Suvestinė redakcija nuo 2018-05-09 iki 2023-08-30

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 8 straipsniu, 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 ir 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 ir 19 punktais:

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

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

TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

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

2. Informacinė sistema yra steigiama vadovaujantis Lietuvos Respublikos sveikatos apsaugos ministerijos nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 1998 m. liepos 24 d. nutarimu Nr. 926 „Dėl Lietuvos Respublikos sveikatos apsaugos ministerijos nuostatų patvirtinimo“, 9 punktu.

3. Informacinės veiklos sritį reglamentuojantys teisės aktai, kuriais vadovaujantis tvarkoma Informacinė sistema:

3.1. Lietuvos Respublikos civilinis kodeksas;

3.2. Lietuvos Respublikos visuomenės sveikatos priežiūros įstatymas;

3.3. Lietuvos Respublikos visuomenės sveikatos stebėsenos (monitoringo) įstatymas;

3.4. Lietuvos Respublikos sveikatos sistemos įstatymas;

3.5. Lietuvos Respublikos sveikatos priežiūros įstaigų įstatymas;

3.6. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

3.7. Lietuvos Respublikos kibernetinio saugumo įstatymas;

Papildyta papunkčiu:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404

3.8. Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimas Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“;
Papildyta papunkčiu:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404

3.9. Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. kovo 28 d. įsakymas Nr. V-294 „Dėl Lietuvos E. sveikatos sistemos funkcinės, techninės ir programinės įrangos modelio patvirtinimo“;
Punkto numeracijos pakeitimas:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404

3.10. Lietuvos Respublikos Vyriausybės 2011 m. rugsėjo 7 d. nutarimas Nr. 1057 „Dėl Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatų patvirtinimo“;
Punkto numeracijos pakeitimas:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404

3.11 Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimas Nr. 180 „Dėl valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“;
Punkto numeracijos pakeitimas:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404

3.12. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas 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“;
Punkto pakeitimai:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404
Punkto numeracijos pakeitimas:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404

3.13. kiti teisės aktai, reglamentuojantys saugų elektroninės informacijos tvarkymą, saugojimą bei sunaikinimą.
Punkto numeracijos pakeitimas:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404

4. Šiuose nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarime Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“ ir kituose teisės aktuose vartojamas sąvokas.

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

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

7. Informacinės sistemos pagrindinės funkcijos:

7.1. iš informacinių sistemų surinkti duomenis apie traumas ir nelaimingus atsitikimus;

7.2. teikti duomenis Informacinės sistemos naudotojams.

II SKYRIUS
INFORMACINĖS SISTEMOS ORGANIZACINĖ STRUKTŪRA

8. Informacinės sistemos organizacinė struktūra:

8.1. Informacinės sistemos valdytoja – Lietuvos Respublikos sveikatos apsaugos ministerija (toliau – Sveikatos apsaugos ministerija);

8.2. Informacinės sistemos tvarkytojas – Higienos institutas.

9. Informacinės sistemos valdytoja vykdo Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme nustatytas funkcijas, turi šiame įstatyme nurodytas teises ir pareigas. Taip pat Informacinės sistemos valdytoja atlieka šias funkcijas:

9.1. priima sprendimus, susijusius su Informacinės sistemos kūrimu, plėtra, likvidavimu, modernizavimu, priežiūra, administravimu ir kontroliuoja jų vykdymą;

9.2. užtikrina nustatyto Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų mainų būdo ir formato laikymąsi;

9.3. tvirtina su Informacinės sistemos veikla, informacinių ir ryšių technologijų infrastruktūra susijusius dokumentus;

9.4. nagrinėja siūlymus tobulinti Informacinę sistemą, tvirtina Informacinės sistemos kūrimo, plėtros planus ir projektus, Informacinės sistemos tvarkymo ir administravimo veiklos planus ir ataskaitas bei kontroliuoja jų vykdymą;

9.5. vertina Informacinės sistemos tvarkytojo siūlymus dėl duomenų tvarkymo tikslų bei priemonių ir priima dėl jų atitinkamus sprendimus;

9.6. analizuoja teisines, technines, technologines, metodines ir organizacines Informacinės sistemos tvarkymo problemas ir pagal savo kompetenciją priima sprendimus, reikalingus Informacinės sistemos veiklai užtikrinti;

9.7. teisės aktų nustatyta tvarka teikia informaciją apie Informacinės sistemos veiklą.

10. Informacinės sistemos tvarkytojas vykdo Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme nustatytas funkcijas, turi šiame įstatyme nurodytas teises ir pareigas. Taip pat atlieka šias funkcijas:

10.1. teisės aktų nustatyta tvarka rengia teisės aktų projektus, susijusius su Informacinės sistemos duomenų tvarkymu ir sauga;

10.2. teikia Informacinės sistemos valdytojui siūlymus, susijusius su duomenų tvarkymu ir duomenų sauga, Informacinės sistemos kūrimu, plėtra, likvidavimu, modernizavimu, priežiūra, administravimu ir kartu su Informacinės sistemos valdytoju priima susijusius sprendimus;

10.3. rengia ir teikia derinimui su Informacinės sistemos veikla, informacinių ir ryšių technologijų infrastruktūra, duomenų tvarkymu ir sauga susijusių teisės aktų projektus;

10.4. rengia ir teikia derinti Informacinės sistemos tvarkymo ir administravimo veiklos planų ir ataskaitų projektus;

10.5. teikia siūlymus teisinėms, techninėms, technologinėms, metodinėms ir organizacinėms Informacinės sistemos tvarkymo problemoms spręsti ir kartu su Informacinės sistemos valdytoju priima susijusius sprendimus;

10.6. užtikrina Informacinės sistemos veikimui ir duomenų mainams su kitomis informacinėmis sistemomis ir registrais būtinos techninės ir programinės įrangos įdiegimą, nepertraukiamą funkcionavimą ir atnaujinimą;

10.7. administruoja Informacinės sistemos duomenų saugyklą, duomenų archyvą techninės ir funkcinės įrangos centre ir užtikrina jų saugą;

10.8. skiria darbuotojus, atsakingus už Informacinės sistemos duomenų tvarkymą;

10.9. organizuoja Informacinės sistemos eksploatavimui, priežiūrai ir plėtrai skirtų funkcinių, techninių, programinių priemonių įsigijimą, diegimą ir modernizavimą;

10.10. įgyvendina Informacinės sistemos techninių ir programinių priemonių įsigijimą, įdiegimą ir modernizavimą;

10.11. sudaro sutartis su Informacinės sistemos duomenų teikėjais ir gavėjais;

10.12. registruoja Informacinės sistemos naudotojus, vadovaudamasis Informacinės sistemos naudotojų administravimo taisyklėmis;

10.13. organizacinėmis, techninėmis, technologinėmis ir metodinėmis priemonėmis užtikrina Informacinės sistemos saugą, Informacinėje sistemoje tvarkomų duomenų konfidencialumą, vientisumą ir prieinamumą, apsaugą nuo neteisėto sunaikinimo, pakeitimo, atskleidimo ar kitokio neteisėto tvarkymo bei saugų duomenų perdavimą kompiuteriniais tinklais.

11. Informacinės sistemos duomenų teikėjai ir jų valdomos informacinės sistemos:

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

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

11.3. Greitosios medicinos pagalbos įstaigos, turinčios informacines sistemas, teikia duomenis iš savo informacinių sistemų;

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

11.5. Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos (toliau – Valstybinio socialinio draudimo fondo valdyba) teikia 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. Bendri 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 (toliau – GMP) 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:

13.2.5.1. apsilankymo data, tipas, diagnozės kodas, specialisto spaudo numeris, paslaugos kodas ir kaina.

13.2.6. epizodo metu nustatytos diagnozės ir traumos priežastys, kodai pagal 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. Bendri formos Nr. 106/a, patvirtintos Lietuvos Respublikos sveikatos apsaugos ministro 1999 m. lapkričio 29 d. įsakymu Nr. 515, duomenys:

13.3.1. mirties data, laikas;

13.3.2. mirties vieta;

13.3.3. mirties priežastys.

13.4. Bendri formos Nr. 110/a, patvirtintos Lietuvos Respublikos sveikatos apsaugos ministro 2013 m. gruodžio 20 d. įsakymu Nr. V-1234, duomenys:

13.4.1. kvietimo data;

13.4.2. kvietimo laikas;

13.4.3. GMP atvykimo laikas;

13.4.4. įvykio vietos adresas;

13.4.5. pristatymo į gydymo įstaigą laikas;

13.4.6. informacija apie traumą: sužalojimo vieta, sužalojimai, traumos sunkumo vertinimas, traumos aplinkybės;

13.4.7. informacija apie pacientą: saugos diržai, sėdėjimo vieta, oro pagalvės, saugumo priemonės;

13.4.8. pagalbos teikimo protokolas;

13.4.9. suteikta pagalba;

13.4.10. transportavimas;

13.4.11. vėlavimo į iškvietimą priežastis;
13.4.12. informacija apie mirtį;
13.4.13. ligonio būklė suteikus medicininę pagalbą;
13.4.14. ligonio būklė atvykus į priėmimo-skubios pagalbos skyrių.
13.5. Duomenys apie asmeniui nustatytą neįgalumo ar darbingumo lygį:
13.5.1. asmeniui nustatytas neįgalumo lygis;
13.5.2. neįgalumo lygio nustatymo pradžios data;
13.5.3. neįgalumo lygio nustatymo pabaigos data;
13.5.4. pagrindinė diagnozė;
13.5.5. asmeniui nustatytas darbingumo lygis;
13.5.6. darbingumo lygio nustatymo pradžios data;
13.5.7. darbingumo lygio nustatymo pabaigos data;
13.5.8. pagrindinė diagnozė.
13.6. Bendri Nedarbingumo pažymėjimo duomenys:
13.6.1. laikinojo nedarbingumo data nuo, data iki;
13.6.2. laikinojo nedarbingumo diagnozė;
13.6.3. išmokėta ligos pašalpos suma;
13.6.4. laikinojo nedarbingumo priežastis (nelaimingas atsitikimas buityje, nelaimingas atsitikimas darbe, kelyje į (iš) darbą (-o));
13.6.5. nelaimingas atsitikimas darbe, kelyje į (iš) darbą (-o) pripažintas draudiminiu įvykiu, pripažintas nedraudiminiu įvykiu.
13.7. Klasifikatorių duomenys:
13.7.1. Tarptautinės statistinės ligų ir sveikatos sutrikimų klasifikacijos dešimtasis pataisytas ir papildytas leidimas „Sisteminis ligų sąrašas“ (Australijos modifikacija, TLK-10-AM), įdiegtas 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“ ir jo pakeitimai;
13.7.2. valstybių ir savivaldybių kodų klasifikatorius ir jo pakeitimai;
13.7.3. kiti su sveikatinimo paslaugų teikimu susiję klasifikatoriai.
14. Ataskaitų duomenų bazėje tvarkomi ir saugomi duomenys, kurių reikia ataskaitoms formuoti, statistikai skaičiuoti ir analizei vykdyti.
15. Informacinės sistemos duomenų teikėjai teikia šiuos duomenis:
15.1. GMP teikia šių Nuostatų 13.1.1-13.1.3 ir 13.4.1-13.4.14 papunkčiuose nurodytus duomenis;
15.2. Valstybinė ligonių kasa, vadovaudamasi Privalomojo sveikatos draudimo informacinės sistemos „Sveidra“ nuostatais, pagal duomenų teikimo – gavimo sutartį, teikia Nuostatų 13.1.1-13.1.3, 13.2.1-13.2.11, 13.7.1-13.7.3 papunkčiuose nurodytus duomenis.
15.3. Valstybinio socialinio draudimo fondo valdyba teikia Valstybinio socialinio draudimo fondo valdybos informacinės sistemos duomenis, nurodytus šių Nuostatų 13.1.1-13.1.2 ir 13.6.1-13.6.5 papunkčiuose;
15.4. Neįgalumo ir darbingumo nustatymo tarnyba teikia Neįgalumo ir darbingumo nustatymo tarnybos informacinės sistemos duomenis, nurodytus šių Nuostatų 13.1.1-13.1.2 ir 13.5.1-13.5.8 papunkčiuose;
15.5. 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 Lietuvos Respublikos įstatymuose, Europos Sąjungos teisės aktuose ir (arba) kituose teisės aktuose nustatyta tvarka institucijoms ir kitiems juridiniams ir fiziniams asmenims.

21. 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 teiktinos 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.

22. Informacinės sistemos duomenys Europos Sąjungos valstybių narių ir (arba) Europos ekonominės erdvės valstybių, trečiųjų šalių fiziniams ir juridiniams asmenims, juridinio asmens statuso neturintiems subjektams, jų filialams ir atstovybėms teikiami Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka.

23. Informacija teikiama šiomis formomis:

23.1. raštu, žodžiu ir (arba) elektroniniu ryšiu;

23.2. peržiūra leidžiamosios kreipties būdu internetu.

24. Duomenys duomenų gavėjams teikiami tokio turinio ir tokios formos, kurie tvarkytojo naudojami ir nereikalauja papildomo duomenų apdorojimo.

25. Tais atvejais, kai paprastai teikiamos informacijos turinys ar forma neatitinka prašančios institucijos poreikių arba prašanti institucija neturi techninių galimybių reikiamai apdoroti gaunamų duomenų, taip pat kai paprastai teikiamos informacijos turinys ir forma neatitinka kitų juridinių ar fizinių asmenų, kurie dažniausiai kreipiasi dėl tokios informacijos ir siekia ją pakartotinai panaudoti, poreikių, informaciją teikianti institucija sukuria reikiamas papildomas priemones.

26. Informacinės sistemos duomenys duomenų gavėjams teikiami neatlygintinai.

27. Duomenų gavėjas, registro ar kitos valstybės informacinės sistemos tvarkytojas, duomenų subjektas, kiti asmenys turi teisę reikalauti ištaisyti netikslius duomenis. Gavęs šį reikalavimą, Informacinės sistemos tvarkytojas privalo per 5 darbo dienas nuo reikalavimo ir jame nurodytus faktus patvirtinančių dokumentų gavimo ištaisyti nurodytus netikslumus ir informuoti apie tai reikalavusį asmenį.

28. Informacinės sistemos tvarkytojo – Higienos instituto interneto svetainėje adresu http://www.hi.lt yra viešai skelbiama statistinė informacija apie traumas ir nelaimingus atsitikimus.

VI SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ SAUGA

29. Informacinės sistemos organizacinės ir techninės duomenų saugos priemonės, skirtos Informacinės sistemos duomenų konfidencialumui, prieinamumui ir vientisumui užtikrinti, įgyvendinamos, vadovaujantis 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“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, Lietuvos standartais LST EN ISO / IEC 27002, LST ISO / IEC 27001, taip pat kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, reglamentuojančiais saugų elektroninės informacijos tvarkymą, bei kitais duomenų saugą reglamentuojančiais Lietuvos Respublikos teisės aktais.

Punkto pakeitimai:
Nr. V-551, 2018-05-07, paskelbta TAR 2018-05-08, i. k. 2018-07404

30. Už Informacinės sistemos duomenų saugą teisės aktų nustatyta tvarka pagal kompetenciją atsako Informacinės sistemos valdytojas ir Informacinės sistemos tvarkytojas.

31. Informacinės sistemos duomenys kaupiami ir saugomi Informacinės sistemos duomenų saugykloje neterminuotai. Informacinės 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.

32. Tvarkant ir saugant Informacinėje sistemoje kaupiamus duomenis turi būti įgyvendintos duomenų saugos organizacinės, programinės, techninės, patalpų apsaugos ir administracinės priemonės, skirtos Informacinės sistemos duomenų konfidencialumui, prieinamumui teisėtiems Informacinės sistemos tvarkytojams, vientisumui ir autentiškumui užtikrinti ir apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, naudojimo, atskleidimo, taip pat bet kokio kito neteisėto tvarkymo. Minėtos priemonės turi užtikrinti tokio lygio saugumą, kuris atitiktų saugotinų Informacinėje sistemoje tvarkomų duomenų pobūdį.

VII SKYRIUS
FINANSAVIMAS

33. Informacinės sistemos kūrimas, eksploatacija, palaikymas ir plėtra finansuojama Lietuvos Respublikos valstybės biudžeto lėšomis.

VIII SKYRIUS
INFORMACINĖS SISTEMOS MODERNIZAVIMAS IR LIKVIDAVIMAS

34. Informacinė sistema modernizuojama arba likviduojama Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo ir Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo nustatyta tvarka.

35. Likviduojamos Informacinės sistemos duomenys perduodami kitai informacinei sistemai,

sunaikinami arba perduodami valstybės archyvams Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

_____

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos
ministro 2014 m. liepos 9 d.
įsakymu Nr. V-776
(Lietuvos Respublikos sveikatos apsaugos
ministro 2018 m. gegužės 7 d.
įsakymo Nr. V-551
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 Lietuvos Respublikos sveikatos apsaugos ministerijos valdomos ir Higienos instituto tvarkomos Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos (toliau – Informacinė sistema) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika).

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

3. Saugos nuostatuose vartojamos sąvokos apibrėžtos 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 saugos reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei struktūrai ir valstybės informaciniams ištekliams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei struktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas), Lietuvos Respublikos „Informacijos technologija. Saugumo metodai“ grupės standartuose.

4. Informacinės sistemos elektroninės informacijos sauga – tai elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

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

5.1. automatiniu būdu tvarkomos elektroninės informacijos saugumo užtikrinimas;

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

5.3. elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai) prevencijos vykdymas.

6. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

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

6.2. elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

6.3. Informacinės sistemos veiklos tęstinumo užtikrinimas.

7. Elektroninės informacijos saugai užtikrinti kompleksiškai naudojamos organizacinės, techninės ir programinės priemonės.

8. Saugos nuostatų reikalavimai yra taikomi:

8.1. Informacinės sistemos valdytojai – Lietuvos Respublikos sveikatos apsaugos ministerijai, Vilnius, Vilniaus g. 33;

8.2. Informacinės sistemos tvarkytojui – Higienos institutui, Vilnius, Didžioji g. 22;

8.3. Informacinės sistemos tvarkytojo paskirtam saugos įgaliotiniui;

8.4. Informacinės sistemos tvarkytojo paskirtam administratoriui;

8.5. Informacinės sistemos kibernetinio saugumo vadovui;

8.6. Informacinės sistemos naudotojams.

9. Informacinės sistemos valdytojo funkcijos:

9.1. pagal kompetenciją atsako už elektroninės informacijos saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą;

9.2. tvirtina Informacinės sistemos saugos nuostatus, saugos politiką įgyvendinančius dokumentus (toliau visi kartu – Saugos dokumentai) ir kitus teisės aktus, susijusius su Informacinės sistemos sauga;

9.3. priima sprendimus dėl Informacinės sistemos techninių ir programinių priemonių, būtinų Informacinės sistemos elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

9.4. nagrinėja Informacinės sistemos tvarkytojo pasiūlymus dėl Informacinės sistemos elektroninės informacijos saugos priemonių tobulinimo ir priima dėl jų sprendimus;

9.5. koordinuoja Informacinės sistemos tvarkytojo veiklą įgyvendinant elektroninės informacijos saugos reikalavimus;

9.6. vykdo kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Informacinės sistemos nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

10. Informacinės sistemos tvarkytojo funkcijos:

10.1. pagal kompetenciją atsako už Informacinės sistemos elektroninės informacijos tvarkymo teisėtumą ir saugą;

10.2. 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;

10.3. teikia pasiūlymus Informacinės sistemos valdytojui dėl Informacinės sistemos elektroninės informacijos saugos tobulinimo, Informacinės sistemos saugos dokumentų priėmimo, keitimo arba panaikinimo, taip pat rengia Informacinės sistemos saugos dokumentų projektus;

10.4. teikia pasiūlymus Informacinės sistemos valdytojui dėl Informacinės sistemos techninių ir programinių priemonių, būtinų Informacinės sistemos elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo, organizuoja jų įdiegimą ir modernizavimą;

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

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

10.7 Informacinės sistemos valdytojo vadovo pavedimu skiria duomenų valdymo įgaliotinį, saugos įgaliotinį, administratorių;

10.8. užtikrina, kad Informacinės sistemos naudotojai, turintys teisę naudotis Informacinės sistemos elektronine informacija, laikytųsi reikalavimų, nustatytų Informacinės sistemos saugos dokumentuose;

10.9. vykdo kibernetinio saugumo organizavimo ir užtikrinimo funkcijas, nustatytas Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose;

10.10. vykdo kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše,

Informacinės sistemos nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

11. Informacinės sistemos saugos įgaliotinio funkcijos:

11.1. atsako už tinkamą Informacinės sistemos elektroninės informacijos saugos priemonių įgyvendinimą;

11.2. teikia Informacinės sistemos tvarkytojo vadovui pasiūlymus dėl:

11.2.1. keliamų reikalavimų Informacinės sistemos administratoriui nustatymo;

11.2.2. elektroninės informacijos saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

11.2.3. Informacinės sistemos informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

11.3. teikia Informacinės sistemos valdytojo vadovui pasiūlymus dėl saugos dokumentų priėmimo, keitimo;

11.4. organizuoja Informacinės sistemos rizikos vertinimą (prireikus ir neeilinius rizikos vertinimus) ir parengia rizikos įvertinimo ataskaitą;

11.5. pagal kompetenciją teikia Informacinės sistemos administratoriui ir naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Informacinės sistemos elektroninės informacijos saugos politikos įgyvendinimu;

11.6. supažindina Informacinės sistemos naudotojus su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais bei atsakomybe už šių reikalavimų nesilaikymą;

11.7. atsako už Informacinės sistemos saugos dokumentų reikalavimų vykdymą;

11.8. periodiškai organizuoja naudotojų mokymą elektroninės informacijos saugos klausimais, reguliariai primena saugos problemas, teikia konsultacijas ir rekomendacijas (elektroniniu paštu, telefonu ir kitais būdais), prireikus parengia atmintines naudotojams;

11.9. koordinuoja elektroninės informacijos saugos incidentų, įvykusių Informacinėje sistemoje, tyrimą;

11.10. vykdo kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, Informacinės sistemos nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

12. Informacinės sistemos administratorius vykdo šias funkcijas:

12.1. atsako už Informacinės sistemos funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugų administravimą;

12.2. pagal kompetenciją rengia pasiūlymus dėl Informacinės sistemos kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir duomenų saugos užtikrinimo ir juos teikia Informacinės sistemos tvarkytojo vadovui;

12.3. registruoja Informacinės sistemos naudotojus ir suteikia prieigos teisę naudotis Informacinės sistemos infrastruktūra paskirtoms funkcijoms atlikti;

12.4. atlieka Informacinės sistemos sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, elektroninės informacijos perdavimo tinklais, bylų serveriais ir kitais) ir šių informacinės sistemos komponentų sąrankos administravimą, pažeidžiamų vietų nustatymą ir saugumo reikalavimų atitikties nustatymą ir stebėseną, reaguoja į elektroninės informacijos saugos incidentus, taip pat privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus, susijusius su Informacinės sistemos saugos užtikrinimu, ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę bei atsako už jų atitiktį Informacinės sistemos saugos politiką įgyvendinančių dokumentų reikalavimams;

12.5. daro atsargines Informacinės sistemos duomenų kopijas, tikrina šių kopijų atkūrimą;

12.6. dalyvauja atliekant Informacinės sistemos rizikos vertinimą ir Informacinės sistemos informacinių technologijų saugos atitikties vertinimą;

12.7. vykdo kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše,

Informacinės sistemos nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

13. Informacinės sistemos kibernetinio saugumo vadovas vykdo kibernetinio saugumo organizavimo ir užtikrinimo funkcijas, nustatytas Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose.

14. Informacinės sistemos naudotojai, vadovaudamiesi saugos politiką įgyvendinančiais dokumentais, pareigybių aprašymais ir kitais teisės aktais, naudojasi Informacinės sistemos elektronine informacija tvarkymo arba kitais su tiesioginių funkcijų vykdymu susijusiais tikslais.

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

15.1. Valstybės informacinių išteklių valdymo įstatymas;

15.2. Kibernetinio saugumo įstatymas;

15.3. Bendrųjų saugos reikalavimų aprašas;

15.4. Kibernetinio saugumo reikalavimų aprašas;

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

15.6. Informacinės sistemos nuostatai;

15.7. Lietuvos standartai LST EN ISO / IEC 27002 ir LST EN ISO / IEC 27001 bei Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, reglamentuojantys saugų elektroninės informacijos tvarkymą;

15.8. kiti teisės aktai, reglamentuojantys elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

16. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių 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“ (toliau – Elektroninės informacijos svarbos nustatymo gairių aprašas), 9.1 ir 9.2 papunkčiais, Informacinėje sistemoje tvarkoma elektroninė informacija priskiriama prie vidutinės svarbos informacijos kategorijos.

17. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 12.3 papunkčiu, Informacinė sistema priskiriama prie trečiosios kategorijos informacinių sistemų – Informacinėje sistemoje tvarkoma vidutinės svarbos informacija.

18. Informacinės sistemos saugos priemonės parenkamos įvertinus galimus rizikos veiksnius elektroninės informacijos vientisumui, konfidencialumui ir prieinamumui.

19. Informacinės sistemos kaupiamų ir apdorojamų duomenų rinkimo tvarka, kriterijai bei sąrašas pateikiami Informacinės sistemos nuostatuose.

20. Informacinės sistemos saugos įgaliotinis, vadovaudamasis Lietuvos Respublikos vidaus reikalų ministerijos metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, kasmet organizuoja Informacinės sistemos rizikos vertinimą. Prireikus Informacinės sistemos saugos įgaliotinis gali organizuoti neeilinį Informacinės sistemos rizikos vertinimą. Informacinės sistemos saugos įgaliotinį paskyrusio tvarkytojo vadovo rašytiniu pavedimu Informacinės sistemos rizikos vertinimą gali atlikti pats Informacinės sistemos saugos įgaliotinis.

21. Informacinės sistemos rizikos vertinimui atlikti naudojama Valstybės informacinių

išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistema (toliau – ARSIS).

22. Informacinės sistemos rizikos vertinimo informacija pateikiama ataskaitoje. Informacinės sistemos rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos Informacinės sistemos informacijos saugai. Svarbiausi rizikos veiksniai:

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

22.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

22.3. 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.

23. Prireikus, Informacinės sistemos tvarkytojo vadovas, atsižvelgdamas į Informacinės sistemos rizikos įvertinimo ataskaitą, tvirtina Informacinės sistemos saugos įgaliotinio parengtą rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti, nurodomi atsakingi vykdytojai, priemonių įgyvendinimo terminai.

24. Siekiant įvertinti Informacinės sistemos saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę kartą per metus organizuojamas Informacinės sistemos informacinių technologijų saugos atitikties vertinimas.

25. Atlikus Informacinės sistemos informacinių technologijų saugos atitikties vertinimą, rengiama Informacinės sistemos informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Informacinės sistemos tvarkytojo vadovui.

26. Atsižvelgdamas į Informacinės sistemos informacinių technologijų saugos atitikties vertinimo ataskaitą, Informacinės sistemos saugos įgaliotinis prireikus parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Informacinės sistemos tvarkytojas.

27. Informacinės sistemos grėsmių ir pažeidžiamumų, galinčių turėti įtakos Informacinės sistemos saugumui, vertinimas atliekamas kartu su Informacinės sistemos rizikos ir / arba Informacinės sistemos informacinių technologijų saugos atitikties vertinimu. Informacinės sistemos rizikos ir / arba informacinių technologijų saugos atitikties vertinimo metu gali būti atliekamas pažeidžiamumų testavimas imituojant kibernetines atakas bei vykdant kibernetinių incidentų imitavimo pratybas. Imituojant kibernetines atakas rekomenduojama vadovautis tarptautiniu mastu pripažintų organizacijų (pavyzdžiui, EC-COUNCIL, ISACA, NIST ir kt.) rekomendacijomis ir gerąja praktika.

28. Informacinės sistemos rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano, Informacinės sistemos informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas Informacinės sistemos valdytojas arba jos įgaliotas Informacinės sistemos tvarkytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti ARSIS Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2012 m. spalio 16 d. įsakymu Nr. 1V-740 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

29. Elektroninės informacijos saugos būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis Informacinės sistemos elektroninės informacijos saugos priemonėmis, kurios pasirenkamos atsižvelgiant į Informacinės sistemos valdytojo skiriamus išteklius, vadovaujantis šiais principais:

29.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

29.2. elektroninės informacijos saugos priemonės diegimo kaina turi atitikti saugomos elektroninės informacijos vertę;

29.3. esant galimybei, turi būti įdiegtos prevencinės elektroninės informacijos saugos priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

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

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

30.3. apsaugai naudojama programinė įranga privalo automatiškai elektroniniu paštu informuoti Informacinės sistemos administratorių apie kompiuterizuotas darbo vietas ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 24 valandas;

30.4. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

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

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

31.2. programinės įrangos priežiūrą ir gedimų šalinimą atlieka tik Informacinės sistemos administratorius arba kitas Informacinės sistemos tvarkytojo įgaliotas asmuo;

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

31.4. Informacinės sistemos neveikimo laikotarpis negali būti ilgesnis nei 16 valandų. Per šį laikotarpį turi būti užtikrintas Informacinės sistemos veiklos atnaujinimas.

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

32.1. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

32.2. Informacinės sistemos programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. SQL injection), XSS (angl. Cross-site scripting), atkirtimo nuo paslaugos (angl. DOS), dedikuoto atkirtimo nuo paslaugos (angl. DDOS);

32.3. 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;

32.4. 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.

33. Leistinos kompiuterių naudojimo ribos:

33.1. Informacinės sistemos naudotojų kompiuteriai privalo būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi Informacinės sistemos duomenys ir Informacinės sistemos informacija;

33.2. Informacinės sistemos duomenų naudotojai privalo naudotis visomis saugumo priemonėmis, siekiant apsaugoti kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

34. Nešiojamuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose Informacinės sistemos programinė įranga nėra diegiama.

35. Metodai, kuriais užtikrinamas saugus Informacinės sistemos elektroninės informacijos

teikimas ir (ar) gavimas:

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

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

35.3. prieiga prie Informacinės sistemos elektroninės informacijos suteikiama tik naudotojui patvirtinus savo tapatybę (įvedus Informacinės sistemos naudotojo vardą ir slaptažodį). Prieigos prie Informacinės sistemos elektroninės informacijos valdymas apibrėžtas Informacinės sistemos naudotojų administravimo taisyklėse;

35.4. įstatymų numatytais atvejais nušalinus Informacinės sistemos naudotoją ar Informacinės sistemos administratorių nuo darbo, neatitinkant kituose teisės aktuose nustatytų Informacinės sistemos naudotojui ir Informacinės sistemos administratoriui keliamų kvalifikacinių reikalavimų, taip pat pasibaigus jų darbo santykiams, praradus patikimumą, Informacinės sistemos naudotojo ar Informacinės sistemos administratoriaus teisė naudotis Informacine sistema turi būti panaikinta.

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

36.1. atsarginės elektroninės informacijos kopijos (toliau – kopijos) daromos automatiškai;

36.2. kopijas turi teisę tvarkyti Informacinės sistemos administratorius;

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

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

37. 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:

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

37.2. Nacionalinio kibernetinio saugumo centrui prie Krašto apsaugos ministerijos ir kitoms atsakingoms institucijoms pagal kompetenciją pranešama apie įvykusius saugos incidentus, jų vertinimą ir suvaldymą.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

38. Informacinės sistemos saugos įgaliotinis ir Informacinės sistemos kibernetinio saugumo vadovas privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos srityje, savo darbe vadovautis Informacinės sistemos saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą. Informacinės sistemos saugos įgaliotinis ar Informacinės sistemos kibernetinio saugumo vadovas pažeidęs Saugos nuostatų ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

39. Informacinės sistemos administratorius privalo išmanyti darbą su duomenų perdavimo tinklais, mokėti užtikrinti jų saugą, administruoti ir prižiūrėti duomenų bazes, turi būti susipažinęs su Informacinės sistemos nuostatais, Informacinės sistemos 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.

40. Informacinės sistemos saugos įgaliotiniu, Informacinės sistemos kibernetinio saugumo vadovu, Informacinės sistemos administratoriumi negali būti skiriamas asmuo, turintis neišnykusį

ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

41. Informacinės sistemos naudotojai privalo turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti Informacinės sistemos duomenis Informacinės sistemos nuostatų nustatyta tvarka, būti susipažinę su Informacinės sistemos saugos dokumentais ir pasirašę pasižadėjimus saugoti konfidencialią elektroninę informaciją (toliau – Pasižadėjimas). Informacinės sistemos naudotojai, pažeidę Informacinės sistemos saugos dokumentų reikalavimus ar kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

42. Informacinės sistemos saugos įgaliotinio, Informacinės sistemos kibernetinio saugumo vadovo, Informacinės sistemos naudotojų ir Informacinės sistemos administratoriaus mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

42.1. Informacinės sistemos saugos įgaliotiniui, Informacinės sistemos kibernetinio saugumo vadovui, Informacinės sistemos naudotojams ir Informacinės sistemos administratoriui turi būti organizuojami mokymai elektroninės informacijos saugos klausimais;

42.2. Informacinės sistemos naudotojams turi būti įvairiais būdais (pavyzdžiui, priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems Informacinės sistemos naudotojams ir Informacinės sistemos administratoriui ir panašiai) primenama apie elektroninės informacijos saugos problemas;

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

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

42.5. Informacinės sistemos naudotojų ir Informacinės sistemos administratoriaus mokymus gali vykdyti Informacinės sistemos saugos įgaliotinis ar kitas Informacinės sistemos valdytojo ar Informacinės sistemos tvarkytojo darbuotojas, išmanantis elektroninės informacijos saugos užtikrinimo principus, arba elektroninės informacijos saugos mokymų paslaugų teikėjas. Informacinės sistemos saugos įgaliotinio ir Informacinės sistemos kibernetinio saugumo vadovo mokymus gali vykdyti tik aukštos kvalifikacijos elektroninės informacijos saugos mokymų paslaugų teikėjas;

42.6. Informacinės sistemos naudotojų mokymai turi būti organizuojami periodiškai, ne rečiau kaip kartą per dvejus metus. Informacinės sistemos saugos įgaliotinio, Informacinės sistemos kibernetinio saugumo vadovo ir Informacinės sistemos administratoriaus mokymai turi būti organizuojami pagal poreikį. Už mokymų organizavimą atsakingas Informacinės sistemos saugos įgaliotinis ar kitas Informacinės sistemos tvarkytojo paskirtas darbuotojas.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

43. Tvarkyti Informacinės sistemos elektroninę informaciją gali tik įgalioti Informacinės sistemos naudotojai, susipažinę su Informacinės sistemos saugos dokumentais ir pasirašę Pasižadėjimus.

44. Už Informacinės sistemos naudotojų supažindinimą su Informacinės sistemos saugos dokumentais ir kitais saugos politiką įgyvendinančiais teisės aktais bei Pasižadėjimų registravimą

yra atsakingas Informacinės sistemos saugos įgaliotinis. Pakartotinai su Informacinės sistemos saugos dokumentais Informacinės sistemos naudotojai supažindinami tik iš esmės jiems pasikeitus.

45. Saugos nuostatai skelbiami Informacinės sistemos tvarkytojo interneto svetainėje.

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

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