Suvestinė redakcija nuo 2023-03-01

Įsakymas paskelbtas: TAR 2021-10-15, i. k. 2021-21588

LIETUVOS RESPUBLIKOS TEISINGUMO MINISTRAS

ĮSAKYMAS DĖL LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2021 m. spalio 14 d. Nr. 1R-349
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“, 7, 12, 19, 26 ir 31 punktus bei 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 punktą:

1. T v i r t i n u Lietuvos Respublikos teisingumo ministerijos informacinių sistemų duomenų saugos nuostatus (pridedama).

2. S k i r i u:

2.1. Lietuvos Respublikos teisingumo ministerijos Teisinių paslaugų politikos grupės vyresniąją patarėją Jurgitą Urbaitę Teisingumo ministerijos informacinių sistemų saugos įgaliotine ir už kibernetinio saugumo organizavimą ir užtikrinimą Teisingumo ministerijoje atsakingu asmeniu;

2.2. Teisingumo ministerijos Veiklos valdymo skyriaus patarėją Ronaldą Turauskienę ir vyriausiąją specialistę Mariną Zukienę Dokumentų valdymo sistemos „Avilys“ naudotojų administratorėmis;

2.3. *Neteko galios nuo 2023-03-01*;

Papunkčio pakeitimai:
Nr. 1R-65, 2023-02-20, paskelbta TAR 2023-02-20, i. k. 2023-03013

2.4. Teisingumo ministerijos Turto valdymo ir aprūpinimo skyriaus vyriausiąjį specialistą Paulių Jarašių Teisingumo ministerijos intraneto svetainės naudotojų administratoriumi;

2.5. Teisingumo ministerijos Komunikacijos ir teisinio švietimo skyriaus patarėją Dalią Milkevičienę ir vyriausiąjį specialistą Evaldą Račį Teisingumo ministerijos interneto svetainės naudotojų administratoriais;

2.6. Teisingumo ministerijos Turto valdymo ir aprūpinimo skyriaus vyriausiuosius specialistus Egidijus Trakšelį ir Paulių Jarašių Teisingumo ministerijos informacinių sistemų komponentų ir saugos administratoriais.

3. N u s t a t a u, kad Teisingumo ministerijos Teisinių paslaugų politikos grupės vyresniosios patarėjos Jurgitos Urbaitės atostogų, laikino nedarbingumo, kvalifikacijos tobulinimo užsienyje (vykdomo kontaktiniu būdu), komandiruotės metu ar nesant kitais teisės aktų nustatytais atvejais Teisingumo ministerijos informacinių sistemų saugos įgaliotinio funkcijas vykdo ir už kibernetinio saugumo organizavimą ir užtikrinimą Teisingumo ministerijoje atsakinga yra Teisingumo ministerijos patarėja Dovilė Mekionytė.

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-349

LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos teisingumo ministerijos informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos Respublikos teisingumo ministerijos vidaus administravimo informacinėse sistemose, taip pat interneto ir intraneto svetainėse (toliau kartu – informacinės sistemos) tvarkomos elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, jos valdymą, oganizacinius ir techninius reikalavimus, personalo kvalifikacijos reikalavimus ir informacinių sistemų naudotojų supažindinimo su saugos dokumentais principus.

2. Saugos nuostatai reglamentuoja Teisingumo ministerijos vidaus administravimo informacinės sistemos – dokumentų valdymo sistemos „Avilys“ elektroninės informacijos saugą (kibernetinį saugumą).

Punkto pakeitimai:
Nr. 1R-65, 2023-02-20, paskelbta TAR 2023-02-20, i. k. 2023-03013

3. Saugos nuostatuose 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 ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių apraše, patvirtintuose 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 atitinkamai – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas ir Klasifikavimo gairių aprašas), 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“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), ir 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“ (toliau – Techninių elektroninės informacijos saugos reikalavimų aprašas).

4. Saugos nuostatai, atskiru Lietuvos Respublikos teisingumo ministro įsakymu tvirtinami saugos politiką įgyvendinantys dokumentai (Teisingumo ministerijos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės, Teisingumo ministerijos informacinių sistemų naudotojų administravimo taisyklės, Teisingumo ministerijos informacinių sistemų veiklos tęstinumo valdymo planas (toliau – saugos politiką įgyvendinantys dokumentai)) ir kiti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo dokumentai (toliau kartu – saugos dokumentai) taikomi:

4.1. Teisingumo ministerijai (Gedimino pr. 30, 01104 Vilnius) – informacinių sistemų valdytojai ir tvarkytojai;

4.2. informacinių sistemų saugos įgaliotiniui, informacinių sistemų administratoriams, už kibernetinio saugumo organizavimą ir užtikrinimą Teisingumo ministerijoje atsakingam asmeniui (toliau – asmuo, atsakingas už kibernetinį saugumą), informacinių sistemų naudotojams, informacinėms sistemoms funkcionuoti reikalingų paslaugų teikėjams.

5. Elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetinės kryptys yra šios:

5.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.2. asmens duomenų apsauga;

5.3. informacinių sistemų veiklos tęstinumo užtikrinimas;

5.4. informacinių sistemų rizikos valdymas;

5.5. informacinių sistemų naudotojų mokymas elektroninės informacijos saugos (kibernetinio saugumo) klausimais;

5.6. organizacinių, techninių, programinių, teisinių, informacijos sklaidos ir kitų priemonių, skirtų elektroninės informacijos saugai (kibernetiniam saugumui) užtikrinti, įgyvendinimas ir kontrolė.

6. Elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo tikslai:

6.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją informacinėse sistemose;

6.2 užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

6.3. vykdyti elektroninės informacijos saugos ir kibernetinių incidentų, asmens duomenų saugos pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos ir kibernetinius incidentus, asmens duomenų saugos pažeidimus ir juos operatyviai suvaldyti, atkuriant įprastą informacinių sistemų veiklą.

7. Teisingumo ministerija, būdama informacinių sistemų valdytoja ir tvarkytoja, atsako už elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir įgyvendinimą, priežiūrą bei elektroninės informacijos tvarkymo teisėtumą, taip pat už reikiamų administracinių, techninių ir organizacinių informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) priemonių įgyvendinimą, užtikrinimą bei elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų laikymąsi saugos dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektoninės informacijos saugą (kibernetinį saugumą), nustatyta tvarka.

8. Teisingumo ministerija, būdama informacinių sistemų valdytoja ir tvarkytoja, atlieka šias funkcijas:

8.1. tvirtinta informacinių sistemų saugos dokumentus;

8.2. užtikrina saugos dokumentų ir kitų teisės aktų, reglamentuojančių elektoninės informacijos saugą (kibernetinį saugumą), tinkamą įgyvendinimą;

8.3. priima sprendimus dėl techninių ir programinių priemonių, būtinų elektroninės informacijos saugai (kibernetiniam saugumui) užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

8.4. priima sprendimus dėl elektroninės informacijos saugos (kibernetinio saugumo) priemonių finansavimo;

8.5. atsižvelgdama į informacinių sistemų rizikos vertinimo ataskaitą, prireikus tvirtina rizikos vertinimo ir rizikos valdymo priemonių planą;

8.6. užtikrina veiksmingą ir spartų pokyčių, susijusių su informacinių sistemų valdymu, planavimą;

8.7. atlikus informacinių technologijų saugos atitikties vertinimą, tvirtina pastebėtų trūkumų šalinimo planą;

8.8. atsižvelgdama į grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinių sistemų kibernetiniam saugumui, rizikos vertinimą, peržiūri patvirtintus saugos dokumentus ir kitus teisės aktus, reglamentuojančius elektoninės informacijos saugą (kibernetinį saugumą) ir jų įgyvendinimą;

8.9. skiria informacinių sistemų elektroninės informacijos saugos įgaliotinį (toliau – saugos įgaliotinis) ir asmenį, atsakingą už kibernetinį saugumą ;

8.10. skiria informacinių sistemų administratorių (administratorius) ir paveda jam (jiems) užtikrinti informacinių sistemų tarnybinių stočių saugų funkcionavimą, administruoti informacinių sistemų duomenų bazes Saugos nuostatų ir kitų saugos politiką įgyvendinančių teisės aktų nustatyta tvarka;

8.11. atlieka kitas saugos dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektoninės informacijos saugą (kibernetinį saugumą), nustatytas funkcijas.

9. Saugos įgaliotinis atlieka ir asmens, atsakingo už kibernetinį saugumą, funkcijas.

10. Saugos įgaliotinis koordinuoja ir prižiūri informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimą informacinėse sistemose, taip pat atlieka šias funkcijas:

10.1. teikia informacinių sistemų valdytojo vadovui arba jo įgaliotam asmeniui pasiūlymus dėl:

10.1.1. saugos dokumentų priėmimo ir keitimo;

10.1.2. informacinių technologijų saugos atitikties vertinimo atlikimo;

10.1.3. informacinių sistemų administratoriaus (administratorių) skyrimo ir reikalavimų jo (jų) pareigybei (-ėms) nustatymo.

10.2. koordinuoja elektroninės informacijos saugos (kibernetinių) incidentų, įvykusių informacinėse sistemose, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninės informacijos saugos (kibernetinius) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetiniais) incidentais, išskyrus atvejus, kai šią funkciją atlieka elektroninės informacijos saugos grupė;

10.3. teikia informacinių sistemų administratoriui (administratoriams) ir informacinių sistemų naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos politikos įgyvendinimu;

10.4. organizuoja informacinių sistemų rizikos vertinimą ir informacinių technologijų saugos atitikties vertinimą;

10.5. periodiškai inicijuoja informacinių sistemų naudotojų mokymus informacinių sistemų elektroninės informacijos saugos klausimais;

10.6. supažindina informacinių sistemų administratorių (administratorius) ir informacinių sistemų naudotojus su saugos dokumentais;

10.7. atlieka kitas informacinių sistemų valdytojo vadovo pavestas ir saugos dokumentuose bei kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą (kibernetinį saugumą), nustatytas funkcijas.

11. Saugos įgaliotinis negali atlikti informacinių sistemų administratoriaus funkcijų.

12. Informacinių sistemų administratoriai pagal atliekamas funkcijas skirstomi į:

12.1. informacinių sistemų naudotojų administratorius, kuris atlieka funkcijas, susijusias su informacinių sistemų naudotojų teisių valdymu;

12.2. informacinių sistemų komponentų administratorius, kuris atlieka funkcijas, susijusias su informacinių sistemų komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazėmis ir jų valdymo sistemomis, taikomųjų programų sistemomis, užkardomis, įsilaužimų aptikimo ir prevencijos sistemomis, elektroninės informacijos perdavimo tinklais, duomenų saugyklomis, bylų serveriais ir kita technine ir programine įranga, kuri yra informacinių sistemų pagrindas ir kuria užtikrinama jose tvarkomos elektroninės informacijos sauga (kibernetinis saugumas) bei informacinių sistemų komponentų sąranka);

12.3. informacinių sistemų saugos administratorius, kuris atlieka funkcijas, susijusias su informacinių sistemų pažeidžiamų vietų nustatymu, saugos reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos incidentus.

13. Informacinių sistemų administratoriai yra atsakingi už tinkamą saugos dokumentuose jiems nustatytų funkcijų vykdymą.

14. Informacinių sistemų administratoriai privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimu, pagal kompetenciją reaguoti į incidentus, susijusius su elektroninės informacijos saugos (kibernetiniais) pažeidimais, ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

15. Atlikdami informacinių sistemų sąrankos pakeitimus, informacinių sistemų komponentų administratoriai turi laikytis teisingumo ministro patvirtintose Teisingumo ministerijos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse nustatytos pokyčių valdymo tvarkos ir reguliariai – ne rečiau kaip kartą per metus ir (arba) įvykus pokyčiams informacinėse sistemose tikrinti (peržiūrėti) informacinių sistemų sąranką bei informacinių sistemų būsenos rodiklius, kurių kategorijos nustatomos šiose taisyklėse.

16. Informacinių sistemų naudotojai, vadovaudamiesi saugos dokumentais ir pareigybių aprašymais, naudojasi informacinių sistemų duomenimis ir informacija tvarkymo arba kitais su tiesioginių funkcijų vykdymu susijusiais tikslais.

17. Tvarkant elektroninę informaciją informacinėse sistemose ir užtikrinant jos saugą (kibernetinį saugumą), vadovaujamasi šiais teisės aktais:

17.1. 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) su visais pakeitimais;

17.2. Kibernetinio saugumo įstatymu;

17.3. Valstybės informacinių išteklių valdymo įstatymu;

17.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

17.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

17.6. Klasifikavimo gairių aprašu;

17.7. Techninių elektroninės informacijos saugos reikalavimų aprašu;

17.8. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu;

17.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta 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“ (toliau – Informacinių technologijų saugos atitikties vertinimo metodika);

17.10. Lietuvos standartu LST EN ISO/IEC 27001;

17.11. Lietuvos standartu LST EN ISO/IEC 27002;

17.12. saugos dokumentais ir kitais teisės aktais, reglamentuojančiais elektoninės informacijos saugą (kibernetinį saugumą).

II SKYRIUS
INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS (KIBERNETINIO SAUGUMO) VALDYMAS

18. Vadovaujantis Klasifikavimo gairių aprašo 10 punktu, informacinėse sistemose tvarkoma elektroninė informacija priskiriama mažiausios svarbos informacijai (tvarkoma elektroninė informacija, kuri nepatenka į Klasifikavimo gairių aprašo 6.1–6.3 papunkčiuose nurodytas kategorijas).

19. Vadovaujantis Klasifikavimo gairių aprašo 12.4 papunkčiu, Saugos nuostatų 2 punkte nurodytos informacinės sistemos priskiriamos ketvirtajai kategorijai, nes jose tvarkoma mažiausios svarbos informacija.

20. Už informacinių sistemų rizikos vertinimo organizavimą yra atsakingas saugos įgaliotinis, kuris, vadovaudamasis Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos interneto svetainėje skelbiama metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, ne rečiau kaip kartą per metus organizuoja informacinių sistemų rizikos vertinimą. Taip pat ne rečiau kaip kartą per metus arba įvykus esminiams organizaciniams ir sisteminiams pokyčiams kartu su informacinių sistemų rizikos vertinimu ir (ar) Saugos nuostatų 30 punkte nurodytu informacinių technologijų saugos atitikties vertinimu gali būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinių sistemų kibernetiniam saugumui, rizikos vertinimas. Prireikus saugos įgaliotinis gali

organizuoti neeilinį informacinių sistemų rizikos vertinimą. Informacinių sistemų valdytojo raštišku pavedimu informacinių sistemų rizikos vertinimą gali atlikti pats saugos įgaliotinis.

21. Organizuojant informacinių sistemų rizikos vertinimą, turi būti paskiriamas už informacinių sistemų rizikos vertinimą, rizikos vertinimo proceso priežiūrą ir tobulinimą atsakingas asmuo arba keli asmenys bei nustatomi jų kvalifikacijai keliami reikalavimai. Atsakingu asmeniu gali būti paskiriamas informacinių sistemų valdytojo darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros ir nuolatinio tobulinimo paslaugas teikiančiu subjektu.

22. Vertinant informacinių sistemų riziką turi būti:

22.1. nustatomi reikalavimai rizikos vertinimo procesui, rizikos išdėstymo pagal prioritetus kriterijai ir priimtinas rizikos dydis;

22.2. nustatomi grėsmės ir pažeidžiamumai, galintys turėti įtakos elektroninės informacijos saugai (kibernetiniam saugumui), galimo grėsmių ir pažeidžiamumų poveikio vykdomai veiklai srities;

22.3. įvertinamos informacinių sistemų pažeidimo grėsmių tikimybė ir pasekmės;

22.4. nustatomi rizikos lygis ir identifikuotų grėsmių, kurios išdėstomos prioriteto tvarka pagal svarbą, nustatomą atsižvelgiant į atliktą rizikos vertinimą, tikimybė.

23. Informacinių sistemų rizikos vertinimo rezultatai išdėstomi rizikos vertinimo ataskaitoje, kuri pateikiama informacinių sistemų valdytojo vadovui. Rizikos vertinimo ataskaita rengiama įvertinus rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai (kibernetiniam saugumui), jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus bei rizikos priimtinumo kriterijus. Rizikos veiksniai rizikos vertinimo ataskaitoje išdėstomi pagal prioritetus ir priimtiną rizikos lygį.

24. Svarbiausi informacinių sistemų rizikos veiksniai yra šie:

24.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos pateikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kt.);

24.2 subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacinėmis sistemomis elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymas, saugos pažeidimai, vagystės ir kt.);

24.3. įvykiai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

25. Atsižvelgdamas į rizikos vertinimo ataskaitą, informacinių sistemų valdytojas prireikus tvirtina rizikos vertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

26. Atsižvelgiant į atlikto rizikos vertinimo rezultatus, turi būti peržiūrimi patvirtinti saugos dokumentai.

27. Siekiant įgyvendinti saugos dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektoninės informacijos saugą (kibernetinį saugumą), nustatytus elektroninės informacijos saugos (kibernetinio saugumo) tikslus ir užtikrinti šio proceso kontrolę, ne rečiau kaip kartą per dvejus metus organizuojamas informacinių technologijų saugos atitikties vertinimas, atliekamas vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika, ir ne rečiau kaip kartą per metus – informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas, atliekamas vadovaujantis Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu.

28. Informacinių technologijų saugos atitikties (informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams) vertinimą gali atlikti saugos įgaliotinis, asmuo, atsakingas už kibernetinį saugumą, informacinės sistemos valdytojo vidaus auditorius ar kitas informacinės sistemos valdytojo paskirtas vertintojas.

29. Atliekant informacinių technologijų saugos atitikties vertinimą turi būti:

29.1. inventorizuojama informacinių sistemų techninė ir programinė įranga;

29.2. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų informacinių sistemų naudotojų kompiuterizuotų darbo vietų, taip pat – visose informacinių sistemų tarnybinėse stotyse įdiegtos programos ir jų sąranka;

29.3. patikrinama (įvertinama) informacinių sistemų naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;

29.4. įvertinamas pasirengimas užtikrinti informacinių sistemų veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui;

29.5. nustatoma informacinių sistemų rizikos vertinimo ir valdymo būklė;

29.6. patikrinama, ar saugos dokumentai persvarstomi (peržiūrimi) saugos reikalavimuose nustatytu laikotarpiu, ir įvertinama jų kokybė.

30. Atlikus informacinių sistemų informacinių technologijų saugos (informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams) atitikties vertinimą, parengiami informacinių sistemų informacinių technologijų saugos (informacinių sistemų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams) vertinimo ataskaita ir pastebėtų trūkumų šalinimo planas ir pateikiami informacinių sistemų valdytojo vadovui. Pastebėtų trūkumų šalinimo planą tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinių sistemų valdytojo vadovas.

31. Patvirtintų saugos politiką įgyvendinančių dokumentų ir jų pakeitimų, informacinių sistemų rizikos vertinimo ataskaitos, rizikos vertinimo ir valdymo priemonių plano, informacinių technologijų saugos atitikties vertinimo ataskaitos, kibernetinio saugumo atitikties reikalavimams vertinimo ataskaitos ir pastebėtų trūkumų šalinimo plano kopijas informacinių sistemų valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo dienos pateikia 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. nutarimu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

32. Elektroninės informacijos saugos (kibernetinio saugumo) priemonės (techninės, programinės, organizacinės ir kt.) parenkamos vadovaujantis šiais principais:

32.1. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei;

32.2. liekamoji rizika turi būti sumažinta iki priimtino lygio;

32.3. turi būti įdiegtos prevencinės, detekcinės ir korekcinės elektroninės informacijos saugos (kibernetinio saugumo) priemonės, atsižvelgiant į jų efektyvumą ir taikymo tikslingumą.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

33. Organizacinius ir techninius elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus nustato Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, Techninių elektroninės informacijos saugos reikalavimų aprašas, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas ir kiti Saugos nuostatų 17 punkte nurodyti teisės aktai.

34. Organizacinių ir techninių elektroninės informacijos saugos (kibernetinio saugumo) priemonių reikalavimų nustatymas turi būti grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos elektroninės informacijos saugai (kibernetiniam saugumui), rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus.

35. Detalūs organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai nustatomi saugos politiką įgyvendinančiuose dokumentuose.

36. Pagrindiniai organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai:

36.1. turi būti naudojama ir operatyviai naujinama programinė įranga, skirta informacinėms sistemoms apsaugoti nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamų elektroninių laiškų ir pan.). Detalios šios programinės įrangos naudojimo nuostatos ir jos naujinimo reikalavimai (ilgiausias leistinas laikas, kai programinė įranga nėra naujinama, ir kita) nustatomi teisingumo ministro tvirtinamose Teisingumo ministerijos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse;

36.2. turi būti naudojama tik legali programinė įranga, įdiegta kompiuterinėse darbo vietose ir tarnybinėse stotyse. Detalios programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos, jos naujinimo reikalavimai nustatomi teisingumo ministro tvirtinamose informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse;

36.3. turi būti naudojama kompiuterių tinklo filtravimo įranga (užkardos, turinio kontrolės sistemos, įgaliotieji serveriai (angl. *proxy*) ir kita). Detalios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos teisingumo ministro tvirtinamose informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse;

36.4. siekiant užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą, turi būti naudojami šifravimas, virtualus privatus tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą (nuotolinio prisijungimo prie informacinių sistemų būdai, protokolai, elektroninės informacijos keitimosi

formatai, šifravimo, elektroninės informacijos kopijų skaičiaus reikalavimai), nustatomi teisingumo ministro tvirtinamose informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse;

36.5. stacionarūs kompiuteriai naudojami informacinių sistemų valdytojo patalpose, iš minėtų patalpų juos išnešti galima tik suderinus su informacinių sistemų saugos administratoriais. Nešiojamiesiems kompiuteriams, išnešamiems iš informacinių sistemų valdytojo patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas ir kt.).

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

37.1. atsarginių elektroninės informacijos kopijų darymo strategija turi būti pasirenkama atsižvelgiant į leistiną elektroninės informacijos praradimą (angl. *recovery point objetive*) ir priimtiną informacinių sistemų neveikimo laikotarpį (angl. *recovery time objective*);

37.2. atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokios apimties, kad informacinių sistemų veiklos sutrikimo, elektroninės informacijos saugos (kibernetinio) incidento ar elektroninės informacijos vientisumo praradimo atvejais neveikimo laikotarpis nebūtų ilgesnis, nei nustatyta atitinkamų informacinių sistemų svarbos kategorijoms, vadovaujantis Techninių elektroninės informacijos saugos reikalavimų aprašu, o elektroninės informacijos praradimas atitiktų rizikos priimtinumo kriterijus;

37.3. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai periodiškai, bet ne rečiau, nei nustatyta teisingumo ministro tvirtinamose informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse;

37.4. elektroninė informacija atsarginėse elektroninės informacijos kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo atsarginių elektroninės informacijos kopijų) arba turėtų būti imamasi kitų priemonių, kurios neleistų neteisėtai atkurti elektroninės informacijos;

37.5. atsarginių elektroninės informacijos kopijų laikmenos turi būti žymimos taip, kad jas būtų galima identifikuoti, ir saugomos nedegioje spintoje, tačiau kitose patalpose – ne tose, kur yra informacinių sistemų tarnybinės stotys ar įrenginys, kurio elektroninė informacija buvo nukopijuota;

37.6. periodiškai, bet ne rečiau kaip kartą per metus turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai;

37.7. patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas teisingumo ministro tvirtinamose informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse nustatyta tvarka.

IV SKYRIUS
PERSONALO KVALIFIKACIJOS REIKALAVIMAI

38. Saugos įgaliotinio (asmens, atsakingo už kibernetinį saugumą), informacinių sistemų administratorių ir naudotojų kvalifikacijos reikalavimai:

38.1. saugos įgaliotinis (asmuo, atsakingas už kibernetinį saugumą) privalo išmanyti informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos (kibernetinio saugumo) srityje,

savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu ir kitais saugos dokumentais;

38.2. saugos įgaliotiniu (asmeniu, atsakingu už kibernetinį saugumą) negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą, susijusį su elektroninių duomenų ir informacinių sistemų saugos pažeidimu, paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, taip pat už elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų bei taisyklių pažeidimą, jeigu nuo jos paskyrimo praėjo mažiau kaip vieni metai;

38.3. informacinių sistemų administratoriai pagal kompetenciją turi būti susipažinę saugos dokumentais, privalo išmanyti informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti informacinių sistemų ir jose tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti duomenų bazes bei priskirtas informacines sistemas, šių sistemų komponentus (stebėti jų veikimą, atlikti profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, gebėti užtikrinti nepertraukiamą komponentų veikimą ir pan.);

38.4. informacinių sistemų naudotojai privalo turėti pagrindinių darbo kompiuteriu, taikomosiomis programomis įgūdžių, mokėti tvarkyti elektroninę informaciją, būti susipažinę su teisės aktais, reglamentuojančiais asmens duomenų, taip pat informacinių sistemų elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo saugoti jų paslaptį ir būti pasirašę tokį pasižadėjimą. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

39. Informacinių sistemų naudotojų mokymo planavimo, organizavimo ir vykdymo tvarka yra tokia:

39.1. saugos įgaliotinis periodiškai inicijuoja naudotojų mokymus informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) klausimais, įvairiais būdais informuoja juos apie informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) problemas (pavyzdžiui, priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems informacinių sistemų naudotojams);

39.2. mokymai informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas diegti technologijas (techninę ar programinę įrangą), informacinių sistemų naudotojų poreikius;

39.3. mokymai gali būti vykdomi tiesiogiai (pavyzdžiui, paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu būdu (pavyzdžiui, vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.);

39.4. mokymai informacinių sistemų naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per dvejus metus. Už informacinių sistemų naudotojų mokymų organizavimą ir koordinavimą atsakingas yra saugos įgaliotinis.

40. Informacinių sistemų valdytojas užtikrina reikiamą saugos įgaliotinio, informacinių sistemų administratorių, naudotojų kvalifikacijos tobulinimą.

V SKYRIUS
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

41. Informacinių sistemų naudotojų, administratorių supažindinimą su saugos dokumentais ir atsakomybe už šiuose dokumentuose nustatytų reikalavimų nesilaikymą organizuoja ir užtikrina saugos įgaliotinis.

42. Informacinių sistemų naudotojai ir administratoriai su saugos dokumentais supažindinami per Dokumentų valdymo bendrąją informacinę sistemą.

Punkto pakeitimai:
Nr. 1R-65, 2023-02-20, paskelbta TAR 2023-02-20, i. k. 2023-03013

43. Pakartotinai su saugos dokumentais informacinių sistemų naudotojai, administratoriai supažindinami tik iš esmės pasikeitus šiems dokumentams arba padažnėjus elektroninės informacijos saugos (kibernetiniams) incidentų.

44. Tvarkyti informacinių sistemų elektroninę informaciją, prižiūrėti informacines sistemas ir (ar) jų infrastruktūrą gali tik informacinių sistemų naudotojai ir administratoriai, kurie yra susipažinę su saugos dokumentais. Informacinių sistemų naudotojai ir administratoriai atsako už informacinių sistemų ir jose tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

45. Už Saugos nuostatų laikymąsi saugos įgaliotinis, asmuo, atsakingas už kibernetinį saugumą, informacinių sistemų administratoriai ir naudotojai atsako teisės aktų nustatyta tvarka.

Pakeitimai:

1.
Lietuvos Respublikos teisingumo ministerija, Įsakymas
Nr. 1R-65, 2023-02-20, paskelbta TAR 2023-02-20, i. k. 2023-03013
Dėl teisingumo ministro 2021 m. spalio 14 d. įsakymo Nr. 1R-349 „Dėl Lietuvos Respublikos teisingumo ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“ pakeitimo