Suvestinė redakcija nuo 2023-08-31 iki 2023-10-30

Įsakymas paskelbtas: TAR 2014-07-14, i. k. 2014-10212

LIETUVOS RESPUBLIKOS SVEIKATOS APSAUGOS MINISTRAS

ĮSAKYMAS DĖL TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS NUOSTATŲ IR DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2014 m. liepos 9 d. Nr. V-776
Vilnius

Įgyvendindamas Lietuvos Respublikos sveikatos apsaugos ministro 2014 m. vasario 3 d. įsakymo Nr. V-153 „Dėl Traumų ir nelaimingų atsitikimų stebėsenos tvarkos aprašo patvirtinimo“ 2.1 ir 2.2 papunkčius ir vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 30 straipsnio 1 ir 2 dalimis, Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, 4 ir 11 punktais, 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 punktu, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 5.3 papunkčiu:

Preambulės pakeitimai:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404
Nr. V-946, 2023-08-30, paskelbta TAR 2023-08-30, i. k. 2023-17075

1. T v i r t i n u pridedamus:

1.1. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos nuostatus;

1.2. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos duomenų saugos nuostatus.

2. P a v e d u Higienos institutui:

2.1. paskirti Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos saugos įgaliotinį, administratorių, duomenų valdymo įgaliotinį;

2.2. per 5 mėnesius nuo šio įsakymo įsigaliojimo parengti, teisės aktų nustatyta tvarka suderinti ir Lietuvos Respublikos sveikatos apsaugos ministerijai pateikti tvirtinti:

2.2.1. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių projektą;

2.2.2. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos veiklos tęstinumo valdymo plano projektą;

2.2.3. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos naudotojų administravimo taisyklių projektą.

3. Įsakymo vykdymą p a v e d u kontroliuoti ministerijos kancleriui.

Sveikatos apsaugos ministras Vytenis Povilas Andriukaitis

SUDERINTA
Lietuvos Respublikos vidaus reikalų ministerijos
2014 m. birželio 5 d. raštu Nr. 1D-4249 (52)

SUDERINTA
Valstybinės duomenų apsaugos inspekcijos
2014 m. birželio 6 d. raštu Nr. 2R-2943 (3.33.)

SUDERINTA
Informacinės visuomenės plėtros komiteto prie
Susisiekimo ministerijos
2014 m. birželio 5 d. raštu Nr. S-807

SUDERINTA
Valstybinės ligonių kasos prie
Sveikatos apsaugos ministerijos
2014 m. birželio 9 d. raštu Nr. 4K-4767

SUDERINTA
Neįgalumo ir darbingumo nustatymo tarnybos
prie Socialinės apsaugos ir darbo ministerijos
2014 m. birželio 5 d. raštu Nr. R-21687

SUDERINTA
Valstybinio socialinio draudimo fondo valdybos
prie Socialinės apsaugos ir darbo ministerijos
2014 m. birželio 9 d. raštu Nr. (11.2) I-5180

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos
ministro 2014 m. liepos 9 d.
įsakymu Nr. V-776
(Lietuvos Respublikos sveikatos apsaugos
ministro 2023 m. rugpjūčio 30 d.
įsakymo Nr. V-946
redakcija)

TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos nuostatai (toliau – Nuostatai) nustato Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos (toliau – Informacinė sistema) steigimo teisinį pagrindą, tikslus, uždavinius ir funkcijas, organizacinę, informacinę ir funkcinę struktūras, Informacinės sistemos duomenų teikimo ir naudojimo tvarką, Informacinės sistemos duomenų saugą, finansavimą, Informacinės sistemos modernizavimą ir likvidavimą.

2. Informacinės sistemos steigimo teisinis pagrindas – Lietuvos Respublikos visuomenės sveikatos priežiūros įstatymo 26 straipsnio 4 dalis.

3. Informacinės sistemos tikslas – informacinių technologijų priemonėmis valdyti duomenis apie traumas ir nelaimingus atsitikimus.

4. Informacinės sistemos uždavinys – centralizuotai tvarkyti duomenis apie traumas ir nelaimingus atsitikimus ir atlikti traumų ir nelaimingų atsitikimų priežasčių analizę.

5. Informacinės sistemos pagrindinės funkcijos:

5.1. rinkti, kaupti ir apdoroti duomenis apie traumas ir nelaimingus atsitikimus;

5.2. rengti statistinę informaciją;

5.3. vykdyti surinktų duomenų apie traumas ir nelaimingus atsitikimus analizę;

5.4. teikti duomenis Informacinės sistemos naudotojams (sprendimų priėmėjams, sveikatos specialistams, mokslininkams, visuomenei) traumų ir nelaimingų atsitikimų valdymo ir prevencijos, statistinės analizės, mokslo tyrimų ir visuomenės informavimo tikslais.

6. Informacinės sistemos asmens duomenų tvarkymo tikslai:

6.1. siekiant užtikrinti oficialiosios statistikos programos vykdymą ir visuomenės interesą, integruoti registrų ir informacinių sistemų kaupiamus duomenis, susijusius su traumomis ir nelaimingais atsitikimais, ir naudoti statistikos tikslams;

6.2. tvarkyti statistinius duomenis apie traumas ir nelaimingus atsitikimus, įskaitant duomenų tvarkymą traumų ir nelaimingų atsitikimų valdymo ir prevencijos, statistinės analizės, mokslo tyrimų ir visuomenės informavimo tikslams įgyvendinti, rengti statistinę informaciją;

6.3. analizuoti duomenis apie traumas ir nelaimingus atsitikimus;

6.4. administruoti Informacinės sistemos naudotojų ir prieigos teises.

7. Informacinė sistema tvarkoma vadovaujantis 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) (toliau – Reglamentas (ES) 2016/679), Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu, Lietuvos Respublikos oficialiosios statistikos ir valstybės duomenų valdysenos įstatymu, Lietuvos Respublikos visuomenės sveikatos stebėsenos (monitoringo) įstatymu, Lietuvos Respublikos kibernetinio saugumo įstatymu, Lietuvos Respublikos teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatymu, Informacinės

visuomenės plėtros komiteto direktoriaus 2013 m. kovo 25 d. įsakymu Nr. T-36 „Dėl Duomenų teikimo formatų ir standartų rekomendacijų patvirtinimo“, Nuostatais ir kitais teisės aktais, reglamentuojančiais informacinių sistemų veiklą.

8. Nuostatuose vartojamos sąvokos atitinka Nuostatų 7 punkte nurodytuose teisės aktuose vartojamas sąvokas.

II SKYRIUS
INFORMACINĖS SISTEMOS ORGANIZACINĖ STRUKTŪRA

9. Informacinės sistemos valdytojas, tvarkytojas ir asmens duomenų valdytojas yra Higienos institutas (toliau – Informacinės sistemos valdytojas ir tvarkytojas).

10. Informacinės sistemos valdytojas ir tvarkytojas turi Reglamente (ES) 2016/679 nustatytas teises ir pareigas, atlieka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme nustatytas funkcijas, taip pat:

10.1. pagal kompetenciją priima sprendimus, susijusius su Informacinės sistemos kūrimu, plėtra, likvidavimu, modernizavimu, priežiūra, administravimu ir juos vykdo;

10.2. užtikrina Informacinės sistemos funkcionavimą;

10.3. tvarko Informacinės sistemos duomenis ir teikia juos duomenų gavėjams;

10.4. sudaro duomenų teikimo sutartis su duomenų gavėjais;

10.5. teikia pasiūlymus Lietuvos Respublikos sveikatos apsaugos ministerijai dėl Informacinės sistemos eksploatavimui, priežiūrai ir plėtrai skirtų funkcinių, techninių, programinių priemonių finansavimo, įsigijimo, įdiegimo ir modernizavimo, organizuoja jų įdiegimą ir modernizavimą;

10.6. užtikrina reikiamas administracines, technines ir organizacines Informacinės sistemos tvarkomų duomenų saugos priemones ir kontroliuoja, kaip jų laikomasi;

10.7. rengia ir tvirtina teisės aktų projektus, susijusius su Informacinės sistemos duomenų tvarkymu ir sauga;

10.8. užtikrina, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję užtikrinti konfidencialumą arba jiems būtų taikomi atitinkamais teisės aktais nustatyti konfidencialumo reikalavimai;

10.9. atsižvelgdamas į Informacinės sistemos duomenų tvarkymo pobūdį, taiko tinkamas technines ir organizacines priemones, kiek tai įmanoma, įgyvendinant prievolę atsakyti į prašymus pasinaudoti Reglamento (ES) 2016/679 III skyriuje nustatytomis duomenų subjektų teisėmis;

10.10. užtikrina Reglamento (ES) 2016/679 32–36 straipsniuose nustatytų prievolių laikymąsi, atsižvelgdamas į asmens duomenų tvarkymo pobūdį ir Informacinės sistemos asmens duomenų informaciją;

10.11. atlieka kitas Nuostatuose ir kituose teisės aktuose, susijusiuose su Informacinės sistemos tvarkymu, nustatytas funkcijas.

11. Informacinės sistemos duomenų teikėjai:

11.1. Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos (toliau – Valstybinė ligonių kasa), teikianti Privalomojo sveikatos draudimo informacinės sistemos „Sveidra“ duomenis;

11.2. Higienos institutas, teikiantis Mirties atvejų ir jų priežasčių valstybės registro duomenis;

11.3. Neįgalumo ir darbingumo nustatymo tarnyba prie Socialinės apsaugos ir darbo ministerijos (toliau – Neįgalumo ir darbingumo nustatymo tarnyba), teikianti Neįgalumo ir darbingumo nustatymo tarnybos informacinės sistemos duomenis;

11.4. Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos (toliau – Valstybinio socialinio draudimo fondo valdyba), teikianti Valstybinio socialinio draudimo fondo valdybos informacinės sistemos duomenis.

III SKYRIUS
INFORMACINĖS SISTEMOS INFORMACINĖ STRUKTŪRA

12. Informacinę struktūrą sudaro:

12.1. traumų ir nelaimingų atsitikimų duomenų bazė;

12.2. ataskaitų duomenų bazė.

13. Traumų ir nelaimingų atsitikimų duomenų bazėje saugomi:

13.1. bendrieji duomenys:

13.1.1. gimimo data;

13.1.2. lytis;

13.1.3. savivaldybė;

13.2. duomenys apie asmens sveikatos priežiūros įstaigą (toliau – ASPĮ) ir asmeniui, patyrusiam sužalojimą / apsinuodijimą, suteiktas sveikatos priežiūros paslaugas:

13.2.1. ASPĮ kodas;

13.2.2. ASPĮ pavadinimas;

13.2.3. atvykimo informacija: siunčianti ASPĮ, siuntimo priežastis, atvežė greitosios medicinos pagalbos brigada, būtinoji pagalba;

13.2.4. stacionarinio gydymo epizodo informacija:

13.2.4.1. atvykimo, išvykimo data ir laikas;

13.2.4.2. lovadienių skaičius;

13.2.4.3. epizodo tipas;

13.2.4.4. skyrius, paslaugos kodas, diagnozės kodas, gydytojo spaudo numeris, paslaugos kaina;

13.2.4.5. medicininės intervencijos data, kodas, specialisto spaudo numeris, paslaugos kodas, kaina;

13.2.5. ambulatorinio gydymo epizodo informacija: apsilankymo data, tipas, diagnozės kodas, specialisto spaudo numeris, paslaugos kodas ir kaina;

13.2.6. epizodo metu nustatytos diagnozės ir traumos priežastys, kodai pagal Tarptautinės statistinės ligų ir sveikatos sutrikimų klasifikacijos dešimtąjį pataisytą ir papildytą leidimą „Sisteminis ligų sąrašas“ (Australijos modifikacija, TLK-10-AM), įdiegtą Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. vasario 23 d. įsakymu Nr. V-164 „Dėl Tarptautinės statistinės ligų ir sveikatos sutrikimų klasifikacijos dešimtojo pataisyto ir papildyto leidimo „Sisteminis ligų sąrašas“ (Australijos modifikacija, TLK-10-AM) įdiegimo“ (toliau – Tarptautinės statistinės ligų ir sveikatos sutrikimų klasifikacijos dešimtasis pataisytas ir papildytas leidimas „Sisteminis ligų sąrašas“ (Australijos modifikacija, TLK-10-AM));

13.2.7. asmens priemokos ir mokamos paslaugos;

13.2.8. centralizuotai perkami vaistai ir medicinos priemonės;

13.2.9. gydymo rezultatas;

13.2.10. bendra epizodo kaina;

13.2.11. gydančio gydytojo spaudo numeris;

13.3. bendrieji formos Nr. 106/a, patvirtintos Lietuvos Respublikos sveikatos apsaugos ministro 2014 m. birželio 9 d. įsakymu Nr. V-667 „Dėl Medicininio mirties liudijimo formų ir jų pildymo taisyklių patvirtinimo“, duomenys:

13.3.1. mirties data, laikas;

13.3.2. mirties vieta;

13.3.3. mirties priežastys;

13.4. duomenys apie asmeniui nustatytą neįgalumo ar darbingumo lygį:

13.4.1. asmeniui nustatytas neįgalumo lygis;

13.4.2. neįgalumo lygio nustatymo pradžios data;

13.4.3. neįgalumo lygio nustatymo pabaigos data;

13.4.4. pagrindinė diagnozė;

13.4.5. asmeniui nustatytas darbingumo lygis;

13.4.6. darbingumo lygio nustatymo pradžios data;

13.4.7. darbingumo lygio nustatymo pabaigos data;

13.4.8. pagrindinė diagnozė;

13.5. bendrieji Nedarbingumo pažymėjimo duomenys:

13.5.1. laikinojo nedarbingumo data nuo, data iki;

13.5.2. laikinojo nedarbingumo diagnozė;

13.5.3. išmokėta ligos pašalpos suma;

13.5.4. laikinojo nedarbingumo priežastis (nelaimingas atsitikimas buityje, nelaimingas atsitikimas darbe, kelyje į (iš) darbą (-o));

13.5.5. nelaimingas atsitikimas darbe, kelyje į (iš) darbą (-o) pripažintas draudiminiu įvykiu, pripažintas nedraudiminiu įvykiu;

13.6. klasifikatorių duomenys:

13.6.1. Tarptautinės statistinės ligų ir sveikatos sutrikimų klasifikacijos dešimtasis pataisytas ir papildytas leidimas „Sisteminis ligų sąrašas“ (Australijos modifikacija, TLK-10-AM) ir jo pakeitimai;

13.6.2. Australijos medicininių intervencijų klasifikacija (ACHI), sisteminis intervencijų sąrašas, įdiegtas Lietuvos Respublikos sveikatos apsaugos ministro 2010 m. kovo 30 d. įsakymu Nr. V-229 „Dėl medicininių intervencijų klasifikacijos naudojimo“;

13.6.3. valstybių ir savivaldybių kodų klasifikatorius.

14. Ataskaitų duomenų bazėje tvarkomi ir saugomi duomenys, kurių reikia ataskaitoms formuoti, statistikai skaičiuoti ir analizei vykdyti:

14.1. ambulatorinių ligonių, gydytų stacionaro priėmimo-skubiosios pagalbos skyriuose dėl traumų ir nelaimingų atsitikimų, skaičius pagal diagnozes, traumų aplinkybes, vietą ir veiklą, pagal asmens sveikatos priežiūros įstaigas, pagal regionus, amžių, lytį, gyvenamąją vietovę;

14.2. stacionaro ligonių, gydytų dėl traumų ir nelaimingų atsitikimų, skaičius pagal diagnozes, traumų aplinkybes, vietą ir veiklą, pagal asmens sveikatos priežiūros įstaigas, pagal regionus, amžių, lytį, gyvenamąją vietovę;

14.3. laikinojo nedarbingumo atvejų dėl traumų ir nelaimingų atsitikimų skaičius pagal diagnozes, nedarbingumo priežastį, regionus, amžių, lytį, gyvenamąją vietovę;

14.4. asmenų, kuriems pirmą kartą nustatytas neįgalumas / darbingumo lygis dėl traumų ir nelaimingų atsitikimų, skaičius pagal diagnozes, neįgalumo / darbingumo lygį, regionus, amžių, lytį, gyvenamąją vietovę;

14.5. asmenų, mirusių nuo traumų ir nelaimingų atsitikimų, skaičius pagal diagnozes, regionus, amžių, lytį, gyvenamąją vietovę.

15. Informacinės sistemos duomenų teikėjai teikia šiuos duomenis:

15.1. Valstybinė ligonių kasa teikia Privalomojo sveikatos draudimo informacinės sistemos „Sveidra“ duomenis, nurodytus šių Nuostatų 13.1.1–13.1.3, 13.2.1–13.2.11, 13.6.1–13.6.3 papunkčiuose;

15.2. Valstybinio socialinio draudimo fondo valdyba teikia Valstybinio socialinio draudimo fondo valdybos informacinės sistemos duomenis, nurodytus šių Nuostatų 13.1.1–13.1.2 ir 13.5.1–13.5.5 papunkčiuose;

15.3. Neįgalumo ir darbingumo nustatymo tarnyba teikia Neįgalumo ir darbingumo nustatymo tarnybos informacinės sistemos duomenis, nurodytus šių Nuostatų 13.1.1–13.1.2 ir 13.4.1–13.4.8 papunkčiuose;

15.4. Higienos institutas teikia Mirties atvejų ir jų priežasčių valstybės registro duomenis, nurodytus šių Nuostatų 13.1.1–13.1.3 ir 13.3.1–13.3.3 papunkčiuose.

IV SKYRIUS
INFORMACINĖS SISTEMOS FUNKCINĖ STRUKTŪRA

16. Informacinės sistemos funkcinę struktūrą sudaro:

16.1. duomenų mainų posistemė;

16.2. analitinės informacijos posistemė;

16.3. administravimo posistemė.

17. Duomenų mainų posistemė vykdo duomenų surinkimą iš kitų informacinių sistemų, jų

kaupimą.

18. Analitinės informacijos posistemė vykdo:

18.1. ataskaitų formavimą,

18.2. informacijos paiešką;

18.3. duomenų eksportą duomenų teikimui, tolimesnei analizei ir apdorojimui.

19. Administravimo posistemė vykdo:

19.1. sistemos naudotojų identifikavimą ir autentifikavimą;

19.2. sistemos naudotojų ir jų prieigos teisių valdymą;

19.3. sistemos parametrų valdymą;

19.4. informacinės sistemos duomenų srautų valdymą.

V SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ TEIKIMAS IR NAUDOJIMAS

20. Informacinės sistemos duomenys yra vieši ir teikiami duomenų gavėjams, jeigu Lietuvos Respublikos įstatymai ir (ar) Europos Sąjungos teisės aktai nenustato kitaip.

21. Informacinės sistemos asmens duomenys teikiami duomenų gavėjams vadovaujantis Reglamento (ES) 2016/679 nustatytais su asmens duomenų tvarkymu susijusiais principais ir esant teisėtoms asmens duomenų tvarkymo sąlygoms bei kitais teisės aktais, reglamentuojančiais asmens duomenų teikimą fiziniams ir juridiniams asmenims. Informacinės sistemos asmens duomenys neteikiami, jeigu duomenų gavėjui gauti šiuos duomenis nėra teisinio pagrindo.

22. Informacinės sistemos duomenys ES valstybių narių ir (arba) Europos ekonominės erdvės valstybių fiziniams ir juridiniams asmenims, juridinio asmens statuso neturintiems subjektams, jų filialams ir atstovybėms teikiami ta pačia tvarka, kaip ir Lietuvos Respublikos fiziniams ir juridiniams asmenims.

23. Informacinės sistemos duomenys trečiųjų šalių fiziniams ir juridiniams asmenims, juridinio asmens statuso neturintiems subjektams, jų filialams ir atstovybėms teikiami ta pačia tvarka, kaip ir Lietuvos Respublikos fiziniams ir juridiniams asmenims, jeigu tai neprieštarauja Lietuvos Respublikos įstatymams, tarptautinėms sutartims ir kitiems teisės aktams bei vadovaujantis Reglamento (ES) 2016/679 V skyriaus nuostatomis.

24. Informacinės sistemos duomenys gali būti teikiami leidžiamosios kreipties būdu internetu ar elektroninių ryšių tinklais, pateikiami raštu, žodžiu ir (arba) elektroninių ryšių priemonėmis.

25. Informacinės sistemos duomenys teikiami pagal duomenų teikimo sutartis (daugkartinio teikimo atvejais) arba pagal duomenų gavėjo prašymą (vienkartinio teikimo atvejais). Kai informacija teikiama pagal duomenų gavėjo prašymą, prašyme turi būti nurodytas prašomos informacijos teikimo ir gavimo teisinis pagrindas, jos naudojimo tikslas, teikimo būdas, apimtis, gavimo būdai, teikiamų duomenų formatas. Kai informacija duomenų gavėjui teikiama pagal duomenų teikimo sutartį, sutartyje turi būti nustatyta teikiamos informacijos apimtis, prašomos informacijos teikimo ir gavimo teisinis pagrindas, naudojimo tikslas, informacijos teikimo būdas, teikiamų duomenų formatas, teikimo terminai, informavimo apie klaidų ištaisymą tvarka ir terminai, sutarties keitimo tvarka.

26. Duomenys duomenų gavėjams teikiami tokio turinio ir tokios formos, kurie Informacinės sistemos valdytojo ir tvarkytojo naudojami ir nereikalauja papildomo duomenų apdorojimo. Valstybės informacinių išteklių valdymo įstatymo 35 straipsnio 3 dalyje nurodytais atvejais Lietuvos Respublikos Vyriausybės nustatyta tvarka duomenys gali būti pateikiami duomenų gavėjo prašomo formato ir turinio.

27. Informacinės sistemos duomenų gavėjo gauti Informacinės sistemos duomenys negali būti naudojami kitaip ar kitu tikslu, negu buvo nurodyta juos gaunant. Informacinės sistemos duomenų pakartotinio naudojimo sąlygas nustato Teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatymo 8 straipsnis.

28. Informacinės sistemos duomenys teikiami neatlygintinai.

29. Kai atsisakoma teikti Informacinės sistemos duomenis, asmeniui, pateikusiam prašymą juos gauti, raštu arba elektroninių ryšių priemonėmis pranešama apie priimtą motyvuotą sprendimą atsisakyti tenkinti jo prašymą ir suteikiama informacija apie tokio sprendimo apskundimo tvarką.

30. Duomenų subjektai, jų įstatyminiai atstovai, duomenų gavėjai, registro ar kitos valstybės informacinės sistemos tvarkytojai, kiti asmenys turi teisę reikalauti ištaisyti neteisingus, netikslius, neišsamius Informacinės sistemos duomenis (toliau – netikslūs duomenys). Rašytinį prašymą ištaisyti netikslius duomenis galima pateikti asmeniškai, paštu ar elektroninių ryšių priemonėmis.

31. Informacinės sistemos valdytojas ir tvarkytojas, gavęs duomenų subjektų, jų įstatyminių atstovų, duomenų gavėjų, registro ar kitos valstybės informacinės sistemos tvarkytojų, kitų asmenų rašytinį prašymą ištaisyti netikslius duomenis, nedelsdamas (ne ilgiau kaip per 5 darbo dienas) patikrina Informacinės sistemos duomenų tikslumą ir prireikus ištaiso netikslius duomenis. Pranešimas apie netikslių duomenų ištaisymą arba apie motyvuotą atsisakymą tai padaryti nedelsiant (ne vėliau kaip per vieną darbo dieną) siunčiamas asmeniui, pateikusiam rašytinį prašymą ištaisyti netikslius duomenis, paštu ir (ar) elektroninių ryšių priemonėmis. Ištaisęs netikslius duomenis, Informacinės sistemos valdytojas ir tvarkytojas per vieną darbo dieną nuo jų ištaisymo apie tai praneša Informacinės sistemos duomenų gavėjams, kuriems perduoti netikslūs duomenys. Informacinės sistemos valdytojas ir tvarkytojas, nustatęs, kad yra Informacinės sistemos duomenų netikslumų, turi nedelsdamas (ne vėliau kaip per vieną darbo dieną) elektroninių ryšių tinklais perduoti šią informaciją susijusiam duomenų teikėjui.

32. Informacinės sistemos duomenų pagrindu parengta statistinė informacija apie traumas ir nelaimingus atsitikimus yra viešai skelbiama Informacinės sistemos valdytojo ir tvarkytojo interneto svetainėje.

VI SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ SAUGA

33. Informacinės sistemos duomenų saugą ir asmens duomenų saugumą reglamentuoja Informacinės sistemos duomenų saugos nuostatai, kiti saugos politiką įgyvendinantys dokumentai, kurie rengiami, derinami ir tvirtinami Lietuvos Respublikos Vyriausybės nustatyta tvarka. Siekiant užtikrinti Informacinės sistemos duomenų saugą, vadovaujamasi:

33.1. Reglamentu (ES) 2016/679;

33.2. Kibernetinio saugumo įstatymu;

33.3. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu 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“;

33.4. 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“;

33.5. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu 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“.

34. Už duomenų saugą Lietuvos Respublikos įstatymų nustatyta tvarka atsako Informacinės sistemos valdytojas ir tvarkytojas. Prireikus nustatoma duomenų teikėjų ir kitų asmenų atsakomybė už Informacinės sistemos duomenų saugą.

35. Duomenų saugos priemonės turi užtikrinti:

35.1. informacinių technologijų priemonėmis perduodamų, saugomų, apdorojamų ir naudojamų duomenų saugą;

35.2. Informacinės sistemos duomenų saugą nuo atsitiktinio ar neteisėto sunaikinimo, atskleidimo, pakeitimo ir kitokio neteisėto tvarkymo.

36. Informacinės sistemos valdytojo ir tvarkytojo darbuotojai, Informacinėje sistemoje tvarkantys asmens duomenis, įpareigojami saugoti Informacinėje sistemoje esančių asmens duomenų paslaptį, nepažeisdami Reglamento (ES) 2016/679 ir kitų teisės aktų reikalavimų. Ši pareiga galioja ir jiems nutraukus su Informacinės sistemos duomenų tvarkymu susijusią veiklą, perėjus dirbti į kitas pareigas, pasibaigus jų darbo ar sutartiniams santykiams.

37. Informacinės sistemos duomenys saugomi 50 metų, po to perkeliami į Informacinės sistemos archyvą, kuriame yra saugomi 30 metų. Pasibaigus duomenų saugojimo Informacinėje sistemoje duomenų bazės archyve terminui, duomenys sunaikinami. Informacinėje sistemoje esantys duomenys, praradę savo aktualumą, sunaikinami arba perduodami valstybės archyvams ar kitai valdytojo informacinei sistemai Lietuvos Respublikos dokumentų ir archyvų įstatymo ir kitų teisės aktų nustatyta tvarka.

VII SKYRIUS
FINANSAVIMAS

38. Informacinė sistema finansuojama iš Lietuvos Respublikos valstybės biudžeto (įskaitant Europos Sąjungos lėšas).

VIII SKYRIUS
INFORMACINĖS SISTEMOS MODERNIZAVIMAS IR LIKVIDAVIMAS

39. Informacinė sistema modernizuojama arba likviduojama Valstybės informacinių išteklių valdymo įstatymo ir Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“, nustatyta tvarka.

40. Jei Informacinė sistema likviduojama, jos duomenys perduodami kitai valstybės informacinei sistemai, valstybės archyvui arba sunaikinami Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

41. Duomenų subjektų teisės yra įgyvendinamos vadovaujantis Reglamentu (ES) Nr. 2016/679 ir Duomenų subjektų teisių įgyvendinimo tvarkant asmens duomenis Higienos instituto valdomuose registruose ir valstybės informacinėse sistemose tvarkos aprašu, patvirtintu Higienos instituto direktoriaus 2023 m. liepos 25 d. įsakymu Nr. V-87 „Dėl Duomenų subjektų teisių įgyvendinimo tvarkant asmens duomenis Higienos instituto valdomuose registruose ir valstybės informacinėse sistemose tvarkos aprašo patvirtinimo“.

Priedo pakeitimai:
Nr. V-946, 2023-08-30, paskelbta TAR 2023-08-30, i. k. 2023-17075

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos
ministro 2014 m. liepos 9 d.
įsakymu Nr. V-776
(Lietuvos Respublikos sveikatos apsaugos
ministro 2023 m. rugpjūčio 30 d.
įsakymo Nr. V-946
redakcija)

TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos (toliau – Informacinė sistema) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika), kurios tikslas – nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, suteikiančias galimybę saugiai tvarkyti elektroninę informaciją, ir užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo ar neteisėto tvarkymo.

2. Informacinės sistemos elektroninės informacijos saugos politika įgyvendinama pagal Lietuvos Respublikos sveikatos apsaugos ministro tvirtinamus Saugos nuostatus ir saugos politiką įgyvendinančius dokumentus: saugaus elektroninės informacijos tvarkymo taisykles, naudotojų administravimo taisykles, veiklos tęstinumo valdymo planą (toliau visi kartu – Saugos dokumentai).

3. Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo 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), 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 – Kibernetinio saugumo reikalavimų aprašas), vartojamas sąvokas.

4. Informacinės sistemos elektroninės informacijos saugos ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) užtikrinimo tikslai:

4.1. automatiniu būdu tvarkomos elektroninės informacijos saugumo užtikrinimas;

4.2. elektroninės informacijos patikimumo ir saugumo nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo ar neteisėto jos tvarkymo, užtikrinimas;

4.3. elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai), asmens duomenų saugumo pažeidimų prevencijos vykdymas, reagavimas į saugos incidentų, asmens duomenų saugumo pažeidimus ir jų operatyvus valdymas.

5. Informacinės sistemos elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Informacinės sistemos duomenų saugai užtikrinti, įgyvendinimas ir šių priemonių kontrolė;

5.2. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.3. Informacinės sistemos veiklos tęstinumo užtikrinimas;

5.4. Informacinės sistemos asmens duomenų apsauga.

6. Saugos nuostatų reikalavimai taikomi:

6.1. Informacinės sistemos valdytojui ir tvarkytojui – Higienos institutui (toliau – Informacinės sistemos valdytojas ir tvarkytojas), Studentų g. 45A, Vilnius;

6.2. Informacinės sistemos saugos įgaliotiniui;

6.3. Informacinės sistemos administratoriui;

6.4. Informacinės sistemos duomenų valdymo įgaliotiniui;

6.5. Informacinės sistemos naudotojams;

6.6. asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą Higienos institute tvarkomuose registruose ir informacinėse sistemose (toliau – kibernetinio saugumo vadovas).

7. Informacinės sistemos valdytojo ir tvarkytojo funkcijos:

7.1. pagal kompetenciją atsako už Informacinės sistemos saugos politikos formavimą, jos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;

7.2. užtikrina veiksmingą ir spartų Informacinės sistemos pokyčių valdymo planavimą;

7.3. skiria kibernetinio saugumo vadovą, Informacinės sistemos duomenų valdymo įgaliotinį, Informacinės sistemos saugos įgaliotinį, Informacinės sistemos administratorių;

7.4. atlieka Informacinės sistemos duomenų bazės techninę priežiūrą ir užtikrina nepertraukiamą Informacinės sistemos veikimą;

7.5. užtikrina saugią Informacinės sistemos sąveiką su kitomis informacinėmis sistemomis ir registrais;

7.6. įgyvendina tinkamas organizacines ir technines priemones, skirtas elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

7.7. teikia pasiūlymus Lietuvos Respublikos sveikatos apsaugos ministerijai dėl Informacinės sistemos techninių ir programinių priemonių, būtinų Informacinės sistemos elektroninės informacijos saugai užtikrinti, finansavimo, įsigijimo, įdiegimo ir modernizavimo, organizuoja jų įdiegimą ir modernizavimą;

7.8. vykdo kitas teisės aktuose, reglamentuojančiuose valstybės registrų ir informacinių sistemų saugą, nustatytas funkcijas.

8. Informacinės sistemos saugos įgaliotinio funkcijos:

8.1. koordinuoja ir prižiūri Informacinės sistemos elektroninės informacijos saugos politikos įgyvendinimą;

8.2. teikia Informacinės sistemos valdytojui ir tvarkytojui pasiūlymus, kaip nustatyta Bendrųjų elektroninės informacijos saugos reikalavimų apraše;

8.3. organizuoja Informacinės sistemos informacinių technologijų saugos atitikties vertinimą ir parengia saugos atitikties vertinimo ataskaitą;

8.4. organizuoja Informacinės sistemos rizikos įvertinimą (prireikus ir neeilinius rizikos vertinimus) ir parengia rizikos įvertinimo ataskaitą;

8.5. supažindina Informacinės sistemos administratorių ir Informacinės sistemos naudotojus su Saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą, organizuoja Informacinės sistemos naudotojų mokymą elektroninės informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas;

8.6. teikia Informacinės sistemos administratoriui ir Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;

8.7. turi teisę pagal savo įgaliojimus duoti privalomus vykdyti nurodymus ir pavedimus ir kitiems Informacinės sistemos valdytojo ir tvarkytojo darbuotojams, jeigu tai būtina saugos politikai įgyvendinti;

8.8. koordinuoja saugos incidentų, įvykusių Informacinėje sistemoje, tyrimą;

8.9. vykdo kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Saugos nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

9. Informacinės sistemos administratoriaus funkcijos:

9.1. atsako už Informacinės sistemos techninės ir programinės įrangos funkcionavimą;

9.2. diegia ir prižiūri programinę įrangą, reikalingą Informacinės sistemos naudotojų funkcijoms vykdyti;

9.3. suteikia teisę Informacinės sistemos naudotojams naudotis elektronine informacija, reikalinga jų funkcijoms atlikti;

9.4. užtikrina Informacinės sistemos komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimo aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą, pagal kompetenciją nustato pažeidžiamas Informacinės sistemos vietas;

9.5. dalyvauja vykdant saugumo reikalavimų įgyvendinimo stebėseną;

9.6. pagal kompetenciją teikia Informacinės sistemos valdytojo ir tvarkytojo vadovui pasiūlymus dėl Informacinės sistemos palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

9.7. nuolat teikia Informacinės sistemos saugos įgaliotiniui informaciją apie Informacinės sistemos saugą užtikrinančių pagrindinių komponentų būklę, taip pat informuoja apie saugos incidentus ir teikia pasiūlymus dėl saugos incidentų pašalinimo;

9.8. vykdo kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Saugos nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

10. Teisės aktai, kuriais vadovaujantis tvarkoma Informacinės sistemos elektroninė informacija ir užtikrinama jos sauga:

10.1. 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);

10.2. Valstybės informacinių išteklių valdymo įstatymas;

10.3. Kibernetinio saugumo įstatymas;

10.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

10.5. Kibernetinio saugumo reikalavimų aprašas;

10.6. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas ir Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinti 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 – Saugos atitikties vertinimo metodika);

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

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

10.9. Informacinės sistemos nuostatai;

10.10. kiti teisės aktai, reglamentuojantys elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugos valdymą valstybės institucijose.

II SKYRIUS

ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

11. Vadovaujantis Klasifikavimo gairių aprašo 9.1, 9.2 ir 12.3 papunkčių reikalavimais:

11.1. Informacinėje sistemoje tvarkoma elektroninė informacija pagal svarbą priskiriama vidutinės svarbos informacijos kategorijai;

11.2. pagal Informacinėje sistemoje tvarkomos elektroninės informacijos svarbą Informacinė sistema priskiriama trečios kategorijos informacinėms sistemoms.

12. Informacinės sistemos saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos (toliau – Kibernetinio saugumo centras) interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja Informacinės sistemos rizikos įvertinimą. Prireikus saugos įgaliotinis gali organizuoti neeilinį Informacinės sistemos rizikos įvertinimą.

13. Informacinės sistemos rizikos vertinimo metu įvertinami rizikos veiksniai, galintys turėti įtakos Informacinės sistemos elektroninės informacijos saugai, jų galima žala, pasireiškimo tikimybė, rizikos laipsnis ir galimi rizikos valdymo būdai. Kartu su Informacinės sistemos rizikos vertinimu gali būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos Informacinės sistemos kibernetiniam saugumui, vertinimas. Svarbiausieji rizikos veiksniai nurodyti Bendrųjų elektroninės informacijos saugos reikalavimų apraše.

14. Informacinės sistemos rizikos veiksniams vertinti naudojama penkiabalė rizikos vertinimo sistema, pagal kurią, nustačius rizikos veiksnių tikimybę ir poveikį, apskaičiuojamas rizikos laipsnis:

14.1. nereikšminga rizikos veiksnių tikimybė, žala – 1 balas;

14.2. maža rizikos veiksnių tikimybė, žala – 2 balai;

14.3. vidutinė rizikos veiksnių tikimybė, žala – 3 balai;

14.4. didelė rizikos veiksnių tikimybė, žala – 4 balai;

14.5. labai didelė rizikos veiksnių tikimybė, žala – 5 balai.

15. Informacinės sistemos rizikos įvertinimo rezultatai pateikiami rizikos įvertinimo ataskaitoje. Atsižvelgdamas į rizikos įvertinimo ataskaitą, Informacinės sistemos valdytojas ir tvarkytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame yra numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

16. Patvirtintas rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano, jei toks buvo parengtas, kopijas Informacinės sistemos valdytojas ir tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – ARSIS).

17. Elektroninės informacijos saugos priemonių parinkimo principai:

17.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

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

17.3. kur galima, turi būti įdiegiamos prevencinės elektroninės informacijos saugos priemonės;

17.4. parenkamos tokios saugos priemonės, kad būtų užtikrintas Informacinės sistemos veiklos tęstinumas ir saugus Informacinės sistemos darbas, patiriant kuo mažiau išlaidų.

18. Siekiant įvertinti Saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, vadovaujantis Saugos atitikties vertinimo metodika, kartą per metus organizuojamas Informacinės sistemos informacinių technologijų saugos atitikties vertinimas naudojantis ARSIS.

19. Atlikus Informacinės sistemos informacinių technologijų saugos reikalavimų atitikties vertinimą, rengiama Informacinės sistemos saugos atitikties vertinimo ataskaita, prireikus ir pastebėtų trūkumų šalinimo planas.

20. Informacinių technologijų saugos atitikties vertinimo ataskaitos kopiją, pastebėtų trūkumų

šalinimo plano kopiją Informacinės sistemos valdytojas ir tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo turi pateikti ARSIS.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

21. Programinės įrangos, skirtos apsaugoti Informacinę sistemą nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir atnaujinimo reikalavimai:

21.1. Informacinės sistemos tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės;

21.2. apsaugai naudojama programinė įranga turi atsinaujinti automatiniu būdu ne rečiau kaip kartą per 24 valandas;

21.3. elektroninės informacijos apsaugai naudojama programinė įranga turi turėti apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti kenkimo programų apsaugas;

21.4. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

22. Programinės įrangos, įdiegtos Informacinės sistemos tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

22.1. turi būti naudojama tik legali Informacinės sistemos funkcijoms vykdyti būtina programinė įranga;

22.2. Informacinės sistemos programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka tik Informacinės sistemos administratorius arba kitas Informacinės sistemos valdytojo ir tvarkytojo įgaliotas asmuo;

22.3. turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie Informacinės sistemos elektroninės informacijos, atliktus veiksmus;

22.4. Informacinės sistemos programinė įranga atnaujinama laikantis gamintojo reikalavimų.

23. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų ir kita) pagrindinės naudojimo nuostatos:

23.1. Informacinės sistemos elektroninės informacijos perdavimo tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, DoS (angl. *Denial of Service*) ir DDoS (angl. *Distributed Denial of Service*), ir kitų atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

23.2. Informacinės sistemos tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių Informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

23.3. viešaisiais ryšių tinklais perduodamos Informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network*), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas priemones.

24. Leistinos kompiuterių naudojimo ribos:

24.1. Informacinės sistemos duomenų tvarkymui leidžiama naudoti tik leistinus stacionarius ir nešiojamuosius kompiuterius, atitinkančius teisės aktų nustatytus elektroninės informacijos saugos reikalavimus;

24.2. stacionarieji ir nešiojamieji Informacinės sistemos naudotojų kompiuteriai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš perduodamų remontuoti ar techninei priežiūrai atlikti kompiuterių turi būti pašalinti visi Informacinės sistemos duomenys ir Informacinės sistemos informacija;

24.3. nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis, jie turi būti atskirti nuo viešojo interneto tinklo užkarda;

24.4. Informacinės sistemos naudotojai privalo naudotis visomis saugumo priemonėmis, siekiant apsaugoti kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo, nenaudojami nešiojamieji kompiuteriai turi būti saugomi saugioje vietoje.

25. Metodai, kuriais užtikrinamas saugus Informacinės sistemos elektroninės informacijos teikimas ir (ar) gavimas:

25.1. elektroninė informacija iš susijusių registrų ir informacinių sistemų gaunama tik pagal duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

25.2. prieigos prie Informacinės sistemos elektroninės informacijos teises gali suteikti tik Informacinės sistemos administratorius. Informacinės sistemos naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

25.3. prieiga prie Informacinės sistemos elektroninės informacijos leidžiama tik per registracijos slaptažodžių sistemą. Prieigos prie Informacinės sistemos elektroninės informacijos valdymas apibrėžtas Informacinės sistemos naudotojų administravimo taisyklėse.

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

26.1. Informacinės sistemos atsarginės elektroninės informacijos kopijos (toliau – kopijos) daromos automatiniu būdu kas 24 valandas, esant aktyviai Informacinės sistemos duomenų bazei;

26.2. elektroninė informacija kopijose turi būti šifruota;

26.3. kopijas turi teisę tvarkyti Informacinės sistemos administratorius arba techninės bei programinės įrangos priežiūros paslaugų teikėjai;

26.4. laikmenos, kuriose yra kopijos, saugomos kitoje patalpoje nei Informacinės sistemos tarnybinės stotys;

26.5. atkurti elektroninę informaciją iš kopijų turi teisę tik Informacinės sistemos administratorius.

27. Kopijų darymo ir saugojimo tvarka nustatoma Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

28. Turi būti užtikrintas saugos incidentų, įvykusių Informacinėje sistemoje, registravimas, valdymas ir tyrimas Kibernetinių saugumo reikalavimo aprašo bei Informacinės sistemos veiklos tęstinumo valdymo plano nustatyta tvarka:

28.1. registruojami Informacinėje sistemoje įvykę saugos incidentai ir nedelsiant į juos reaguojama, techninėmis ir programinėmis priemonėmis pagal kompetenciją saugos incidentai valdomi, tiriami ir šalinami bei atkuriama Informacinės sistemos veikla;

28.2. Kibernetinio saugumo centrui ir kitoms atsakingoms institucijoms pagal kompetenciją pranešama apie įvykusius saugos incidentus, jų vertinimą ir suvaldymą.

29. Perkant paslaugas, darbus ar įrangą, susijusius su Informacine sistema, jos projektavimu, kūrimu, diegimu, modernizavimu, priežiūra, palaikymu, saugos užtikrinimu, auditavimu, elektroninės informacijos perdavimo tinklais, taip pat kitus, suteikiančius teisę ir galimybę prieiti prie elektroninės informacijos, pirkimo dokumentuose turi būti nustatyta, kad asmuo, atliekantis Informacinės sistemos techninės ir programinės įrangos priežiūros ir duomenų, informacijos ir dokumentų ir (arba) jų kopijų tvarkymo funkcijas, negali turėti neišnykusio ar nepanaikinto teistumo už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat negali turėti paskirtos administracinės nuobaudos už Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 20 punkte nurodytus atvejus, jeigu nuo jos paskyrimo yra praėję mažiau kaip vieni metai, taip pat privalo laikytis Informacinės sistemos Saugos dokumentuose nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį nustatytiems Kibernetinio saugumo reikalavimų aprašo reikalavimams.

30. Į paslaugų pirkimo sutartį turi būti įtraukta nuostata, įpareigojanti paslaugų teikėjo darbuotojus pasirašyti konfidencialumo pasižadėjimą neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant šią sutartį, išskyrus tiek, kiek būtina sutarčiai vykdyti.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

31. Informacinės sistemos saugos įgaliotinis ir kibernetinio saugumo vadovas privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, prireikus tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą. Informacinės sistemos saugos įgaliotinis ar kibernetinio saugumo vadovas

pažeidęs Saugos nuostatų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

32. Informacinės sistemos saugos įgaliotiniu ir kibernetinio saugumo vadovu negali būti skiriami asmenys, turintys neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už Bendrųjų saugos reikalavimų aprašo 20 punkte nurodytus atvejus, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

33. Informacinės sistemos administratorius privalo išmanyti darbą su duomenų perdavimo tinklais, gebėti administruoti ir prižiūrėti Informacinės sistemos duomenų bazę, turi būti susipažinęs su Saugos nuostatais, Saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų duomenų tvarkymą. Informacinės sistemos administratorius, pažeidęs Saugos nuostatų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

34. Informacinės sistemos naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti Informacinės sistemos duomenis Saugos nuostatų nustatyta tvarka, būti susipažinę su Saugos dokumentais ir pasirašę pasižadėjimus saugoti konfidencialią elektroninę informaciją (toliau – Pasižadėjimas).

35. Informacinės sistemos naudotojai, pastebėję saugos reikalavimų, pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones Informacinėje sistemoje, privalo nedelsdami pranešti apie tai Informacinės sistemos administratoriui ar Informacinės sistemos saugos įgaliotiniui.

36. Kibernetinio saugumo vadovas arba Informacinės sistemos saugos įgaliotinis ne rečiau kaip kartą per dvejus metus inicijuoja Informacinės sistemos naudotojų mokymą elektroninės informacijos saugos klausimais, prireikus įvairiais būdais – pranešimais elektroniniu paštu, naujų darbuotojų instruktavimu, atmintinių rengimu, teminių seminarų organizavimu ir kitais informavimo būdais – primena apie saugumo problemas.

37. Informacinės sistemos naudotojų mokymai elektroninės informacijos saugos klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), Informacinės sistemos naudotojų, Informacinės sistemos duomenų valdymo įgaliotinio ir Informacinės sistemos administratoriaus poreikius.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

38. Tvarkyti Informacinės sistemos duomenis ir gauti informaciją gali tik Informacinės sistemos naudotojai, susipažinę su Saugos dokumentais ir raštu pasirašę Pasižadėjimus. Pasikeitus Informacinės sistemos Saugos dokumentams ar kitiems saugos politiką įgyvendinantiems teisės aktams, Informacinės sistemos naudotojai su jais supažindinami pakartotinai.

39. Už Informacinės sistemos naudotojų supažindinimą su Saugos dokumentais ir kitais saugos politiką įgyvendinančiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą atsakingas Informacinės sistemos saugos įgaliotinis.

40. Informacinės sistemos naudotojai, pažeidę Saugos nuostatų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

Priedo pakeitimai:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404
Nr. V-946, 2023-08-30, paskelbta TAR 2023-08-30, i. k. 2023-17075

Pakeitimai:

1.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404
Dėl Lietuvos Respublikos sveikatos apsaugos ministerijos 2014 m. liepos 9 d. įsakymo Nr. V-776 "Dėl Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos nuostatų ir duomenų saugos nuostatų patvirtinimo" pakeitimo

2.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-946, 2023-08-30, paskelbta TAR 2023-08-30, i. k. 2023-17075
Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2014 m. liepos 9 d. įsakymo Nr. V-776 „Dėl Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos nuostatų ir duomenų saugos nuostatų patvirtinimo“ pakeitimo