Suvestinė redakcija nuo 2020-02-25 iki 2020-08-14

Įsakymas paskelbtas: TAR 2017-12-07, i. k. 2017-19722

VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS VALDOMŲ INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2017 m. gruodžio 6 d. Nr. 1K-234
Vilnius

Vadovaudamasi Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimo 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, 11 ir 19 punktų nuostatomis:

1. T v i r t i n u Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų duomenų saugos nuostatus (pridedama).

2. P r i p a ž į s t u netekusiais galios:

2.1. Eilių ir atsargų valdymo informacinės sistemos duomenų saugos nuostatus, patvirtintus Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos (toliau – VLK) direktoriaus 2015 m. spalio 23 d. įsakymu Nr. 1K-301 „Dėl Eilių ir atsargų valdymo informacinės sistemos nuostatų ir šios informacinės sistemos duomenų saugos nuostatų patvirtinimo“;

2.2. Europos Sąjungos socialinės apsaugos duomenų mainų informacinės sistemos duomenų saugos nuostatus, patvirtintus VLK direktoriaus 2016 m. birželio 16 d. įsakymu Nr. 1K-186 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos direktoriaus 2012 m. gruodžio 20 d. įsakymo Nr. 1K-338 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos Europos Sąjungos socialinės apsaugos duomenų mainų informacinės sistemos nuostatų ir šios sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo“;

2.3. Finansų valdymo ir apskaitos informacinės sistemos saugos nuostatus, patvirtintus VLK direktoriaus 2016 m. balandžio 6 d. įsakymu Nr. 1K-110 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos direktoriaus 2010 m. liepos 21 d. įsakymo Nr. 1K-143 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos finansų valdymo ir apskaitos informacinės sistemos nuostatų ir šios sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo“;

2.4. Konsultavimo informacinės sistemos duomenų saugos nuostatus, patvirtintus VLK direktoriaus 2013 m. spalio 15 d. įsakymu Nr. 1K-228 „Dėl Konsultavimo informacinės sistemos duomenų saugos nuostatų patvirtinimo“;

2.5. Projektų valdymo informacinės sistemos duomenų saugos nuostatus, patvirtintus VLK direktoriaus 2016 m. balandžio 14 d. įsakymu Nr. 1K-122 „Dėl Valstybinės ligonių kasos prie

Sveikatos apsaugos ministerijos direktoriaus 2013 m. gegužės 15 d. įsakymo Nr. 1K-98 „Dėl Projektų valdymo informacinės sistemos nuostatų ir duomenų saugos nuostatų patvirtinimo“ pakeitimo“;

2.6. Žalos atlyginimo informacinės sistemos duomenų saugos nuostatus, patvirtintus VLK direktoriaus 2015 m. liepos 15 d. įsakymu Nr. 1K-192 „Dėl Žalos atlyginimo informacinės sistemos nuostatų ir Žalos atlyginimo informacinės sistemos duomenų saugos nuostatų patvirtinimo“.

3. P a v e d u:

3.1. VLK informacijos saugos įgaliotiniui per 6 mėnesius nuo VLK valdomų informacinių sistemų duomenų saugos nuostatų patvirtinimo dienos parengti VLK valdomų informacinių sistemų veiklos tęstinumo valdymo plano, naudotojų administravimo taisyklių ir saugaus informacijos tvarkymo taisyklių projektus;

3.2. šio įsakymo vykdymą kontroliuoti VLK Informacinių technologijų departamento direktoriui.

Direktorė Jūratė Sabalienė

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2017-09-20 raštu Nr. 1D-4970

PATVIRTINTA
Valstybinės ligonių kasos prie
Sveikatos apsaugos ministerijos
direktoriaus 2017 m. gruodžio 6 d.
įsakymu Nr. 1K-234

VALSTYBINĖS LIGONIŲ KASOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS VALDOMŲ INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato reikalavimus, užtikrinančius saugų elektroninės informacijos tvarkymą Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos (toliau – VLK) valdomose informacinėse sistemose, nurodytose 2 punkte (toliau – informacinės sistemos).

2. Saugos nuostatų reikalavimai taikomi tvarkant:

2.1. Buhalterinės ir darbo užmokesčio apskaitos informacinę sistemą (STEKAS);

2.2. Dokumentų valdymo informacinę sistemą (DVS);

2.3. Eilių ir atsargų valdymo informacinę sistemą (EVIS);

2.4. Europos Sąjungos socialinės apsaugos duomenų mainų informacinę sistemą (EDMIS);

2.5. Finansų valdymo ir apskaitos informacinę sistemą (FVAIS);

2.6. Informacinių technologijų ir informacinių sistemų pagalbos tarnybos informacinę sistemą (NAT IS);

2.7. Kokybės valdymo informacinę sistemą (QPR);

2.8. Konsultavimo informacinę sistemą (KIS);

2.9. Projektų valdymo informacinę sistemą (PVIS);

2.10. Žalų atlyginimo informacinę sistemą (ŽAIS).

3. 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, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių apraše, patvirtintuose Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 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.

4. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

4.2. organizacinių, administracinių, techninių ir programinių elektroninės informacijos saugos priemonių įgyvendinimas ir kontrolė;

4.3. informacinių sistemų veiklos tęstinumo užtikrinimas;

4.4. asmens duomenų apsauga.

5. Elektroninės informacijos saugumo užtikrinimo tikslai:

5.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti ir saugoti elektroninę informaciją;

5.2. užtikrinti, kad elektroninė informacija būtų teisinga ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

6. Informacinių sistemų valdytoja yra VLK, buveinės adresas: Europos aikštė 1, LT 03505 Vilnius.

7. Informacinių sistemų tvarkytojai yra VLK ir teritorinės ligonių kasos (toliau – TLK):

7.1. Vilniaus TLK, buveinės adresas: Ž. Liauksmino g. 6, LT 01101 Vilnius;

7.2. Kauno TLK, buveinės adresas: Aukštaičių g. 10, LT 44147 Kaunas;

7.3. Klaipėdos TLK, buveinės adresas: Pievų Tako g. 38, LT 92236 Klaipėda;

7.4. Šiaulių TLK, buveinės adresas: Vilniaus g. 273, LT 76332 Šiauliai;

7.5. Panevėžio TLK, buveinės adresas: Respublikos g. 66, LT 35158 Panevėžys.

8. Informacinių sistemų valdytojas pagal kompetenciją atsako už informacinių sistemų saugos politikos formavimą, jos įgyvendinimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

9. VLK, kaip informacinių sistemų valdytoja, vykdo šias funkcijas:

9.1. rengia ir tvirtina teisės aktus, susijusius su informacinėse sistemose kaupiamų elektroninių duomenų tvarkymu ir jų sauga;

9.2. skiria informacinių sistemų saugos įgaliotinį ir administratorius;

9.3. kontroliuoja, kaip laikomasi informacinių sistemų saugos politiką įgyvendinančių dokumentų ir kitų teisės aktų, reglamentuojančių šių sistemų duomenų tvarkymo teisėtumą ir saugos valdymą;

9.4. priima sprendimus dėl informacinių sistemų techninių ir programinių priemonių, būtinų šių sistemų duomenų saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

9.5. prižiūri, kaip laikomasi informacinėse sistemose kaupiamų duomenų ir elektroninės informacijos saugos reikalavimų;

9.6. koordinuoja informacinių sistemų tvarkytojų funkcijų vykdymą ir metodiškai vadovauja šių sistemų tvarkytojų veiklai, užtikrindama informacinių sistemų veikimą, tobulinimą ir elektroninės informacijos saugą;

9.7. nagrinėja informacinių sistemų tvarkytojų pasiūlymus dėl šių sistemų veiklos ir elektroninės informacijos saugos užtikrinimo, juos apibendrina ir priima sprendimus dėl informacinių sistemų tobulinimo;

9.8. priima sprendimą atlikti informacinėse sistemose naudojamų informacinių technologijų saugos reikalavimų atitikties vertinimą;

9.9. vykdo kitas Saugos nuostatuose ir kituose elektroninės informacijos saugą reglamentuojančiuose teisės aktuose priskirtas funkcijas.

10. Informacinių sistemų tvarkytojai atsako už reikiamų administracinių, techninių ir organizacinių informacinių sistemų saugos priemonių įgyvendinimą ir Saugos nuostatų bei informacinių sistemų saugos politiką įgyvendinančių dokumentų nuostatų laikymąsi.

11. VLK, kaip informacinių sistemų tvarkytoja, vykdo šias funkcijas:

11.1. užtikrina informacinių sistemų prieinamumą;

11.2. užtikrina informacinių sistemų funkcionavimui būtinos informacinių technologijų infrastruktūros saugą;

11.3. daro duomenų, kaupiamų informacinėse sistemose, atsargines kopijas;

11.4. atlieka kitas informacinių sistemų saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose šių sistemų duomenų tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas.

12. TLK, kaip informacinių sistemų tvarkytojos, vykdo šias funkcijas:

12.1. užtikrina tinkamą informacinių sistemų valdytojo priimtų teisės aktų ir rekomendacijų įgyvendinimą;

12.2. užtikrina, kad informacinės sistemos būtų tvarkomos vadovaujantis šių sistemų nuostatais, Saugos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais;

12.3. teikia pasiūlymus informacinių sistemų valdytojui dėl šių sistemų veiklos ir elektroninės informacijos saugos užtikrinimo;

12.4. atlieka kitas informacinių sistemų saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose šių sistemų duomenų tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas.

13. Informacinių sistemų saugos įgaliotinis, koordinuodamas ir prižiūrėdamas saugos politikos įgyvendinimą, atlieka šias funkcijas:

13.1. rengia informacinių sistemų saugos politiką įgyvendinančių dokumentų projektus;

13.2. teikia VLK direktoriui pasiūlymus dėl:

13.2.1. informacinių sistemų administratorių skyrimo ir reikalavimų jiems nustatymo;

13.2.2. informacinių sistemų saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

13.2.3. informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

13.3. koordinuoja elektroninės informacijos saugos incidentų, įvykusių informacinėse sistemose, tyrimą ir bendradarbiauja 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;

13.4. teikia informacinių sistemų administratoriams ir šių sistemų naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su informacinių sistemų saugos politikos įgyvendinimu;

13.5. organizuoja rizikos vertinimą;

13.6. atsako už informacinių sistemų saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

13.7. vykdo kitas informacinių sistemų saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose šių sistemų duomenų tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas.

14. Informacinių sistemų administratoriai skiriami VLK direktoriaus įsakymu kiekvienai informacinei sistemai atskirai.

15. Informacinės sistemos administratorius atsako už atitinkamos informacinės sistemos funkcionavimą ir atlieka šias funkcijas:

15.1. užtikrina informacinės sistemos techninės ir programinės įrangos funkcionavimą, prižiūri programinę įrangą, reikalingą šios sistemos naudotojų funkcijoms vykdyti;

15.2. administruoja ir tvarko informacinės sistemos duomenų bazę, užtikrina duomenų bazėje naudojamų klasifikatorių atnaujinimą;

15.3. registruoja informacinės sistemos naudotojus, suteikia jiems prisijungimo vardus ir nustato prieigos teises naudotis reikiama elektronine informacija;

15.4. pagal kompetenciją nustato informacinės sistemos komponentų (kompiuterių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių ir kt.) pažeidžiamas vietas;

15.5. pagal kompetenciją dalyvauja vykdant saugumo reikalavimų įgyvendinimo stebėseną;

15.6. pagal kompetenciją rengia pasiūlymus dėl informacinės sistemos palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo, teikia juos informacinės sistemos duomenų valdymo įgaliotiniui ir (ar) informacinių sistemų saugos įgaliotiniui;

15.7. informuoja informacinių sistemų saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia siūlymus dėl šių incidentų pašalinimo;

15.8. vykdo informacinių sistemų saugos įgaliotinio, informacinės sistemos duomenų

valdymo įgaliotinio nurodymus ar pavedimus, susijusius su informacinės sistemos saugos užtikrinimu;

15.9. atlieka kitas VLK direktoriaus arba informacinių sistemų saugos įgaliotinio pavestas, saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose informacinių sistemų duomenų tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas.

16. Informacinių sistemų duomenys tvarkomi ir jų sauga užtikrinama vadovaujantis:

16.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

16.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

16.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

16.4. Lietuvos Respublikos kibernetinio saugumo įstatymu;

16.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

16.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

16.7. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais 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“;

16.8. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

16.9. Lietuvos standartais – LST ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ ir LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“;

16.10. VLK ir teritorinių ligonių kasų organizacinių ir techninių kibernetinio saugumo reikalavimų aprašu, patvirtintu VLK direktoriaus 2017 m. kovo 9 d. įsakymu Nr. 1K-52 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos ir teritorinių ligonių kasų organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo patvirtinimo“;

16.11. kitais teisės aktais, reglamentuojančiais informacinių sistemų valdytojo ir tvarkytojų veiklą, elektroninės informacijos tvarkymo teisėtumą ir saugos valdymą.

Punkto pakeitimai:
Nr. 1K-55, 2020-02-20, paskelbta TAR 2020-02-24, i. k. 2020-03949

17. Saugos nuostatais privalo vadovautis informacinių sistemų valdytojas, tvarkytojai, saugos įgaliotinis, visi šių sistemų naudotojai ir administratoriai.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

18. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo (toliau – Aprašas) 8.1, 8.3 ir 8.6 papunkčiuose nurodytais informacijos svarbos kriterijais, informacija priskirtina svarbios informacijos kategorijai, kai ji tvarkoma:

18.1. Eilių ir atsargų valdymo informacinėje sistemoje;

18.2. Europos Sąjungos socialinės apsaugos duomenų mainų informacinėje sistemoje;

18.3. Finansų valdymo ir apskaitos informacinėje sistemoje.

19. Vadovaujantis Aprašo 9.1 ir 9.3 papunkčiuose nurodytais informacijos svarbos kriterijais, informacija priskirtina vidutinės svarbos informacijos kategorijai, kai ji tvarkoma:

19.1. Dokumentų valdymo informacinėje sistemoje;

19.2. Konsultavimo informacinėje sistemoje;

19.3. Žalų atlyginimo informacinėje sistemoje.

Punkto pakeitimai:
Nr. 1K-55, 2020-02-20, paskelbta TAR 2020-02-24, i. k. 2020-03949

20. Vadovaujantis Aprašo 10 punktu, informacija priskirtina mažiausios svarbos informacijos kategorijai, kai ji tvarkoma:

20.1. Buhalterinės ir darbo užmokesčio apskaitos informacinėje sistemoje;

20.2. Informacinių technologijų ir informacinių sistemų pagalbos tarnybos informacinėje sistemoje;

20.3. Kokybės valdymo informacinėje sistemoje;

20.4. Projektų valdymo informacinėje sistemoje.

21. Informacinės sistemos klasifikuojamos pagal kategorijas, atsižvelgiant į jose apdorojamos elektroninės informacijos svarbą:

21.1. pagal Aprašo 12.2 papunktį antrai kategorijai priskiriamos:

21.1.1. Eilių ir atsargų valdymo informacinė sistema;

21.1.2. Europos Sąjungos socialinės apsaugos duomenų mainų informacinė sistema;

21.1.3. Finansų valdymo ir apskaitos informacinė sistema;

21.2. pagal Aprašo 12.3 papunktį trečiai kategorijai priskiriamos:

21.2.1. Dokumentų valdymo informacinė sistema;

21.2.2. Konsultavimo informacinė sistema;

21.2.3. Žalų atlyginimo informacinė sistema;

21.3. pagal Aprašo 12.4 papunktį ketvirtai kategorijai priskiriamos:

21.3.1. Buhalterinės ir darbo užmokesčio apskaitos informacinė sistema;

21.3.2. Informacinių technologijų ir informacinių sistemų pagalbos tarnybos informacinė sistema;

21.3.3. Kokybės valdymo informacinė sistema;

21.3.4. Projektų valdymo informacinė sistema.

22. Atsižvelgiant į saugotinų asmens duomenų pobūdį bei jų tvarkymo keliamą riziką ir vadovaujantis Bendrųjų reikalavimų 11 punkto nuostatomis, informacinėms sistemoms nustatomi šie automatiniu būdu tvarkomų asmens duomenų saugumo lygiai:

22.1. pirmasis saugumo lygis nustatomas:

22.1.1. Buhalterinės ir darbo užmokesčio apskaitos informacinei sistemai;

22.1.2. Dokumentų valdymo informacinei sistemai;

22.1.3. Informacinių technologijų ir informacinių sistemų pagalbos tarnybos informacinei sistemai;

22.1.4. Kokybės valdymo informacinei sistemai;

22.1.5. Konsultavimo informacinei sistemai;

22.1.6. Projektų valdymo informacinei sistemai;

22.1.7. Žalų atlyginimo informacinei sistemai;

22.2. antrasis saugumo lygis nustatomas:

22.2.1. Europos Sąjungos socialinės apsaugos duomenų mainų informacinei sistemai;

22.2.2. Finansų valdymo ir apskaitos informacinei sistemai;

22.3. trečiasis saugumo lygis nustatomas Eilių ir atsargų valdymo informacinei sistemai.

23. Informacinių sistemų saugos įgaliotinis ne rečiau kaip kartą per metus organizuoja informacinių sistemų rizikos vertinimą, kuris atliekamas vadovaujantis Lietuvos Respublikos vidaus reikalų ministerijos išleistu metodiniu leidiniu „Rizikos analizės vadovas“, Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos (toliau –ARSIS) metodika bei reikalavimais ir Lietuvos bei tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais. Prireikus informacinių sistemų saugos įgaliotinis gali organizuoti neeilinį rizikos vertinimą.

Punkto pakeitimai:
Nr. 1K-55, 2020-02-20, paskelbta TAR 2020-02-24, i. k. 2020-03949

24. Informacinių sistemų rizikos vertinimas pateikiamas rizikos įvertinimo ataskaitoje. Ši ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai, ir yra pateikiama informacinių sistemų valdytojo vadovui.

25. Svarbiausi rizikos veiksniai yra šie:

25.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų suvedimas ir teikimas, fiziniai informacinių technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kt.);

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

25.3. 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.

26. Atsižvelgdamas į rizikos įvertinimo ataskaitą, informacinių sistemų valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

27. Informacinių sistemų valdytojas ne rečiau kaip vieną kartą per metus organizuoja informacinių technologijų saugos atitikties vertinimą, kurio metu:

27.1. inventorizuojama informacinių sistemų techninė ir programinė įranga;

27.2. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų informacinių sistemų naudotojų kompiuterinių darbo vietų, visose tarnybinėse stotyse įdiegtos programos ir jų sąranka;

27.3. patikrinama ir įvertinama, ar informacinių sistemų naudotojams suteiktos teisės atitinka jų vykdomas funkcijas;

27.4. įvertinamas pasirengimas užtikrinti informacinės sistemos veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui;

27.5. įvertinama informacinės sistemos rizikos įvertinimo ir valdymo būklė.

28. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama informacinių sistemų valdytojo vadovui.

29. Atsižvelgdamas į informacinių technologijų saugos atitikties vertinimo ataskaitą, informacinių sistemų saugos įgaliotinis prireikus parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakinguosius vykdytojus paskiria ir įgyvendinimo terminus nustato informacinių sistemų valdytojo vadovas.

30. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano, saugos atitikties vertinimo ataskaitos ir pastebėtų trūkumų šalinimo plano kopijas informacinių sistemų valdytojas ne vėliau kaip per 5 (penkias) darbo dienas nuo šių dokumentų priėmimo dienos

įkelia į ARSIS, vadovaudamasis šios sistemos nuostatais, patvirtintais 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“.

Punkto pakeitimai:
Nr. 1K-55, 2020-02-20, paskelbta TAR 2020-02-24, i. k. 2020-03949

31. Techninės, programinės ir organizacinės informacinių sistemų elektroninės informacijos saugos priemonės pasirenkamos atsižvelgiant į informacinių sistemų valdytojo turimus išteklius ir vadovaujantis šiais principais:

31.1. saugos sistema turi būti valdoma centralizuotai;

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

31.3. pagal galimybes turi būti įdiegtos prevencinės informacijos saugos priemonės.

32. Informacinių sistemų saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas informacinių sistemų valdytojas ne vėliau kaip per 5 (penkias) darbo dienas nuo jų patvirtinimo dienos įkelia į ARSIS, vadovaudamasis šios sistemos nuostatais, patvirtintais 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“.

Punkto pakeitimai:
Nr. 1K-55, 2020-02-20, paskelbta TAR 2020-02-24, i. k. 2020-03949

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

33. Programinės įrangos, skirtos apsaugoti informacines sistemas nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir panašiai) ir užtikrinančios saugų informacinių sistemų veikimą, naudojimo nuostatos:

33.1. tarnybinėse stotyse ir kompiuterinėse darbo vietose privalo būti įdiegta centralizuotai valdoma programinė įranga, apsauganti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos ir kt.);

33.2. elektroninio pašto tarnybinės stotys turi būti apsaugotos nuo nepageidaujamo turinio elektroninių laiškų;

33.3. informacinių sistemų apsaugai naudojama programinė įranga privalo būti atnaujinama ne rečiau kaip kas trys dienos;

33.4. informacinių sistemų apsaugai naudojamos programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

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

34.1. naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga;

34.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

34.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka tik šias funkcijas vykdantis administratorius.

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

35.1. kompiuterių tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, turi būti įdiegta įranga, skirta atakų prevencijai, taip pat įsilaužimų aptikimo įranga;

35.2. visas duomenų srautas į internetą ir iš jo yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos.

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

36.1. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą naudojami saugūs

ryšio kanalai. Informacijai perduoti gali būti naudojamas Saugus valstybinis duomenų perdavimo tinklas;

36.2. prieigos prie informacinių sistemų elektroninės informacijos teises gali suteikti tik atitinkamos informacinės sistemos administratorius;

36.3. informacinių sistemų naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

36.4. prieiga prie informacinių sistemų elektroninės informacijos leidžiama tik per registravimo slaptažodžių sistemą. Prieigos prie informacinių sistemų elektroninės informacijos valdymas yra reglamentuotas informacinių sistemų naudotojų administravimo taisyklėse.

37. Nešiojamieji ir stacionarūs kompiuteriai, kuriuose saugomi informacinių sistemų duomenys, turi būti apsaugoti prisijungimo vardu ir slaptažodžiu.

38. Už nešiojamojo kompiuterio ir jame tvarkomų ar saugomų duomenų saugą Lietuvos Respublikos teisės aktų nustatyta tvarka atsako darbuotojas, kuriam šis kompiuteris yra skirtas.

39. Iš nešiojamųjų ir stacionarių kompiuterių, kurie perduodami remontuoti ar techniniam aptarnavimui atlikti, turi būti pašalinti informacinėse sistemose saugomi asmens duomenys.

40. Nešiojamieji informacinių sistemų naudotojų kompiuteriai ne informacinių sistemų tvarkytojo patalpose turi būti naudojami tik tiesioginėms jų funkcijoms vykdyti.

41. Nešiojamuosiuose naudotojų kompiuteriuose turi būti įdiegtos papildomos saugos priemonės, skirtos informacinių sistemų elektroniniams duomenims perduoti saugiu šifruotu duomenų perdavimo protokolu.

42. Atsarginės duomenų, kaupiamų informacinėse sistemose, kopijos daromos Elektroniniu būdu tvarkomų duomenų atsarginių kopijų valdymo tvarkos aprašo, patvirtinto VLK direktoriaus 2016 m. kovo 1 d. įsakymu Nr. 1K-68 „Dėl 2012 m. sausio 24 d. įsakymo Nr. 1K-14 „Dėl Elektroninių duomenų kopijų darymo tvarkos aprašo patvirtinimo“ pakeitimo“, nustatyta tvarka.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

43. Informacinių sistemų saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą, susijusį su elektroninių duomenų ir informacinių sistemų saugumu, 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 paskyrimo praėję mažiau kaip vieneri metai.

44. Informacinių sistemų saugos įgaliotinis turi:

44.1. išmanyti elektroninės informacijos saugos užtikrinimo principus;

44.2. sugebėti vertinti rizikos veiksnius ir galimą žalą, organizuoti ir kontroliuoti pastebėtų trūkumų šalinimą;

44.3. savo darbe vadovautis informacinių sistemų saugos politiką įgyvendinančiais dokumentais, standartais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

45. Informacinės sistemos administratorius turi:

45.1. išmanyti elektroninės informacijos saugos principus, darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugą;

45.2. stebėti techninės ir programinės įrangos veikimą, atlikti šios įrangos profilaktinę priežiūrą, sutrikimų diagnostiką ir šalinimą;

45.3. mokėti administruoti ir prižiūrėti duomenų bazę;

45.4. būti susipažinęs su informacinės sistemos nuostatais ir kitais saugos politiką įgyvendinančiais dokumentais.

46. Informacinių sistemų naudotojai turi:

46.1. turėti pagrindinius darbo su kompiuteriu įgūdžius, mokėti tvarkyti duomenis;

46.2. pasirašyti pasižadėjimą saugoti asmens duomenų paslaptį ir susipažinti su Saugos nuostatais bei kitais informacinių sistemų saugos politiką įgyvendinančiais dokumentais.

47. Informacinių sistemų naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti informacinių sistemų saugos įgaliotiniui.

48. Informacinių sistemų saugos įgaliotinis informacinių sistemų administratoriams ir naudotojams periodiškai, bet ne rečiau kaip kartą per dvejus metus, organizuoja mokymus elektroninės informacijos saugos klausimais, įvairiais būdais primena apie saugumo problemas (pvz., siunčia pranešimus elektroniniu paštu, instruktuoja naujus darbuotojus ir pan.).

V SKYRIUS
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

49. Informacinių sistemų naudotojus su Saugos nuostatais, informacinių sistemų saugos politiką įgyvendinančiais dokumentais ir atsakomybe už jų reikalavimų nesilaikymą pasirašytinai supažindina informacinių sistemų saugos įgaliotinis.

50. Informacinių sistemų saugos įgaliotinis, informacinių sistemų administratoriai ir naudotojai raštu įsipareigoja laikytis Saugos nuostatų ir kitų informacinių sistemų saugos politiką įgyvendinančių dokumentų reikalavimų.

51. Pakartotinai su Saugos nuostatais ir informacinių sistemų saugos politiką įgyvendinančiais dokumentais, šiems pasikeitus, informacinių sistemų naudotojai supažindinami elektroninėmis priemonėmis.

Punkto pakeitimai:
Nr. 1K-55, 2020-02-20, paskelbta TAR 2020-02-24, i. k. 2020-03949

52. Informacinių sistemų naudotojų supažindinimo su saugos dokumentais tvarka yra reglamentuota informacinių sistemų naudotojų administravimo taisyklėse.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

53. Saugos nuostatai, kiti informacijos saugos valdymo sistemos dokumentai, reglamentuojantys informacinių sistemų saugą, peržiūrimi ir prireikus keičiami ne rečiau kaip kartą per metus.

Pakeitimai:

1.
Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos, Įsakymas
Nr. 1K-55, 2020-02-20, paskelbta TAR 2020-02-24, i. k. 2020-03949
Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos direktoriaus 2017 m. gruodžio 6 d. įsakymo Nr. 1K-234 „Dėl Valstybinės ligonių kasos prie Sveikatos apsaugos ministerijos valdomų informacinių sistemų duomenų saugos nuostatų patvirtinimo“