Suvestinė redakcija nuo 2018-09-04

Įsakymas paskelbtas: TAR 2016-02-03, i. k. 2016-02260

LIETUVOS RESPUBLIKOS TEISINGUMO MINISTRAS

ĮSAKYMAS
DĖL KALĖJIMŲ DEPARTAMENTO PRIE LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO, SAUGOS ĮGALIOTINIO, ADMINISTRATORIŲ SKYRIMO IR SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ RENGIMO

2016 m. vasario 3 d. Nr. 1R-34
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 7 ir 19 punktais:

1. T v i r t i n u Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos informacinės sistemos (toliau – KADIS) saugos nuostatus (pridedama).

2. P a v e d u Kalėjimų departamentui prie Lietuvos Respublikos teisingumo ministerijos ir valstybės įmonei Registrų centrui:

2.1. paskirti KADIS saugos įgaliotinį ir KADIS administratorius;

2.2. paskirti valstybės tarnautoją ar darbuotoją, dirbantį pagal darbo sutartį, kuris kontroliuotų KADIS techninės ir programinės įrangos priežiūros funkcijas teikiančio paslaugų teikėjo darbą, jei tokios funkcijos paslaugų teikėjui perduotos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka;

2.3. ne vėliau kaip per 2 mėnesius nuo šio įsakymo įsigaliojimo dienos parengti ir pateikti Lietuvos Respublikos teisingumo ministrui tvirtinti saugos politiką įgyvendinančių dokumentų projektus.

Teisingumo ministras Juozas Bernatonis

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2015-12-14 raštu Nr. 1D-9743

PATVIRTINTA
Lietuvos Respublikos teisingumo ministro
2016 m. vasario 3 d. įsakymu Nr. 1R-34

KALĖJIMŲ DEPARTAMENTO PRIE LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos informacinės sistemos (toliau – KADIS) duomenų saugos nuostatai (toliau – saugos nuostatai) reglamentuoja KADIS elektroninės informacijos saugos politiką.

2. Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių apraše, Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, ir kituose teisės aktuose bei Lietuvos „Informacijos technologija. Saugumo metodai“ grupės standartuose.

3. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

3.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

3.2. KADIS veiklos tęstinumo užtikrinimas;

3.3. KADIS naudotojų mokymas;

3.4. asmens duomenų apsauga.

4. Elektroninės informacijos saugumo užtikrinimo tikslai:

4.1. sudaryti sąlygas automatiniu būdu saugiai tvarkyti elektroninę informaciją;

4.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo ar neteisėto jos tvarkymo.

5. Saugos nuostatai taikomi KADIS valdytojai – Lietuvos Respublikos teisingumo ministerijai (Gedimino pr. 30, Vilnius) – ir KADIS tvarkytojams: Kalėjimų departamentui prie Lietuvos Respublikos teisingumo ministerijos (L. Sapiegos g. 1, Vilnius), Alytaus pataisos namams (Ulonų g. 8A, Alytus), Kybartų pataisos namams (J. Biliūno g. 14, Kybartai), Marijampolės pataisos namams (Sporto g. 7, Marijampolė), Panevėžio pataisos namams (P. Puzino g. 12, Panevėžys), Pravieniškių pataisos namams-atvirajai kolonijai (Pravieniškių g. 5, Pravieniškių k., Kaišiadorių r.), Vilniaus pataisos namams (Rasų g. 8, Vilnius), Kauno nepilnamečių tardymo izoliatoriui-pataisos namams (Technikos g. 34, Kaunas), Kauno tardymo izoliatoriui (A. Mickevičiaus g. 11, Kaunas), Lukiškių tardymo izoliatoriui-kalėjimui (Lukiškių skg. 6, Vilnius),

Šiaulių tardymo izoliatoriui (Trakų g. 10, Šiauliai), Laisvės atėmimo vietų ligoninei (Pravieniškių g. 57, Pravieniškių k., Kaišiadorių r.), Lietuvos probacijos tarnybai (Anykščių g. 4, Panevėžys), valstybės įmonei Registrų centrui (V. Kudirkos g. 18-3, Vilnius).

Punkto pakeitimai:

Nr. 1R-170, 2018-09-03, paskelbta TAR 2018-09-03, i. k. 2018-13847

6. KADIS valdytojo funkcijos:

6.1. metodiškai vadovauti KADIS tvarkytojams ir koordinuoti KADIS funkcionavimą;

6.2. koordinuoti KADIS tvarkytojų, techninės ir programinės įrangos priežiūros funkcijas teikiančio paslaugų teikėjo darbą, nustatyta tvarka atlikti jų veiklos priežiūrą;

6.3. prižiūrėti, kaip laikomasi elektroninės informacijos saugos reikalavimų;

6.4. nagrinėti KADIS tvarkytojų pasiūlymus dėl KADIS elektroninės informacijos saugos tobulinimo ir priimti dėl jų sprendimus;

6.5. priimti įsakymus dėl KADIS elektroninės informacijos saugumo užtikrinimo;

6.6. užtikrinti vienodą ir spartų KADIS pokyčių valdymo planavimą;

6.7. skirti KADIS saugos įgaliotinį (toliau – saugos įgaliotinis) arba pavesti jį paskirti KADIS tvarkytojui – Kalėjimų departamentui prie Lietuvos Respublikos teisingumo ministerijos;

6.8. skirti KADIS administratorius (toliau – administratoriai) arba pavesti juos paskirti KADIS tvarkytojui – Kalėjimų departamentui prie Lietuvos Respublikos teisingumo ministerijos;

6.9. prireikus tvirtinti rizikos įvertinimo ir rizikos valdymo priemonių planą;

6.10. prireikus tvirtinti KADIS informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

6.11. atlikti kitas KADIS saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

7. KADIS tvarkytojų funkcijos:

7.1. užtikrinti nepertraukiamą KADIS veikimą;

7.2. užtikrinti KADIS elektroninės informacijos saugą ir saugų jos perdavimą elektroninių ryšių tinklais;

7.3. užtikrinti KADIS valdytojo priimtų teisės aktų ir rekomendacijų tinkamą įgyvendinimą;

7.4. ne rečiau kaip kartą per metus organizuoti saugos dokumentų persvarstymą (peržiūrėjimą);

7.5. organizuoti KADIS naudotojams mokomuosius ir pažintinius kursus KADIS elektroninės informacijos tvarkymo klausimais;

7.6. atlikti kitas KADIS saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

8. Už elektroninės informacijos saugą pagal kompetenciją atsako KADIS valdytojas ir tvarkytojai.

9. KADIS valdytojas atsako už saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

10. KADIS tvarkytojai atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi saugos nuostatus ir saugos politiką įgyvendinančių dokumentų nustatyta tvarka.

11. KADIS saugos įgaliotinio, koordinuojančio ir prižiūrinčio KADIS saugos politiką, funkcijos ir atsakomybė:

11.1. teikti KADIS tvarkytojo vadovui pasiūlymus dėl:

11.1.1. KADIS administratoriaus paskyrimo ir reikalavimų administratoriams nustatymo;

11.1.2. informacinių technologijų saugos atitikties vertinimo pagal Informacinių technologijų saugos atitikties vertinimo metodiką, patvirtintą Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

11.2. teikti KADIS valdytojo vadovui pasiūlymus dėl saugos dokumentų priėmimo, keitimo;

11.3. koordinuoti KADIS elektroninės informacijos saugos incidentų tyrimą ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos

incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

11.4. teikti administratoriams ir KADIS naudotojams privalomus vykdyti nurodymus ir pavedimus dėl saugos politikos įgyvendinimo;

11.5. organizuoti rizikos ir informacinių technologijų saugos atitikties įvertinimą;

11.6. atlikti kitas saugos nuostatuose, kituose teisės aktuose nustatytas ir 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, saugos įgaliotiniui priskirtas funkcijas.

12. Saugos įgaliotinis negali atlikti administratoriaus funkcijų.

13. Saugos įgaliotinis, atlikdamas savo funkcijas, turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems KADIS valdytojo ir informacinių sistemų tvarkytojų darbuotojams, jeigu tai būtina saugos politikai įgyvendinti.

14. Administratoriai skiriami keliems KADIS posistemiams, funkciškai savarankiškoms sudedamosioms dalims ar tam tikroms administratoriaus funkcijoms atlikti.

15. Administratoriai skirstomi į šias grupes:

15.1. koordinuojantis administratorius, kuris prižiūri administratorių veiklą siekdamas užtikrinti tinkamą administratorių funkcijų vykdymą;

15.2. KADIS naudotojų administratorius, kuris atlieka KADIS naudotojų teisių valdymo funkcijas;

15.3. KADIS komponentų administratorius, kuris atlieka funkcijas, susijusias su KADIS komponentais (kompiuteriais, operacinėmis sistemomis, duomenų bazių valdymo sistemomis, taikomųjų programų sistemomis, užkardomis, įsilaužimų aptikimo sistemomis, elektroninės informacijos perdavimu tinklais, bylų serveriais ir kitais komponentais) ir jų sąranka;

15.4. saugumo administratorius, kuris atlieka KADIS pažeidžiamų vietų nustatymo, saugumo reikalavimų atitikties nustatymo ir stebėsenos funkcijas.

16. Administratorių skaičius nustatomas KADIS valdytojo, kai jis skiria administratorius, arba informacinių sistemų tvarkytojo įsakyme dėl administratorių skyrimo.

17. Administratoriai privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus dėl KADIS saugos užtikrinimo, pagal kompetenciją reaguoti į elektroninės informacijos saugos incidentus ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

18. Atlikdamas KADIS sąrankos pakeitimus, KADIS komponentų administratorius turi laikytis KADIS valdytojo KADIS pokyčių valdymo tvarkos, nustatytos informacinių sistemų valdytojo tvirtinamose KADIS saugaus elektroninės informacijos tvarkymo taisyklėse.

19. KADIS komponentų administratoriai privalo patikrinti (peržiūrėti) KADIS sąranką ir KADIS būsenos rodiklius reguliariai – ne rečiau kaip kartą per metus ir (ar) po informacinių sistemų pokyčio.

20. Teisės aktai, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugą:

20.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

20.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

20.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

20.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

20.5. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, patvirtintas Lietuvos Respublikos

Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Informacinių sistemų klasifikavimo gairių aprašas);

20.6. Saugos dokumentų turinio gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;

20.7. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

20.8. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtinti Valstybės duomenų apsaugos inspekcijos direktoriaus 2014 m. gruodžio 18 d. įsakymu Nr. 1T-74(1.12.E) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“ (toliau – Bendrieji reikalavimai saugumo priemonėms);

20.9. Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001, Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo technika“ grupės standartai, nustatantys saugų informacinės sistemos duomenų tvarkymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

21. KADIS tvarkoma elektroninė informacija priskiriama žinybinės svarbos elektroninės informacijos kategorijai. Elektroninė informacija šiai kategorijai priskiriama vadovaujantis Informacinių sistemų klasifikavimo gairių aprašo 4.3 papunkčio nuostatomis.

22. KADIS priskiriama trečiai kategorijai, vadovaujantis Informacinių sistemų klasifikavimo gairių aprašo 5.3 papunkčio nuostatomis, atsižvelgiant į informacinėje sistemoje apdorojamos elektroninės informacijos svarbos kategoriją.

23. Informacinės sistemos asmens duomenų tvarkymas automatiniu būdu priskirtinas antrajam saugumo lygiui, vadovaujantis Bendrųjų reikalavimų saugumo priemonėms 11.2 papunkčio nuostatomis.

24. KADIS saugos įgaliotinis, vadovaudamasis Lietuvos Respublikos vidaus reikalų ministerijos metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, kasmet organizuoja KADIS rizikos veiksnių vertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį KADIS rizikos veiksnių vertinimą.

25. KADIS rizikai įvertinti gali būti naudojamos interaktyvios priemonės (kompiuterinės programos ir pan.).

26. KADIS rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama KADIS tvarkytojo vadovui. KADIS rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai yra šie:

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

26.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis KADIS elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kt.);

26.3. veiksniai, 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.

27. KADIS rizikos vertinimo metu atliekami darbai:

27.1. KADIS sudarančių informacinių išteklių inventorizacija;

27.2. įtakos KADIS veiklai vertinimas;

27.3. grėsmės ir pažeidimų analizė;

27.4. liekamosios rizikos vertinimas.

28. Elektroninės informacijos saugos priemonių parinkimo principai:

28.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

28.2. informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;

28.3. atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

29. Atsižvelgdamas į rizikos įvertinimo ataskaitą, KADIS valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame nustatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

30. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas KADIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

31. Siekiant užtikrinti saugos dokumentuose nustatytų reikalavimų įgyvendinimo organizavimą ir kontrolę, ne rečiau kaip kartą per dvejus metus organizuojamas informacinių technologijų saugos atitikties vertinimas.

32. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama KADIS tvarkytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato KADIS valdytojas.

33. Informacinių technologijų saugos atitikties vertinimo ataskaitas, pastebėtų trūkumų šalinimo plano kopijas KADIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

34. Programinės įrangos, skirtos KADIS apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

34.1. tarnybinėse stotyse ir vidinių KADIS naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo, stebėjimo realiu laiku priemonės;

34.2. KADIS komponentai be kenksmingos programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu rizikos vertinimo metu patvirtinama, kad šių komponentų rizika yra priimtina;

34.3. kenksmingos programinės įrangos aptikimo priemonės turi atsinaujinti automatiškai ne rečiau kaip kartą per 24 valandas. KADIS komponentų administratorius turi būti automatiškai informuojamas, kurie KADIS posistemiai, funkciškai savarankiškos sudedamosios dalys neatsinaujino laiku dėl kenksmingos programinės įrangos aptikimo.

35. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

35.1. tarnybinėse stotyse ir vidinių KADIS naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga, įtraukta į su KADIS valdytoju suderintą leistinos programinės įrangos sąrašą. Saugos įgaliotinis turi parengti, su informacinės sistemos valdytojo vadovu suderinti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti leistinos programinės įrangos sąrašą;

35.2. vidinių KADIS naudotojų kompiuterinėje įrangoje turi būti naudojama tik darbo (tarnybos) funkcijoms atlikti reikalinga programinė įranga;

35.3. tarnybinių stočių ir vidinių informacinių sistemų naudotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai turi būti operatyviai išbandomi ir įdiegiami;

35.4. saugos administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius KADIS posistemiuose, funkciškai savarankiškose sudedamosiose dalyse, vidinių KADIS naudotojų darbo vietų kompiuterinėje įrangoje. Apie įvertinimo rezultatus saugos administratorius turi informuoti saugos įgaliotinį;

35.5. programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

35.6. programinės įrangos diegimą, konfigūravimą, priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai – KADIS administratoriai arba tokias paslaugas teikiantys kvalifikuoti paslaugų teikėjai;

35.7. programinė įranga turi būti testuojama naudojant atskirą testavimo aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendraisiais reikalavimais saugumo priemonėms.

36. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių ir kt.) pagrindinės naudojimo nuostatos:

36.1. kompiuterių tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant užkardas, DOS ir DDOS atakų prevencijai skirtą įrangą bei įsilaužimų aptikimo ir prevencijos įrangą;

36.2. kompiuterių tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešajame ryšių tinkle naršančių vidinių KADIS naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

36.3. apsaugai nuo elektroninės informacijos nutekinimo turi būti naudojama duomenų srautų analizės ir kontrolės įranga, kuri šifruoja įeinančių ir išeinančių duomenų srautų duomenis.

37. Leistinos kompiuterių naudojimo ribos:

37.1. stacionarius kompiuterius leidžiama naudoti tik KADIS valdytojo ir KADIS tvarkytojų patalpose;

37.2. nešiojamiesiems kompiuteriams, išnešamiems iš KADIS valdytojo ar tvarkytojų patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, papildomas tapatybės patvirtinimas, prisijungimo ribojimai, rakinimo įrenginių naudojimas);

37.3. iš stacionarių ir nešiojamųjų kompiuterių ar elektroninės informacijos laikmenų, kurie perduodami remonto, techninės priežiūros paslaugų teikėjui arba nurašomi, turi būti neatkuriamai pašalinta visa nevieša elektroninė informacija.

38. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

38.1. elektroninė informacija teikiama (daugkartinio ir vienkartinio teikimo atvejais) KADIS nuostatuose nustatyta tvarka;

38.2. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą naudojamas šifravimas, virtualus privatus tinklas, skirtinės linijos, saugus elektroninių ryšių tinklas ar kitos priemonės, kuriomis užtikrinamas saugus elektroninės informacijos perdavimas;

38.3. elektroninė informacija automatiniu būdu turi būti teikiama ir (ar) gaunama tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas.

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

39.1. išsamios atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai kartą per savaitę, dalinės atsarginės duomenų kopijos – kiekvieną darbo dieną;

39.2. atsarginių kopijų darymas turi būti registruojamas kopijų darymo apskaitos žurnale;

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

39.4. atsarginės duomenų kopijos turi būti saugomos atskiroje patalpoje nei įrenginys, kuriuo elektroninė informacija buvo nukopijuota, ir laikomos užrakintoje nedegioje spintoje;

39.5. atsarginės laikmenos su KADIS programinės įrangos kopijomis turi būti laikomos kitose patalpose arba kitame pastate nei informacinių sistemų tarnybinės stotys;

39.6. atsarginių kopijų laikmenos turi būti žymimos taip, kad jas būtų galima identifikuoti;

39.7. elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, dėl kurių nebūtų galima neteisėtai atkurti elektroninės informacijos;

39.8. patekimas į KADIS tarnybinių stočių patalpas ir patalpas, kuriose saugomos atsarginės kopijos, galimas tik su asmens, atsakingo už atsarginių kopijų darymą, leidimu.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

40. Reikalavimai KADIS naudotojams, administratoriams ir saugos įgaliotiniui:

40.1. vidinių KADIS naudotojų, administratorių, saugos įgaliotinio kvalifikacija turi atitikti bendruosius ir specialiuosius reikalavimus, nustatytus jų pareigybių aprašymuose;

40.2. visi KADIS naudotojai privalo turėti darbo kompiuteriu, taikomosiomis programomis įgūdžių;

40.3. KADIS naudotojai privalo rūpintis KADIS ir joje tvarkomos elektroninės informacijos saugumu;

40.4. KADIS saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis;

40.5. KADIS saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, 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 ir taisyklių pažeidimą, jeigu nuo jos skyrimo praėjo mažiau kaip vieni metai;

40.6. administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, darbą su kompiuterių tinklais, gebėti užtikrinti jų saugą, išmanyti informacinių sistemų komponentų administravimo priežiūros pagrindus, būti susipažinę su saugos dokumentais ir laikytis jų reikalavimų.

41. KADIS naudotojų ir administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

41.1. KADIS naudotojams ir administratoriams turi būti periodiškai, bet ne rečiau kaip kartą per dvejus metus, organizuojami mokymai elektroninės informacijos saugos klausimais, įvairiais būdais primenama apie elektroninės informacijos saugos problemas (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems KADIS naudotojams, administratoriams ir pan.);

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

41.3. mokymai turi būti vykdomi pagal KADIS tvarkytojo patvirtintą mokymų planą. Mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kt. teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.). Mokymus gali vykdyti saugos įgaliotinis ar kitas KADIS valdytojo ar tvarkytojo valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, išmanantis elektroninės informacijos saugos užtikrinimo principus, arba elektroninės informacijos saugos mokymo paslaugų teikėjas;

41.4. už mokymų organizavimą atsakingas saugos įgaliotinis.

V SKYRIUS
KADIS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

42. Už KADIS naudotojų supažindinimą su šiais saugos nuostatais ir kitais saugos politiką įgyvendinančiais teisės aktais bei atsakomybe už saugos dokumentų pažeidimus yra atsakingas KADIS saugos įgaliotinis.

43. Vidinius KADIS naudotojus su saugos dokumentais supažindina saugos įgaliotinis. Kiti KADIS naudotojai su saugos dokumentais supažindinami elektroniniu būdu KADIS naudotojams pasiekiamame tinklalapyje.

44. KADIS naudotojai pirmojo prisijungimo prie KADIS metu turi patvirtinti, kad susipažino su saugos dokumentais ir sutinka laikytis jų reikalavimų. KADIS naudotojų patvirtinimai saugomi KADIS elektroniniame įvykių žurnale siekiant užtikrinti susipažinimo su saugos dokumentais įrodomumą.

45. Pakartotinai su saugos dokumentais KADIS naudotojai supažindinami tik iš esmės pasikeitus KADIS arba elektroninės informacijos saugą reglamentuojantiems teisės aktams.

Informacija apie pasikeitimus saugos politiką įgyvendinančiuose teisės aktuose siunčiama elektroniniu būdu.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

46. KADIS valdytojas saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Keičiami saugos dokumentai turi būti derinami su Lietuvos Respublikos vidaus reikalų ministerija. Keičiami saugos dokumentai gali būti nederinami su Lietuvos Respublikos vidaus reikalų ministerija tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika.

47. KADIS tvarkytojai saugos dokumentus turi persvarstyti (peržiūrėti) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos įvertinimą ar informacinių technologijų atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems KADIS pokyčiams.

_____

Pakeitimai:

1.
Lietuvos Respublikos teisingumo ministerija, Įsakymas
Nr. 1R-170, 2018-09-03, paskelbta TAR 2018-09-03, i. k. 2018-13847
Dėl teisingumo ministro 2016 m. vasario 3 d. įsakymo Nr. 1R-34 „Dėl Kalėjimų departamento prie Lietuvos Respublikos teisingumo ministerijos informacinės sistemos duomenų saugos nuostatų patvirtinimo, saugos įgaliotinio, administratorių skyrimo ir saugos politiką įgyvendinančių dokumentų rengimo“ pakeitimo