Suvestinė redakcija nuo 2023-01-01

Įsakymas paskelbtas: Žin. 2007, Nr. 105-4324, i. k. 1072050ISAK001K-289

Nauja redakcija nuo 2020-11-26:
Nr. 1K-385, 2020-11-24, paskelbta TAR 2020-11-25, i. k. 2020-24947

LIETUVOS RESPUBLIKOS FINANSŲ MINISTRAS

ĮSAKYMAS DĖL FINANSŲ MINISTERIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2007 m. spalio 3 d. Nr. 1K-289
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 12, 19 ir 31 punktais, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 6 punktu:

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

2. S k i r i u Finansų ministerijos informacinių sistemų saugos įgaliotiniu Finansų ministerijos Informacinių technologijų departamento vyriausiąjį specialistą, pagal pareigybės aprašymą atliekantį Finansų ministerijos informacinių sistemų saugos įgaliotinio funkcijas. Laikinai nesant saugos įgaliotinio dėl ligos, komandiruotės ar kitų objektyvių priežasčių, šias funkcijas laikinai atlieka Informacinių technologijų departamento direktorius.

FINANSŲ MINISTRAS RIMANTAS ŠADŽIUS

PATVIRTINTA
Lietuvos Respublikos finansų ministro
2007 m. spalio 3 d. įsakymu Nr. 1K-289
(Lietuvos Respublikos finansų ministro
2020 m. lapkričio 24 d. įsakymo
Nr. 1K-385 redakcija)

FINANSŲ MINISTERIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos finansų ministerijos informacinių sistemų duomenų saugos nuostatuose (toliau – Saugos nuostatai) reglamentuojama Lietuvos Respublikos finansų ministerijos (toliau – ministerija) valdomose ir tvarkomose valstybės informacinėse sistemose, vidaus administravimui skirtoje informacinėje sistemoje, interneto ir intraneto svetainėse (toliau kartu – IS) tvarkomos elektroninės informacijos saugos (kibernetinio saugumo) politika.

2. 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, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos 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 – Techniniai elektroninės informacijos saugos reikalavimai).

Punkto pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

3. IS elektroninės informacijos saugos (kibernetinio saugumo) politika įgyvendinama pagal IS valdytojo tvirtinamus IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentus:

3.1. Saugos nuostatus;

3.2. Saugaus elektroninės informacijos tvarkymo taisykles;

3.3. IS naudotojų administravimo taisykles;

3.4. IS veiklos tęstinumo valdymo planą.

4. IS elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetinės kryptys:

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

4.2. IS elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

4.3. IS kibernetinio saugumo užtikrinimas;

4.4. IS tvarkymo kontrolės užtikrinimas;

4.5. IS paslaugų ir naudojimosi IS elektronine informacija kontrolės užtikrinimas;

4.6. IS tvarkomų asmens duomenų apsauga;

4.7. IS veiklos tęstinumo užtikrinimas;

4.8. IS naudotojų mokymas.

5. IS elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo tikslai:

5.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti IS elektroninę informaciją;

5.2. užtikrinti IS elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, praradimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

5.3. vykdyti IS elektroninės informacijos saugos (kibernetinio saugumo) incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į IS elektroninės informacijos saugos (kibernetinio saugumo) incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai valdyti.

6. Saugos nuostatai taikomi:

6.1. Lietuvos Respublikos finansų ministerijai (Lukiškių g. 2, Vilnius), kuri yra šių IS valdytoja:

6.1.1. Valstybės biudžeto, apskaitos ir mokėjimų sistemos (toliau – VBAMS);

6.1.2. Europos Sąjungos struktūrinės paramos kompiuterinės informacinės valdymo ir priežiūros sistemos (toliau – SFMIS);

6.1.3. Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinės sistemos (toliau – VSAKIS);

6.1.4. Stebėsenos informacinės sistemos (toliau – SIS);

6.1.5. vidaus administravimui skirtos Administracinės informacinės sistemos (toliau – AIS);

6.1.6. Atvirųjų finansų informacinės sistemos (toliau – AFIS);

6.2. ministerijos valdomų valstybės informacinių sistemų tvarkytojams, nurodytiems IS nuostatuose:

6.2.1. VBAMS – ministerijai, kaip VBAMS tvarkytojai, ir kitiems VBAMS tvarkytojams, nurodytiems Valstybės biudžeto, apskaitos ir mokėjimų sistemos nuostatų, patvirtintų Lietuvos Respublikos finansų ministro 2006 m. balandžio 6 d. įsakymu Nr. 1K-152 „Dėl Valstybės biudžeto, apskaitos ir mokėjimų sistemos nuostatų patvirtinimo“ (toliau – Valstybės biudžeto, apskaitos ir mokėjimų sistemos nuostatai), 10 punkte;

6.2.2. SFMIS – tvarkytojams, nurodytiems Europos Sąjungos struktūrinės paramos kompiuterinės informacinės valdymo ir priežiūros sistemos nuostatų, patvirtintų Lietuvos Respublikos finansų ministro 2006 m. liepos 20 d. įsakymu Nr. 1K-263 „Dėl Europos Sąjungos struktūrinių fondų ir Europos Sąjungos sanglaudos fondo kompiuterinės informacinės valdymo ir priežiūros sistemos nuostatų patvirtinimo“ (toliau – Europos Sąjungos struktūrinės paramos kompiuterinės informacinės valdymo ir priežiūros sistemos nuostatai), 10 punkte;

6.2.3. VSAKIS – ministerijai, viešojo sektoriaus subjektams, atsakingiems už konsoliduotųjų ataskaitų parengimą, tvarkantiems tik savo lygio duomenis ir atliekantiems tik VSAKIS duomenų tvarkymo funkcijas;

6.2.4. SIS – ministerijai;

6.2.5. AIS – ministerijai;

6.2.6. AFIS – ministerijai;

6.3. ministerijos IS saugos įgaliotiniui;

6.4. ministerijos IS infrastruktūros administratoriams;

6.5. ministerijos IS administratoriams;

6.6. ministerijos IS naudotojams;

6.7. paslaugų, susijusių su IS, teikėjams;

6.8. vietiniams IS naudotojų administratoriams.

Papildyta papunkčiu:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

7. Saugos nuostatai netaikomi šioms ministerijos valdomoms IS:

7.1. Valstybės turto informacinei paieškos sistemai;

7.2. Apribojusių savo galimybę lošti asmenų registrui.

8. IS valdytojas atlieka IS nuostatuose nustatytas funkcijas, taip pat:

8.1. tvirtina IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentus, kitus dokumentus, susijusius su IS elektroninės informacijos sauga;

8.2. prižiūri ir kontroliuoja, kad IS būtų tvarkomos vadovaujantis IS nuostatais, IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentais ir kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais;

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

8.4. koordinuoja IS tvarkytojų darbą įgyvendinant IS elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus;

8.5. nagrinėja IS tvarkytojų pasiūlymus dėl IS elektroninės informacijos saugos (kibernetinio saugumo) priemonių tobulinimo ir priima sprendimus dėl jų;

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

8.7. užtikrina elektroninės informacijos ir duomenų tvarkymo bei duomenų teikimo IS duomenų gavėjams teisėtumą ir duomenų saugą;

8.8. teikia Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – NKSC) techninę informaciją, reikalingą IS kibernetiniam saugumui įvertinti, NKSC reikalavimu nurodytais formatais ir terminais arba savo iniciatyva;

8.9. atlieka kitas Saugos nuostatuose, Bendrųjų elektroninės informacijos saugos reikalavimų apraše ir 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), nustatytas funkcijas.

9. IS tvarkytojai atlieka IS nuostatuose nustatytas funkcijas, taip pat:

9.1. užtikrina IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų ir kitų IS valdytojo priimtų teisės aktų, susijusių su IS sauga ir kibernetiniu saugumu, tinkamą įgyvendinimą IS tvarkytojo įstaigos tvarkomose IS;

9.2. užtikrina IS elektroninės informacijos saugą (kibernetinį saugumą) IS tvarkytojo įstaigos tvarkomose IS;

9.3. užtikrina elektroninės informacijos, esančios IS duomenų bazėse, sistemų kataloguose, saugą;

9.4. užtikrina saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

9.5. teikia IS valdytojui pasiūlymus dėl IS elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo;

9.6. planuoja ir įgyvendina priemones, mažinančias IS duomenų atskleidimo ir praradimo riziką bei užtikrinančias prarastų duomenų atkūrimą ir duomenų apsaugą nuo klastojimo;

9.7. užtikrina nepertraukiamą IS veikimą;

9.8. užtikrina IS elektroninės informacijos ir duomenų tvarkymo bei duomenų teikimo IS duomenų gavėjams teisėtumą;

9.9. valdo IS elektroninės informacijos saugos (kibernetinio saugumo) incidentus;

9.10. atlieka kitas IS valdytojo pavestas IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentuose ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, jiems priskirtas funkcijas.

10. Tais atvejais, kai IS valdytoja yra ministerija, o IS tvarkytoja – kita institucija, IS valdytoja turi teisę pavesti IS tvarkytojai parengti ir pateikti IS valdytojai tvirtinti Saugos nuostatų 3.1–3.4 papunkčiuose nurodytų dokumentų projektus.

11. Už IS saugą (kibernetinį saugumą) pagal kompetenciją atsako IS valdytojas ir IS tvarkytojai.

12. IS valdytojas atsako už IS elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

13. IS tvarkytojai atsako už reikiamų administracinių, techninių ir organizacinių IS elektroninės informacijos saugos (kibernetinio saugumo) priemonių įgyvendinimą, užtikrinimą ir laikymąsi IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentuose nustatyta tvarka.

14. IS saugos įgaliotinis – ministerijos valstybės tarnautojas ar pagal darbo sutartį dirbantis darbuotojas (toliau – darbuotojas (-ai) atlieka Bendrųjų elektroninės informacijos saugos reikalavimų apraše nustatytas funkcijas, taip pat:

14.1. koordinuoja ir prižiūri IS elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimą IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentuose nustatyta tvarka;

14.2. teikia IS valdytojui siūlymus dėl:

14.2.1. IS administratorių, vietinių IS naudotojų administratorių skyrimo ir reikalavimų jiems nustatymo;

Papunkčio pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

14.2.2. IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų priėmimo, keitimo ar pripažinimo netekusiais galios;

14.2.3. informacinių technologijų saugos atitikties vertinimo atlikimo;

14.3. koordinuoja IS elektroninės informacijos saugos (kibernetinio saugumo) incidentų, įvykusių IS, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, elektroninės informacijos saugos (kibernetinio saugumo) incidentus, neteisėtas veikas, susijusias su šiais incidentais, išskyrus atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

14.4. atlieka Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

14.5. duoda IS administratoriui, vietiniam IS naudotojų administratoriui ar IS infrastruktūros administratoriui ir IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų įgyvendinimu;

Papunkčio pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

14.6. teisės aktų nustatyta tvarka organizuoja IS rizikos vertinimą ir rizikos vertinimo ataskaitos parengimą;

14.7. supažindina IS administratorius, vietinius IS naudotojų administratorius ir IS infrastruktūros administratorius su IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentuose nustatytais reikalavimais ir atsakomybe už reikalavimų nesilaikymą;

Papunkčio pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

14.8. organizuoja IS naudotojų supažindinimą su Saugos nuostatų 3.1–3.3 papunkčiuose nurodytų dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą;

14.9. organizuoja IS naudotojų mokymus IS elektroninės informacijos saugos (kibernetinio saugumo) klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

14.10. atlieka kitas ministerijos IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentuose ir kituose teisės aktuose, reglamentuojančiuose ministerijos duomenų tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas;

14.11. užtikrina ministerijos IS elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų atitiktį Lietuvos Respublikos teisės aktų reikalavimams.

15. IS administratorius – ministerijos darbuotojas atlieka Bendrųjų elektroninės informacijos saugos reikalavimų apraše nustatytas funkcijas, taip pat:

15.1. užtikrina IS techninės ir programinės įrangos įdiegimą, atnaujinimą ir veikimą;

15.2. diegia ir prižiūri programinę įrangą, reikalingą IS naudotojų funkcijoms atlikti;

15.3. registruoja IS naudotojus, skiria registravimosi vardus, nustato IS naudotojams prieigos prie IS teises;

15.4. pagal kompetenciją rengia pasiūlymus dėl IS kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir IS elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo;

15.5. užtikrina priskirtos IS ar jos komponentų (posistemių, duomenų bazių valdymo sistemų, taikomųjų programų sistemų) tinkamą veikimą, priežiūrą ir IS elektroninės informacijos saugą (kibernetinį saugumą), rengia ir atnaujina IS sąrankos aprašymo dokumentaciją, pagal kompetenciją nustato IS pažeidžiamas vietas, parenka ir diegia saugos priemones bei užtikrina jų atitiktį IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų reikalavimams;

15.6. informuoja IS saugos įgaliotinį apie IS elektroninės informacijos saugos (kibernetinio saugumo) incidentus, teikia pasiūlymus dėl šių incidentų pašalinimo;

15.7. daro IS duomenų bazės atsargines kopijas, atlieka informacijos atkūrimo iš kopijų bandymus (IS administratorius, kuriam priskirta ši funkcija);

15.8. teikia IS valdytojui ir IS saugos įgaliotiniui pasiūlymus dėl IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų priėmimo, keitimo ar pripažinimo netekusiais galios;

15.9. tvarkydamas duomenis, įskaitant ir asmens duomenis, IS elektroninę informaciją, dokumentus ir jų kopijas, saugo tų duomenų ir informacijos paslaptį, neatskleidžia, neperduoda tvarkomų duomenų ir informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija. Ši pareiga galioja ir nutraukus su ministerijos IS duomenų, informacijos, dokumentų ir jų kopijų tvarkymu susijusią veiklą;

15.10. neperduoda neįgaliotiems asmenims prisijungimo vardų ir slaptažodžių, IS naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitą IS tvarkomą elektroninę informaciją, ir nesudaro kitų sąlygų susipažinti su IS tvarkoma elektronine informacija;

15.11. atlieka IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentuose ir kituose teisės aktuose, reglamentuojančiuose IS saugą ir kibernetinį saugumą, priskirtas funkcijas.

15^1. Vietinis IS naudotojų administratorius – IS tvarkytojo įstaigos darbuotojas:

15^1.1. registruoja savo įstaigos IS naudotojus, skiria registravimosi vardus, nustato IS naudotojams prieigos prie IS teises;

15^1.2. informuoja IS saugos įgaliotinį apie IS elektroninės informacijos saugos (kibernetinio saugumo) incidentus, teikia pasiūlymus dėl šių incidentų pašalinimo;

15^1.3. tvarkydamas asmens duomenis saugo tų duomenų ir informacijos paslaptį, neatskleidžia, neperduoda tvarkomų duomenų ir informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija. Ši pareiga galioja ir nutraukus su ministerijos IS duomenų, informacijos, dokumentų ir jų kopijų tvarkymu susijusią veiklą;

15^1.4. neturi teisės perduoti neįgaliotiems asmenims prisijungimo vardų ir slaptažodžių, IS naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitą IS tvarkomą elektroninę informaciją, ir neturi teisės sudaryti sąlygų susipažinti su IS tvarkoma elektronine informacija.

Papildyta punktu:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

16. IS infrastruktūros administratorius – ministerijos darbuotojas atlieka Bendrųjų elektroninės informacijos saugos reikalavimų apraše nustatytas funkcijas, taip pat:

16.1. administruoja IS veikimą užtikrinančią techninę ir programinę įrangą, infrastruktūrą bei informacinių technologijų paslaugas, užtikrina IS infrastruktūros veikimą, informacinių

technologijų paslaugų teikimą ir jų naudotojų registravimą, registravimosi vardų skyrimą ir prieigos prie IS infrastruktūros išteklių teisių suteikimą;

16.2. administruoja priskirtus IS komponentus (kompiuterius, serverius, operacines sistemas, užkardas (angl. *firewall*), įsilaužimo aptikimo sistemas, duomenų perdavimo tinklus, duomenų perdavimo tinklų techninę įrangą, spausdinimo techninę įrangą, vaizdo stebėjimo techninę įrangą), parengia ir keičia IS komponentų sąrankos aprašymo dokumentaciją, vykdo pažeidžiamų vietų nustatymą ir saugos priemonių parinkimą bei užtikrina jų atitiktį IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų reikalavimams;

16.3. užtikrina kompiuterizuotų darbo vietų veikimą, diegia ir konfigūruoja kompiuterizuotų darbo vietų programinę įrangą, diegia kompiuterizuotų darbo vietų programinės įrangos atnaujinimus, stebi ir analizuoja kompiuterizuotų darbo vietų veikimą;

16.4. pagal ministerijos Informacinių technologijų departamento (toliau – ITD) direktoriaus patvirtintą Rezervinio kopijavimo į išorines laikmenas procedūrų vadovą vykdo rezervinį (fizinių serverių, virtualiųjų serverių ir kitų komponentų) kopijavimą, užtikrina IS administratorių sukurtų rezervinių kopijų įrašymą į magnetines laikmenas ir saugojimą nutolusioje patalpoje, archyve esančių kopijų saugojimą;

16.5. pagal kompetenciją rengia pasiūlymus dėl IS kūrimo, palaikymo, priežiūros ir IS elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų įgyvendinimo;

16.6. informuoja IS saugos įgaliotinį apie IS elektroninės informacijos saugos (kibernetinio saugumo) incidentus ir teikia pasiūlymus dėl šių incidentų pašalinimo;

16.7. tvarkydamas IS duomenis, įskaitant ir asmens duomenis, IS elektroninę informaciją, dokumentus ir jų kopijas, saugo tų duomenų ir informacijos paslaptį, neatskleidžia, neperduoda tvarkomų duomenų ir informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija. Ši pareiga galioja ir nutraukus su ministerijos IS duomenų, informacijos, dokumentų ir jų kopijų tvarkymu susijusią veiklą;

16.8. neperduoda neįgaliotiems asmenims prisijungimo vardų ir slaptažodžių, IS naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitą IS tvarkomą elektroninę informaciją, ir nesudaro kitų sąlygų susipažinti su IS tvarkoma elektronine informacija;

16.9. teikia IS valdytojui ir IS saugos įgaliotiniui pasiūlymus dėl IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų priėmimo, keitimo ar pripažinimo netekusiais galios;

16.10. užtikrina tinkamą Saugos nuostatuose nustatytų funkcijų, susijusių su IS priežiūra ir informacinių technologijų paslaugų teikimu, atlikimą;

16.11. atlieka IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentuose ir kituose teisės aktuose, reglamentuojančiuose IS saugą ir kibernetinį saugumą, priskirtas funkcijas;

16.12. registruoja AIS naudotojus, skiria registravimosi vardus, nustato naudotojų prieigos teises.

Papildyta papunkčiu:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

17. IS administratoriai, vietiniai IS naudotojų administratoriai ir IS infrastruktūros administratoriai, atlikdami jiems priskirtas funkcijas, vadovaujasi Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytais reikalavimais.

Punkto pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

18. IS administratoriai, vietiniai IS naudotojų administratoriai ir IS infrastruktūros administratoriai atsakingi už tinkamą IS elektroninės informacijos saugos (kibernetinio saugumo) dokumentuose nustatytų funkcijų atlikimą.

Punkto pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

19. IS administratoriai, vietiniai IS naudotojų administratoriai ir IS infrastruktūros administratoriai privalo vykdyti visus IS saugos įgaliotinio nurodymus ir pavedimus dėl IS elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo, pagal kompetenciją reaguoti į IS elektroninės informacijos saugos (kibernetinio saugumo) incidentus ir nuolat teikti IS saugos įgaliotiniui informaciją apie pagrindinių IS saugos užtikrinimo komponentų būklę.

Punkto pakeitimai:

Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

20. Atlikdami IS sąrankos pakeitimus, IS administratoriai turi laikytis IS pokyčių valdymo tvarkos, nustatytos IS valdytojo tvirtinamose IS saugaus elektroninės informacijos tvarkymo taisyklėse.

21. IS vidinių naudotojų – ministerijos darbuotojų ar IS išorinių naudotojų – kitų asmenų, kuriems suteikta teisė naudotis ministerijos tvarkomų IS elektronine informacija ir (ar) ją tvarkyti, funkcijos:

21.1. vadovaudamiesi IS valdytojo patvirtintais IS nuostatais, Saugos nuostatų 3.1–3.3 papunkčiuose nurodytų dokumentų reikalavimais, IS duomenų teikimo sutartimis, IS naudojimo instrukcijomis ir pareigybių aprašymais, naudoja ministerijos IS;

21.2. tvarko IS elektroninę informaciją ir naudojasi kitomis ministerijos IS teikiamomis galimybėmis pagal nustatytą funkcijoms atlikti reikalingą IS prieigos teisių lygmenį, kuris apriboja naudojimosi elektronine informacija apimtį;

21.3. tvarko tik tą elektroninę informaciją, kuri IS naudotojui prieinama naudojant konkrečios IS programinę įrangą;

21.4. pagal kompetenciją rengia pasiūlymus dėl IS modernizavimo ir IS elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo;

21.5. pastebėję IS elektroninės informacijos saugos (kibernetinio saugumo) pažeidimų, nusikalstamos veikos požymių, neveikiančių arba netinkamai veikiančių IS elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo priemonių, privalo nedelsdami apie tai pranešti IS administratoriui, IS infrastruktūros administratoriui ir (arba) IS saugos įgaliotiniui;

21.6. tvarkydami duomenis, įskaitant ir asmens duomenis, IS elektroninę informaciją, dokumentus ar jų kopijas, saugo tų duomenų ir informacijos paslaptį, neatskleidžia, neperduoda tvarkomų duomenų ir informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija. Ši pareiga galioja ir nutraukus su ministerijos IS duomenų, informacijos, dokumentų ir jų kopijų tvarkymu susijusią veiklą;

21.7. neperduoda neįgaliotiems asmenims prisijungimo vardų ir slaptažodžių, IS naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitą IS tvarkomą elektroninę informaciją, ir nesudaro kitų sąlygų susipažinti su IS tvarkoma elektronine informacija;

21.8. atlieka kitas IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentuose priskirtas funkcijas ir kitus IS valdytojo, IS saugos įgaliotinio, IS administratoriaus ir IS infrastruktūros administratoriaus nurodymus, susijusius su IS naudojimu ir IS elektroninės informacijos sauga (kibernetiniu saugumu).

22. Paslaugų, susijusių su ministerijos IS, teikėjai privalo pasirašyti finansų ministro įsakymu nustatytos formos įsipareigojimą saugoti duomenų, įskaitant ir asmens duomenis, informacijos paslaptį. Įsipareigojimas saugoti asmens duomenų ir informacijos paslaptį galioja ir pasibaigus paslaugų teikimo laikui ar nutraukus šią veiklą.

23. Teisės aktai, kuriais vadovaujantis tvarkoma IS elektroninė informacija ir užtikrinama IS elektroninės informacijos sauga (kibernetinis saugumas):

23.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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);

23.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

23.3. Kibernetinio saugumo įstatymas;

23.4. Valstybės informacinių išteklių valdymo įstatymas;

23.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

23.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

23.7. Techniniai elektroninės informacijos saugos reikalavimai;

23.8. 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);

Papunkčio pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

23.9. Valstybės biudžeto, apskaitos ir mokėjimų sistemos nuostatai;

23.10. Europos Sąjungos struktūrinės paramos kompiuterinės informacinės valdymo ir priežiūros sistemos nuostatai;

23.11. Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinės sistemos nuostatai, patvirtinti Lietuvos Respublikos finansų ministro 2011 m. gegužės 13 d. įsakymu Nr. 1K-182 „Dėl Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinės sistemos nuostatų patvirtinimo“;

23.12. Stebėsenos informacinės sistemos nuostatai, patvirtinti Lietuvos Respublikos finansų ministro 2020 m. sausio 10 d. įsakymu Nr. 1K-1 „Dėl Stebėsenos informacinės sistemos nuostatų patvirtinimo“;

23.13. Atvirųjų finansų informacinės sistemos nuostatai, patvirtinti Lietuvos Respublikos finansų ministro 2020 m. sausio 22 d. įsakymu Nr. 1K-7 „Dėl Atvirųjų finansų informacinės sistemos steigimo“;

23.14. Lietuvos standartai LST EN ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“, LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ ir kiti standartai;

23.15. Lietuvos Respublikos teisės aktai, reglamentuojantys elektroninės informacijos tvarkymo teisėtumą, IS valdytojo ir tvarkytojų veiklą ir elektroninės informacijos saugos valdymą, Europos Sąjungos ir Lietuvos Respublikos teisės aktai, reglamentuojantys asmens duomenų apsaugą ir tvarkymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

24. Ministerijos IS tvarkomos elektroninės informacijos svarbos kategorija, ministerijos IS kategorijos ir priskyrimo tam tikrai kategorijai kriterijai nurodyti Saugos nuostatų priede.

25. IS saugos įgaliotinis, atsižvelgdamas į NKSC interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, kasmet organizuoja IS rizikos vertinimą. Įdiegus IS pokyčius (sistemos pakeitimai, konfigūracijų pakeitimai, programinės įrangos versijų naujinimas, papildymas naujomis taikomosiomis programomis, taikomųjų programų pašalinimas ir kt.) arba atlikus esminius organizacinius ar sisteminius pokyčius ir nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis IS rizikos vertinimas.

26. Organizuojant IS rizikos vertinimą turi būti paskirtas už rizikos vertinimo proceso priežiūrą ir tobulinimą atsakingas asmuo arba keli asmenys ir nustatyti jiems taikomi kvalifikaciniai reikalavimai. Atsakingu asmeniu gali būti skiriamas IS tvarkytojo darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros ir nuolatinio tobulinimo paslaugas teikiančiu subjektu.

27. IS rizikos vertinimo metu įvertinami rizikos veiksniai, galintys turėti įtakos IS elektroninės informacijos saugai (kibernetiniam saugumui), jų galima žala, pasireiškimo tikimybė ir pobūdis, galimi rizikos valdymo būdai, rizikos priimtinumo kriterijai.

28. Svarbiausi IS rizikos veiksniai:

28.1. 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, netinkamas veikimas ir kita);

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

28.3. 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.

29. IS rizikos veiksniams įvertinti naudojama kokybinė rizikos vertinimo sistema vadovaujantis metodika, pateikta NKSC interneto svetainėje skelbiamame Rizikos analizės vadove, ir Lietuvos ir tarptautiniais „Informacinės technologijos. Saugumo metodai“ grupės standartais:

29.1. IS rizikos įvertinimo rezultatai ir priemonės, reikalingos siekiant išvengti rizikos veiksnių, išdėstomi IS rizikos vertinimo ataskaitoje, kuri pateikiama IS valdytojo vadovui ir IS tvarkytojų vadovams.

29.2. IS rizikos įvertinimo ataskaita rengiama vertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus.

29.3. Rizikos veiksniai ir nustatyta rizikos tikimybė išdėstomi prioriteto tvarka pagal svarbą, kuri nustatoma atsižvelgiant į atliktą rizikos vertinimą.

30. Atsižvelgdamas į IS rizikos įvertinimo ataskaitą, IS valdytojas prireikus tvirtina IS rizikos vertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis IS rizikos valdymo priemonėms įgyvendinti.

31. Informacinių technologijų saugos atitikties vertinimo organizavimas:

31.1. Siekiant užtikrinti IS saugos dokumentuose nustatytų IS elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų įgyvendinimo organizavimą ir kontrolę, ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip, organizuojamas informacinių technologijų saugos atitikties vertinimas.

31.2. Informacinių technologijų saugos atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka.

31.3. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama IS valdytojo vadovui ir IS tvarkytojų vadovams.

31.4. Atlikus informacinių technologijų saugos atitikties vertinimą, prireikus rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus plano vykdytojus paskiria ir įgyvendinimo terminus nustato IS valdytojo vadovas.

32. IS atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

33. IS rizikos vertinimo ataskaitos, IS rizikos vertinimo ir rizikos valdymo priemonių plano, IS informacinių technologijų saugos atitikties vertinimo ataskaitos, taip pat pastebėtų trūkumų šalinimo plano kopijas IS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo dienos turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatuose, patvirtintuose Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl

Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

34. Atsižvelgiant į atlikto IS rizikos vertinimo rezultatus, taip pat jeigu informacinių technologijų saugos atitikties vertinimo metu nustatoma kibernetinių incidentų valdymo ir šalinimo, institucijos nepertraukiamos veiklos užtikrinimo trūkumų, atitinkamai turi būti tobulinamas IS veiklos tęstinumo valdymo planas. Šio plano veiksmingumo išbandymo rezultatai išdėstomi šio plano veiksmingumo išbandymo ataskaitoje ir pastebėtų trūkumų ataskaitoje, kurių kopijos ne vėliau kaip per 5 darbo dienas nuo šių dokumentų priėmimo dienos pateikiamos NKSC.

35. IS valdytojai turi teisę informacinių išteklių rizikos vertinimą atlikti kartu su informacinių technologijų saugos atitikties vertinimu.

36. IS elektroninės informacijos saugos (kibernetinio saugumo) priemonės (techninės, programinės, organizacinės ir kitos IS elektroninės informacijos saugos priemonės) parenkamos vadovaujantis šiais principais:

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

36.2. liekamoji rizika turi būti sumažinta iki priimtino lygio;

36.3. atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės IS elektroninės informacijos saugos (kibernetinio saugumo) priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

37. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai nustatomi pagal Saugos nuostatų 24 punkte nustatytas IS svarbos kategorijas ir vadovaujantis Saugos nuostatų 23 punkte nurodytais teisės aktais ir standartais.

38. Kibernetinio saugumo priemonės, nurodytos Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo priede, turi būti diegiamos atsižvelgiant į naujausius technikos laimėjimus, vadovaujantis gamintojo pateikiama bent viena gerosios saugumo praktikos rekomendacija.

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

40. Už IS veikimą užtikrinančios techninės ir programinės įrangos administravimą ir priežiūrą yra atsakingi ITD darbuotojai, kuriems priskirtos atitinkamos IS administratoriaus ir (arba) IS infrastruktūros administratoriaus funkcijos.

41. Programinės įrangos, skirtos IS nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

41.1. IS tarnybinėse stotyse ir kompiuterinėse darbo vietose turi būti įdiegtos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai ir operatyviai atnaujinamos automatiniu būdu. Ilgiausias leidžiamas priemonių neatnaujinimo laikas – 5 darbo dienos. Kompiuterio operacinės sistemos kritinės pataisos diegiamos ne vėliau kaip per 5 darbo dienas nuo jų išleidimo dienos.

41.2. IS tarnybinėse stotyse, kuriose turi būti užtikrinta didelė greitaveika (pvz., duomenų bazių tarnybinės stotys) ir kurios yra izoliuotame kompiuterių tinklo segmente, kenksmingos programinės įrangos aptikimo priemonės gali būti nediegiamos.

41.3. IS turi būti naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų.

41.4. Antivirusinės programinės įrangos virusų parašų bazės automatinio atnaujinimo ir kompiuterių operacinių sistemų kritinių pataisų diegimo terminai netaikomi toms kompiuterinėms

darbo vietoms, kurios yra laikinai nenaudojamos. Pradėjus naudoti kompiuterines darbo vietas, visos pataisos įdiegiamos per 3 darbo dienas.

41.5. Detalios programinės įrangos, skirtos IS nuo kenksmingos programinės įrangos apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai (ilgiausias leidžiamas neatnaujinimo laikas ir kt.) nustatomi IS saugaus elektroninės informacijos tvarkymo taisyklėse.

42. Programinės įrangos, įdiegtos kompiuterinėse darbo vietose ir tarnybinėse stotyse, naudojimo nuostatos:

42.1. Turi būti naudojama tik legali IS funkcijoms atlikti būtina programinė įranga.

42.2. Turi būti naudojama gamintojo palaikymą turinti programinė įranga.

42.3. Programinė įranga turi būti prižiūrima ir nuolatos atnaujinama.

42.4. Operacinių sistemų ir taikomųjų programų sąranka parenkama tokiu būdu, kad būtų užtikrintas didžiausias saugumo lygis, sustabdomi nereikalingi darbui procesai.

42.5. IS naudotojų paskyros yra ribotų teisių, kurios neleidžia įdiegti papildomos programinės įrangos ir keisti sistemos, kompiuterio ar programinės įrangos sisteminių nustatymų, nebent tai nustatyta IS naudotojo pareigybės aprašyme. IS administratoriaus teisės gali būti suteikiamos išimties tvarka, pateikiant prašymą ITD, nurodant motyvuotą pagrindą.

42.6. Programinę įrangą diegia, atnaujina ir kontroliuoja IS infrastruktūros administratoriai arba IS administratoriai (pagal atliekamas funkcijas). Paslaugų teikėjai programinę įrangą gali atnaujinti tik dalyvaujant IS infrastruktūros administratoriui arba IS administratoriui.

42.7. Serveriuose, IS administratorių, IS infrastruktūros administratorių, ministerijos darbuotojų kompiuterinėse darbo vietose naudojama ITD direktoriaus sprendimu į ministerijoje naudojamos tipinės programinės įrangos sąrašą įtraukta programinė įranga.

42.8. Programinės įrangos, nesusijusios su ministerijos veikla ar naudojamų IS funkcijomis (žaidimų, bylų siuntimo, pokalbių programų ir pan.), naudojimas draudžiamas.

42.9. Programinės įrangos testavimas negali būti vykdomas su realiais duomenimis.

42.10. Programinės įrangos atnaujinimai prieš diegiant gamybinėje aplinkoje turi būti ištestuoti testavimo aplinkoje.

42.11. Turi būti įdiegta prieigos prie IS elektroninės informacijos registruojantis, suteikiant prieigos teises ir slaptažodžius sistema.

42.12. Turi būti įgyvendinta prievolė sudaryti slaptažodžius vadovaujantis slaptažodžių sudarymo reikalavimais. IS naudotojų slaptažodžiai turi būti keičiami ne rečiau kaip kas tris mėnesius, IS administratorių, vietinių IS naudotojų administratorių ir IS infrastruktūros administratorių slaptažodžiai – ne rečiau kaip kas du mėnesius.

Papunkčio pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

42.13. Turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie IS elektroninės informacijos, atliktus veiksmus.

43. Kompiuterių tinklo ir tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita) pagrindinės naudojimo nuostatos:

43.1. IS elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant užkardas, užkardų įvykių žurnalai turi būti reguliariai analizuojami.

43.2. Pirmos ir antros svarbos kategorijoms priskirtoms IS turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: struktūrizuotų užklausų kalbos įsiskverbties (angl. *SQL injection*), įterptinių instrukcijų atakų (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), paskirstyto atsisakymo aptarnauti (angl. *DDOS*) ir kitų, priemonės; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP)*) interneto svetainėje www.owasp.org.

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

43.4. IS serveriai ir administruoti naudojami kompiuteriai negali turėti tiesioginio ryšio su internetu, jei toks ryšys nėra būtinas IS veikimui.

43.5. Prie pirmos ir antros svarbos kategorijų priskirtų IS serveriai turi būti atskiruose loginiuose kompiuterių tinkluose.

43.6. Ribojama arba blokuojama prieiga prie operacinės sistemos prievadų.

43.7. Turi būti naudojama duomenų srautų analizės ir kontrolės įranga, padedanti nustatyti galimų informacijos saugos incidentų priežastis, taip pat naudojama saugos incidentų prevencijai.

44. Pirmos ir antros svarbos kategorijoms priskirtų IS tarnybinių stočių, kuriose yra svetainės, svetainių saugos parametrai turi būti teigiamai įvertinti naudojant NKSC rekomenduojamą testavimo priemonę.

45. Tarnybinės stotys, kuriose yra svetainės, neturi rodyti svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį.

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

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

48. Tarnybinėse stotyse draudžiama saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai.

49. Belaidžio tinklo naudojimas:

49.1. Naudojami tik atitinkantys techninius kibernetinio saugumo reikalavimus belaidžio tinklo įrenginiai.

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

49.3. Prisijungti prie belaidžio tinklo turi būti taikomas ryšių ir IS naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) arba TLS (angl. *Transport Layer Security*) protokolas ir uždrausti visi nebūtini valdymo protokolai.

50. Siekiant užtikrinti IS elektroninės informacijos saugą (kibernetinį saugumą) ir tinkamą jų veikimą, kaupiami ir analizuojami žurnalų įrašai (angl. *log file*). Žurnalų įrašai kaupiami ir analizuojami naudojant sisteminių žurnalų įrašų valdymo sistemą.

51. Detalios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos IS saugaus elektroninės informacijos tvarkymo taisyklėse.

52. Leidžiamos kompiuterių naudojimo ribos:

52.1. Stacionarieji ir nešiojamieji IS naudotojų kompiuteriai ir kiti mobilieji įrenginiai turi būti naudojami tik tiesioginėms pareigoms atlikti.

52.2. Iš kompiuterių ir kitų mobiliųjų įrenginių, kurie perduodami taisyti trečiosioms šalims, techninei priežiūrai atlikti ar nurašomi, turi būti neatkuriamai pašalinti visi IS duomenys ir informacija.

52.3. IS naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

52.4. IS administruoti naudojami kompiuteriai prie elektros tinklo turi būti prijungti naudojant nepertraukiamo maitinimo šaltinius.

53. Ministerijos nešiojamųjų kompiuterių saugojimo, išdavimo ir naudojimo tvarka nustatyta Finansų ministerijos nešiojamųjų kompiuterių saugojimo, išdavimo ir naudojimo taisyklėse, patvirtintose Lietuvos Respublikos finansų ministerijos valstybės sekretoriaus 2005 m. vasario 4 d. potvarkiu Nr. 2K-004 „Dėl Finansų ministerijos nešiojamų kompiuterių saugojimo, išdavimo ir naudojimo taisyklių patvirtinimo“.

54. Ministerijoje taikomos šios nešiojamųjų kompiuterių ir mobiliųjų įrenginių informacijos apsaugos priemonės:

54.1. Leidžiama naudoti tik IS valdytojo nustatytus saugumo reikalavimus atitinkančius mobiliuosius įrenginius;

54.2. Turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas ir pan.).

54.3. Turi būti naudojami šie slaptažodžiai – IS naudotojo slaptažodis ir administravimo slaptažodis.

54.4. Kaip papildoma duomenų saugos priemonė (naudojant kompiuterį už ministerijos ribų) gali būti naudojama programinė įranga, skirta standžiojo disko duomenims šifruoti.

54.5. Naudojant nešiojamuosius kompiuterius ir mobiliuosius įrenginius, draudžiama jungtis prie nežinomų ar nepatikimų bevielių kompiuterių tinklų, naršyti pavojingose ar nepatikimose interneto svetainėse.

54.6. Draudžiama nešiojamuosiuose kompiuteriuose ir mobiliuosiuose įrenginiuose saugoti IS informaciją (nešiojamieji kompiuteriai ir mobilieji įrenginiai gali būti naudojami tik prisijungt prie stacionariojo darbo kompiuterio).

55. Ministerijos IS naudotojams gali būti suteikiama nuotolinio prisijungimo prie ministerijos IS galimybė:

55.1. Jungiantis prie ministerijos vidinio tinklo išteklių nuotoliniu būdu, turi būti naudojamas šifruotas prisijungimas ir papildomos tapatybės patvirtinimo priemonės – dviejų lygių autentifikacija.

55.2. Nuotolinio prisijungimo teisė ministerijos darbuotojui suteikiama vadovaujantis Nuotolinio darbo Lietuvos Respublikos finansų ministerijoje taisyklėmis, patvirtintomis Lietuvos Respublikos finansų ministro 2018 m. spalio 1 d. įsakymu Nr. 1K-331 „Dėl Nuotolinio darbo Lietuvos Respublikos finansų ministerijoje taisyklių patvirtinimo“ (toliau – Nuotolinio darbo taisyklės).

55.3. Viešaisiais ryšių tinklais perduodamos informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualųjį privatų tinklą (angl. *Virtual private network, VPN*).

55.4. Ministerijos darbuotojų nustatytų pareigų (funkcijų) ar jų dalies atlikimo dalį darbo laiko ne nuolatinėje darbo vietoje sąlygos ir tvarka reglamentuota Nuotolinio darbo taisyklėse;

55.5. IS vidiniams naudotojams jungiantis prie VBAMS Valstybės iždo konsoliduoto sąskaitų valdymo posistemio (toliau – VIKSVA posistemis) E. iždo funkcinės srities vidinės dalies, naudojama Valstybės informacinių išteklių sąveikumo platformos (VIISP) autentifikacija, o nesant galimybės ja naudotis – alternatyvius vidinės dalies autentifikavimo funkcinis sprendimas.

Papildyta papunkčiu:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

56. Metodai, kuriais užtikrinamas saugus IS elektroninės informacijos teikimas ir (ar) gavimas:

56.1. Elektroninė informacija iš susijusių registrų, informacinių sistemų gaunama ir teikiama susijusiems registrams, informacinėms sistemoms tik pagal duomenų teikimo ir gavimo sutartis nustatant duomenų naudojimo tikslus ir sąlygas, duomenų teikimo ar gavimo būdus, laiką ir periodiškumą, perduodamų duomenų specifikacijas ir tvarką.

56.2. Prieigos prie IS elektroninės informacijos teises gali suteikti IS administratorius arba vietinis IS naudotojų administratorius. IS naudotojams suteikiamos tik jų funkcijoms atlikti būtinos teisės.

Papunkčio pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

56.3. IS naudotojai jungiasi prie IS naudodami tik IS programinę įrangą, naudodamiesi techninėmis ir programinėmis priemonėmis, užtikrinančiomis saugų duomenų perdavimą kompiuterių tinklais.

56.4. Prieiga prie IS elektroninės informacijos leidžiama tik per registravimosi slaptažodžių sistemą. Prieigos prie IS elektroninės informacijos valdymas reglamentuotas IS naudotojų administravimo taisyklėse.

56.5. Prieiga prie IS suteikiama tik registruotiems ir turintiems teisę naudotis IS naudotojams.

56.6. IS naudotojui turi būti leista atlikti tik tuos veiksmus, kuriuos atlikti jam yra suteiktos teisės.

56.7. Visi IS naudotojo atliekami duomenų keitimo veiksmai fiksuojami žurnalų įrašuose.

56.8. Neaktyvumo dirbant su IS laikas, kuriam pasibaigus IS naudotojų ryšio sesijos automatiškai nutraukiamos, nustatytas IS naudotojų administravimo taisyklėse. Automatinis IS sesijos nutraukimas, tapatybės kodo blokavimas taikomi ten, kur tai leidžia naudojamos technologijos.

56.9. Kiekvienas atitinkamos IS tvarkytojas atsako už elektroninės informacijos, kuri jam prieinama naudojant IS, tvarkymo teisėtumą ir tvarkomų duomenų saugą.

56.10. Ministerijos IS duomenų teikėjai ir (arba) gavėjai už duomenų tvarkymo teisėtumą ir gautų arba teikiamų duomenų saugą atsako teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą, nustatyta tvarka.

56.11. Pasibaigus IS naudotojo valstybės tarnybos santykiams ar darbo sutarčiai, teisė naudotis IS elektronine informacija turi būti panaikinta. IS naudotojui prieiga prie IS turi būti ribojama ar sustabdoma, kai vyksta IS naudotojo veiklos tyrimas, IS naudotojas turi ilgesnės trukmės atostogas arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos.

56.12. Elektroninei informacijai teikti ir (ar) gauti iš kitų valstybės institucijų naudojamasi Kertinio valstybės telekomunikacijų centro teikiama paslauga – Saugiu valstybiniu duomenų perdavimo tinklu (SVDPT) arba ribojant prieigą pagal IP adresą, jei teikėjas ar gavėjas nėra šio tinklo naudotojas.

56.13. Prieiga prie ministerijos IS programinio išeities kodo suteikiama tik IS priežiūros, plėtros ar palaikymo paslaugas teikiančiam teikėjui, pasirašiusiam finansų ministro nustatytos formos įsipareigojimą saugoti duomenų, įskaitant asmens duomenis, informacijos paslaptį.

56.14. Ministerijos kompiuterinėse darbo vietose turi būti naudojamos tik tarnybinės išorinės duomenų laikmenos (USB, CD / DVD ir kt.) ir kiti tarnybiniai įrenginiai, kurie yra išduoti tarnybinėms funkcijoms atlikti;

56.15. Vykdant mokėjimo nurodymus (išskyrus mokėjimo nurodymus į kitą VIKSVA posistemyje esančią sąskaitą) VIKSVA E. iždo modulyje turi būti naudojamas kvalifikuotas elektroninis parašas.

Papildyta papunkčiu:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

57. Pagrindinės atsarginių IS elektroninės informacijos kopijų darymo ir atkūrimo nuostatos:

57.1. Atsarginės IS elektroninės informacijos kopijos turi būti daromos ir saugomos tokios apimties, kad ministerijos IS veiklos sutrikimo, IS elektroninės informacijos saugos (kibernetinio saugumo) incidento ar elektroninės informacijos vientisumo praradimo atveju IS elektroninės informacijos praradimas atitiktų priimtinumo kriterijus.

57.2. IS atsarginės duomenų bazės kopijos daromos periodiškai automatiniu būdu. Bent kartą per savaitę daroma visos apimties kopija, pasikeitimų kopijos – kiekvieną dieną, žurnalų kopijos (jei daromos) – ne rečiau kaip kas valandą;

57.3. IS duomenų bazių kopijos daromos IS administratorių į nutolusį kopijų serverį.

57.4. IS duomenų bazių kopijos IS infrastruktūros administratorių papildomai įrašomos į magnetines laikmenas (juosteles).

57.5. Atkūrimas iš IS elektroninės informacijos kopijų turi būti išbandomas.

57.6. Atsarginių IS elektroninės informacijos kopijų darymas ir atkūrimo bandymas turi būti fiksuojami.

57.7. Atsarginės kopijos turi būti saugomos kitoje patalpoje, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota. IS elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) ir saugiai laikomos visiškai atjungus (angl. *offline*) nuo kompiuterinių tinklų arba turi būti imtasi kitų priemonių, dėl kurių nebūtų galima neteisėtai atkurti elektroninės informacijos, jei kopija daroma ar saugoma ne ministerijos patalpose.

57.8. Prireikus atkurti atsargines kopijas, teisę tam turi tik IS administratorius ar jį pavaduojantis asmuo. Periodiškai, bet ne rečiau kaip kartą per metus, turi būti atliekami IS elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai.

57.9. Patekimas į patalpas, kuriose saugomos atsarginės IS elektroninės informacijos kopijos, turi būti kontroliuojamas.

57.10. IS infrastruktūros administratorius atsako už IS atsarginių kopijų darymą, tikrinimą, saugojimą ir atkūrimą. Atsarginės kopijos daromos IS saugaus elektroninės informacijos tvarkymo taisyklėse nustatyta tvarka.

58. Organizaciniai ir techniniai elektroninės informacijos saugos reikalavimai detalizuojami IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentuose.

59. Perkant paslaugas, darbus ar įrangą, susijusius su IS, jos projektavimu, kūrimu, diegimu, modernizavimu, priežiūra, palaikymu, saugos užtikrinimu, taip pat kitus, suteikiančius teisę ir galimybę prieiti prie elektroninės informacijos, ją apdoroti, saugoti, keistis elektronine informacija ar tiekti informacinių technologijų infrastruktūros komponentus, darbus, pirkimo dokumentuose iš anksto turi būti nustatyta, kad paslaugų teikėjas, darbų vykdytojas ar techninės ir programinės įrangos tiekėjas (toliau kartu – paslaugų teikėjas) privalo laikytis Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše, Saugos nuostatuose, IS saugaus elektroninės informacijos tvarkymo taisyklėse nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį nustatytiems elektroninės informacijos saugos reikalavimams.

60. Į paslaugų pirkimo sutartį turi būti įtraukta nuostata, įpareigojanti paslaugų teikėjo darbuotojus pasirašyti finansų ministro nustatytos formos įsipareigojimą neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant šią sutartį, išskyrus tiek, kiek būtina sutarčiai vykdyti, taip pat nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams laikantis principo, kad visa paslaugų teikėjui suteikta informacija (įskaitant IS tvarkomą elektroninę informaciją) yra konfidenciali.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

61. IS saugos įgaliotinio, IS administratorių, vietinių IS naudotojų administratorių ir IS infrastruktūros administratorių, IS naudotojų kvalifikacijos reikalavimai:

Punkto pakeitimai:

Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

61.1. IS saugos įgaliotinis privalo išmanyti IS elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais elektroninės informacijos saugą.

61.2. IS saugos įgaliotinis, IS administratorius ir IS infrastruktūros administratorius turi atitikti Valstybės informacinių išteklių valdymo įstatymo 42 straipsnyje nustatytus reikalavimus.

61.3. IS administratoriai pagal kompetenciją privalo išmanyti IS elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti IS ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti duomenų bazes ir priskirtas IS, IS komponentus (stebėti IS komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti nepertraukiamą IS komponentų veikimą ir pan.), IS administratoriai turi būti susipažinę su IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentais bei Lietuvos ir tarptautiniais „Informacinės technologijos. Saugumo metodai“ grupės standartais ir sutikę laikytis IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų reikalavimų.

61.4. IS infrastruktūros administratorius privalo išmanyti IS elektroninės informacijos saugos (kibernetinio saugumo) principus, administruoti ir prižiūrėti IS komponentus (kompiuterius, serverius, operacines sistemas, taikomųjų programų sistemas, užkardas, įsilaužimo aptikimo sistemas, duomenų perdavimo tinklus), taip pat mokėti užtikrinti jų saugumą, turi būti susipažinęs su IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentais bei Lietuvos ir

tarptautiniais „Informacinės technologijos. Saugumo metodai“ grupės standartais ir sutikęs laikytis IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų reikalavimų.

61.5. IS vidiniai naudotojai turi būti susipažinę su teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, Saugos nuostatais, IS naudotojų administravimo taisyklėmis ir IS saugaus elektroninės informacijos tvarkymo taisyklėmis, sutikę laikytis šių teisės aktų, taip pat turi būti susipažinę su kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą (kibernetinį saugumą). Su IS veiklos tęstinumo valdymo planu susipažįsta ministerijos darbuotojai ir IS vidiniai naudotojai, kuriems toks planas yra privalomas.

Papunkčio pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

61.6. IS išoriniai naudotojai ir ministerijos IS plėtros ir palaikymo paslaugų teikėjai turi būti susipažinę su teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, Saugos nuostatais, IS naudotojų administravimo taisyklėmis ir Saugaus elektroninės informacijos tvarkymo taisyklėmis, sutikę laikytis šių teisės aktų reikalavimų.

61.7. IS saugos įgaliotinis, IS infrastruktūros administratorius, IS administratorius, vietinis IS naudotojų administratorius ir IS naudotojai pagal kompetenciją privalo išmanyti pagrindinius informacijos saugos principus, mokėti saugiai tvarkyti elektroninę informaciją, nuolat kelti kvalifikaciją saugaus elektroninės informacijos tvarkymo kursuose, mokymuose, seminaruose.

Papunkčio pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

61.8. IS vidinių naudotojų, administratorių, IS infrastruktūros administratoriaus ir IS saugos įgaliotinio kvalifikacija turi atitikti reikalavimus, nustatytus jų pareiginiuose nuostatuose ar pareigybių aprašymuose.

62. IS administratoriai, vietiniai IS naudotojų administratoriai ir IS infrastruktūros administratoriai, kuriems suteikta prieiga prie IS komponentų, tvarkantys duomenis ir informaciją, įskaitant ir asmens duomenis, privalo saugoti jų paslaptį ir turi būti pasirašę finansų ministro nustatytos formos įsipareigojimą saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir nutraukus su šių duomenų ir informacijos tvarkymu susijusią veiklą.

Punkto pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

63. IS naudotojai, tvarkantys duomenis ir informaciją, įskaitant ir asmens duomenis, privalo saugoti jų paslaptį ir turi būti pasirašę finansų ministro nustatytos formos įsipareigojimą saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir nutraukus su šių duomenų ir informacijos tvarkymu susijusią veiklą.

64. Įvykus elektroninės informacijos saugos incidentui, nenumatytai situacijai, IS saugos įgaliotinio, IS administratoriaus, IS infrastruktūros administratoriaus veiksmus reglamentuoja ITD direktoriaus 2014 m. spalio 14 d. sprendimu patvirtinta „Elektroninės informacijos saugos incidentų valdymo procedūra“.

65. IS vidinių naudotojų ir IS administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo periodiškumo reikalavimai:

65.1. IS vidiniams naudotojams turi būti įvairiais būdais primenama apie IS elektroninės informacijos saugos (kibernetinio saugumo) problemas (pavyzdžiui, priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems IS vidiniams naudotojams, IS administratoriams ir pan.).

65.2. Mokymai IS elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į IS elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), IS saugos įgaliotinio, IS administratorių, IS infrastruktūros administratorių ir IS vidinių naudotojų poreikius.

65.3. Mokymai gali būti vykdomi fiziškai susirenkant (pavyzdžiui, paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu būdu (pavyzdžiui, vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.).

65.4. Mokymai IS vidiniams naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už mokymų organizavimą atsakingas IS saugos įgaliotinis. Mokymai IS saugos įgaliotiniui, IS administratoriams ir IS infrastruktūros administratoriams turi būti organizuojami pagal poreikį.

Punkto pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

66. IS valdytojas užtikrina tinkamą IS saugos įgaliotinio, IS administratorių, IS infrastruktūros administratorių ir IS vidinių naudotojų kvalifikacijos tobulinimą.

V SKYRIUS
SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

67. IS naudotojų, IS administratorių, vietinių IS naudotojų administratorių ir IS infrastruktūros administratorių supažindinimą su Saugos nuostatais, kitais IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentais ir atsakomybe už tokiuose dokumentuose nustatytų reikalavimų nesilaikymą organizuoja IS saugos įgaliotinis.

Punkto pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

68. IS naudotojų, IS administratorių, vietinių IS naudotojų administratorių ir IS infrastruktūros administratorių supažindinimo su IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentais tvarka nustatyta IS naudotojų administravimo taisyklėse.

Punkto pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

69. Pakartotinai su Saugos nuostatais ir IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentais IS naudotojai, IS administratorius, vietinis IS naudotojų administratorius ir IS infrastruktūros administratorius supažindinami tik iš esmės pasikeitus šiems dokumentams.

Punkto pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

70. Tvarkyti IS elektroninę informaciją gali tik IS naudotojai, kurie yra susipažinę su IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentų reikalavimais pagal principą „būtina žinoti“ ir sutikę laikytis šiuose dokumentuose nustatytų reikalavimų. IS naudotojai atsako už IS ir joje tvarkomos elektroninės informacijos saugą pagal savo kompetenciją.

71. IS duomenų teikėjai ar gavėjai Saugos nuostatų, IS naudotojų administravimo taisyklių ir IS saugaus elektroninės informacijos tvarkymo taisyklių kopijas gauna sutarties dėl elektroninės informacijos arba duomenų teikimo pasirašymo metu, jei šie teisės aktai nėra paskelbti IS valdytojo. Kitais atvejais sutartyje pateikiama nuoroda į IS valdytojo interneto svetainę.

72. Saugos nuostatai, IS naudotojų administravimo taisyklės ir IS saugaus elektroninės informacijos tvarkymo taisyklės skelbiami IS valdytojo interneto svetainėje.

73. Supažindinimo su Saugos nuostatais, IS naudotojų administravimo taisyklėmis ir IS saugaus elektroninės informacijos tvarkymo taisyklėmis būdai turi būti pasirenkami atsižvelgiant į IS specifiką (t. y. IS ir jos naudotojų buvimo vietą, organizacinių ar techninių priemonių, leidžiančių identifikuoti su šiais dokumentais susipažinusį asmenį ir užtikrinančių supažindinimo procedūros įrodomumą, panaudojimo galimybes). IS naudotojai, IS administratoriai, vietiniai IS naudotojų administratoriai ir IS infrastruktūros administratoriai su šiais dokumentais turi būti supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą.

Punkto pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

74. IS naudotojai, IS infrastruktūros administratoriai, IS administratoriai, vietiniai IS naudotojų administratoriai, IS saugos įgaliotinis ir ministerijos IS plėtros ir palaikymo paslaugų teikėjai yra atsakingi už IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentuose nustatytų reikalavimų laikymąsi.
Punkto pakeitimai:
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

75. IS valdytojas IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentus gali keisti savo arba IS saugos įgaliotinio iniciatyva. Keičiami saugos dokumentai turi būti derinami su NKSC. Keičiamų dokumentų projektai gali būti nederinami su NKSC tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar IS elektroninės informacijos saugos (kibernetinio saugumo) politikos nekeičiantys pakeitimai arba taisoma teisės technika. Tokiais atvejais NKSC turi būti pateiktos šių dokumentų kopijos.

76. IS saugos ir kibernetinio saugumo politikos įgyvendinimo dokumentai iš esmės turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Šie dokumentai taip pat turi būti persvarstomi (peržiūrimi) atlikus IS rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Persvarsčius (peržiūrėjus) dokumentus, turi būti nustatoma, kuriuos iš juose nustatytų reikalavimų būtina atnaujinti ir (ar) įgyvendinti pirmiausia, siekiant užtikrinti IS saugą (kibernetinį saugumą).

Priedo pakeitimai:
Nr. 1K-265, 2015-08-13, paskelbta TAR 2016-02-04, i. k. 2016-02273

Pakeitimai:

1.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-232, 2011-06-30, Žin., 2011, Nr. 81-3995 (2011-07-05), i. k. 1112050ISAK001K-232
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 "Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo" pakeitimo

2.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-093, 2012-03-09, Žin., 2012, Nr. 32-1502 (2012-03-15), i. k. 1122050ISAK001K-093
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 "Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo" pakeitimo

3.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-362, 2012-10-29, Žin., 2012, Nr. 128-6438 (2012-11-06), i. k. 1122050ISAK001K-362
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 "Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo" pakeitimo

4.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-265, 2015-08-13, paskelbta TAR 2016-02-04, i. k. 2016-02273
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 „Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“ pakeitimo

5.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-122, 2016-04-08, paskelbta TAR 2016-04-12, i. k. 2016-08670
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 „Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“ pakeitimo

6.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-385, 2020-11-24, paskelbta TAR 2020-11-25, i. k. 2020-24947
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 „Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“ pakeitimo

7.
Lietuvos Respublikos finansų ministerija, Įsakymas
Nr. 1K-283, 2022-08-03, paskelbta TAR 2022-08-04, i. k. 2022-16605
Dėl finansų ministro 2007 m. spalio 3 d. įsakymo Nr. 1K-289 „Dėl Finansų ministerijos informacinių sistemų duomenų saugos nuostatų patvirtinimo“ pakeitimo