiuose, parengimą, saugojimą ir prireikus atnaujinimą yra atsakingas informacinių sistemų komponentų administratorius.

IV SKYRIUS
VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

24. Valdymo plano veiksmingumas turi būti išbandytas per 6 mėnesius nuo jo patvirtinimo dienos. Valdymo plano veiksmingumo patikrinimas atliekamas ne rečiau kaip kartą per vienus metus, modeliuojant saugos incidentą. Valdymo plano bandymo būdą ir datą, atsižvelgiant į per vienus metus įvykusius saugos incidentus, įrašytus saugos incidentų registravimo žurnale, saugos įgaliotinio teikimu tvirtina informacinių sistemų valdytojo vadovas arba jo įgaliotas asmuo.

25. Informacinių sistemų komponentų administratorius per 15 darbo dienų po Valdymo plano veiksmingumo bandymo parengia Valdymo plano veiksmingumo bandymo metu pastebėtų trūkumų ataskaitą ir trūkumų šalinimo priemonių planą, suderina juos su saugos įgaliotiniu ir pateikia tvirtinti informacinių sistemų valdytojo vadovui arba jo įgaliotam asmeniui.

26. Valdymo plano veiksmingumo bandymo ataskaitų kopijos ne vėliau kaip 5 darbo dienas nuo ataskaitų priėmimo pateikiamos Nacionaliniam kibernetinio saugumo centrui.

27. Valdymo plano veiksmingumo bandymo metu pastebėti trūkumai šalinami vadovaujantis veiksmingumo, operatyvumo ir ekonomiškumo principais.

_____

Lietuvos Respublikos teisingumo ministerijos
informacinių sistemų veiklos tęstinumo
valdymo plano
1 priedas

LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJOS VIDAUS ADMINISTRAVIMO INFORMACINIŲ SISTEMŲ VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Elektroninės informacijos saugos incidentas	**Veiklos atkūrimo veiksmai (ministerijos darbo valandomis)**	**Atsakingi vykdytojai**
1. Nenugalima jėga *(force majeure)*	1.1. Atitinkamos tarnybos (prireikus ir darbuotojų) informavimas apie pavojaus pobūdį Vykdymo terminas – 10 min.	Darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	1.2. Komunikacijų, keliančių pavojų, išjungimas Vykdymo terminas – 1 val.	Informacinių sistemų komponentų administratorius, darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	1.3. Darbuotojų informavimas Vykdymo terminas – 10 min.	Darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	1.4. Elektroninės informacijos saugos incidento padarinių įvertinimas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas Vykdymo terminas – 3 d. d.	Asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą, informacinių sistemų administratorius, saugos įgaliotinis, naudotojai
2. Gaisras	2.1. Ugniagesių tarnybos informavimas Vykdymo terminas – 10 min.	Darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	2.2. Darbuotojų evakavimas (pagal ugniagesių tarnybos rekomendaciją) Vykdymo terminas – 30 min.	Teisingumo ministerijos darbuotojas, atsakingas už civilinę saugą
	2.3. Komunikacijų, keliančių pavojų, išjungimas Vykdymo terminas – 1 val.	Informacinių sistemų komponentų administratorius, darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą

Elektroninės informacijos saugos incidentas	Veiklos atkūrimo veiksmai (ministerijos darbo valandomis)	Atsakingi vykdytojai
	2.4. Darbuotojų informavimas Vykdymo terminas – 10 min.	Darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	2.5. Elektroninės informacijos saugos incidento padarinių įvertinimas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas Vykdymo terminas – 3 d. d.	Asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą, informacinių sistemų administratorius, saugos įgaliotinis, naudotojai
3. Elektros energijos tiekimo sutrikimai	3.1. Energijos tiekimo sutrikimo priežasčių nustatymas Vykdymo terminas – 1 val.	Darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	3.2. Kreipimasis į energijos tiekimo tarnybą dėl sutrikimo trukmės ir pašalinimo galimybių Vykdymo terminas – 10 min.	Darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	3.3. Techninės įrangos elektros energijos maitinimo išjungimas Vykdymo terminas – 30 min.	Informacinių sistemų komponentų administratorius, darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	3.4. Elektroninės informacijos saugos incidento padarinių įvertinimas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas Vykdymo terminas – 3 d. d.	Asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą, informacinių sistemų administratorius, saugos įgaliotinis, naudotojai
4. Vandentiekio ir šildymo sistemų sutrikimai	4.1. Vandentiekio ir šildymo sistemos sutrikimų priežasčių nustatymas Vykdymo terminas – 1 val.	Darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	4.2. Kreipimasis į vandentiekio ir šildymo sistemos paslaugų teikimo tarnybą dėl sutrikimo trukmės ir pašalinimo galimybių Vykdymo terminas – 10 min.	Darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	4.3. Pavojų keliančių komunikacijų išjungimas Vykdymo terminas – 1 val.	Informacinių sistemų komponentų

Elektroninės informacijos saugos incidentas	Veiklos atkūrimo veiksmai (ministerijos darbo valandomis)	Atsakingi vykdytojai
		administratorius, darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	4.4. Darbuotojų informavimas Vykdymo terminas – 10 min.	Darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą
	4.5. Elektroninės informacijos saugos incidento padarinių įvertinimas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas Vykdymo terminas – 3 d. d.	Asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, darbuotojas, atsakingas už Teisingumo ministerijos ūkinę veiklą, informacinių sistemų administratorius, saugos įgaliotinis, naudotojai
5. Telekomunikacijų ir kitų ryšio tinklų sutrikimai	5.1. Telekomunikacijų ir kitų ryšio tinklų sutrikimų priežasčių nustatymas Vykdymo terminas – 1 val.	Informacinių sistemų komponentų administratorius
	5.2. Kreipimasis į telekomunikacijų ir kitų ryšio tinklų paslaugų teikimo tarnybą dėl sutrikimo trukmės ir pašalinimo galimybių Vykdymo terminas – 10 min.	Informacinių sistemų komponentų administratorius
	5.3. Darbuotojų informavimas Vykdymo terminas – 10 min.	Informacinių sistemų komponentų administratorius
	5.4. Elektroninės informacijos saugos incidento padarinių įvertinimas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas Vykdymo terminas – 3 d. d.	Asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, informacinių sistemų administratorius, saugos įgaliotinis, naudotojai
6. Kompiuterių tinklo įrangos sugadinimas	6.1. Kompiuterių tinklo įrangos sugadinimo priežasčių nustatymas Vykdymo terminas – 1 val.	Informacinių sistemų komponentų administratorius
	6.2. Kreipimasis į įrangos tiekėjus dėl įrangos remonto arba naujos įrangos įsigijimo Vykdymo terminas – 10 min.	Informacinių sistemų komponentų administratorius
	6.3. Darbuotojų informavimas Vykdymo terminas – 10 min.	Informacinių sistemų komponentų administratorius
	6.4. Elektroninės informacijos saugos incidento	Asmuo, atsakingas už

Elektroninės informacijos saugos incidentas	Veiklos atkūrimo veiksmai (ministerijos darbo valandomis)	Atsakingi vykdytojai
	padarinių įvertinimas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas Vykdymo terminas – 3 d. d.	kibernetinio saugumo organizavimą ir užtikrinimą, informacinių sistemų administratorius, saugos įgaliotinis, naudotojai
7. Įsilaužimas į vidinį kompiuterių tinklą	7.1. Įsilaužimo būdo nustatymas Vykdymo terminas – 1 val.	Informacinių sistemų komponentų administratorius
	7.2. Aptikto įsilaužimo užkardymas Vykdymo terminas – 10 min.	Informacinių sistemų komponentų administratorius
	7.3. Viso vidinio tinklo patikra ir papildomų saugos trūkumų analizė Vykdymo terminas – 3 d. d.	Informacinių sistemų komponentų ir saugos administratorius
8. Programinės įrangos sugadinimas, praradimas	8.1. Programinės įrangos sugadinimo priežasčių nustatymas Vykdymo terminas – 2 val.	Informacinių sistemų komponentų ir saugos administratorius
	8.2. Sugadintos ar prarastos programinės įrangos atkūrimas Vykdymo terminas – 20 val.	Informacinių sistemų komponentų administratorius
	8.3. Darbuotojų informavimas Vykdymo terminas – 10 min.	Informacinių sistemų komponentų administratorius
	8.4. Elektroninės informacijos saugos incidento padarinių įvertinimas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas Vykdymo terminas – 3 d. d.	Asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, informacinių sistemų administratorius, saugos įgaliotinis

Pastabos:

1. Apie kibernetinius incidentus Nacionalinis kibernetinio saugumo centras turi būti informuojamas užpildant pranešimo apie incidentą formą, esančią interneto svetainėje https://nksc.lt, arba išsiunčiant informaciją apie incidentą el. paštu cert@nksc.lt, arba skambinant telefonu 1805.

2. Kibernetinių incidentų kategorijos nurodytos Nacionaliniame kibernetinių incidentų valdymo plane.

_____

Lietuvos Respublikos teisingumo
ministerijos informacinių sistemų
veiklos tęstinumo valdymo plano
2 priedas

ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	**Elektroninės informacijos saugos incidentas**						
	Požymio kodas	**Elektroninės informacijos saugos incidento aprašymas**	**Pradžia (data, laikas)**	**Pabaiga (data, laikas)**	**Elektroninės informacijos saugos incidentą pašalinęs (-ę) darbuotojas (-ai) (vardas (-ai), pavardė (-ės), parašas (-ai))**	**Saugos įgaliotinis (vardas, pavardė, parašas)**	**Elektroninės informacijos saugos incidento poveikio mažinimo priemonės**
1.							
2.							
3.							
4.							
5.							
6.							

Pastaba. Elektroninės informacijos saugos incidento požymio kodai: 1. nenugalima jėga; 2. gaisras; 3. elektros energijos tiekimo sutrikimai;
4. vandentiekio ir šildymo sistemų sutrikimai; 5. telekomunikacijų ir kitų ryšio tinklų sutrikimai; 6. kompiuterių tinklo įrangos sugadinimas; 7. įsilaužimas į vidinį kompiuterių tinklą; 8. programinės įrangos sugadinimas.

_____

Pakeitimai:

1.
Lietuvos Respublikos teisingumo ministerija, Įsakymas
Nr. 1R-66, 2023-02-21, paskelbta TAR 2023-02-21, i. k. 2023-03047
Dėl teisingumo ministro 2021 m. spalio 14 d. įsakymo Nr. 1R-350 „Dėl Lietuvos Respublikos teisingumo ministerijos informacinių sistemų saugos politiką įgyvendinančių dokumentų patvirtinimo“ pakeitimo