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

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

SUDERINTA
Valstybinės ligonių kasos prie
Sveikatos apsaugos ministerijos

2014 m. birželio 5 d. raštu Nr. S-807

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

2014 m. birželio 9 d. raštu Nr. 4K-4767

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 sveikatos apsaugos ministro 2011 m. kovo 28 d. įsakymas Nr. V-294 „Dėl Lietuvos E. sveikatos sistemos funkcinės, techninės ir programinės įrangos modelio patvirtinimo“;

3.8. Lietuvos Respublikos Vyriausybės 2011 m. rugsėjo 7 d. nutarimas Nr. 1057 „Dėl Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos nuostatų patvirtinimo“;

3.9 Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimas Nr. 180 „Dėl valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“;

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

3.11. kiti teisės aktai, reglamentuojantys saugų elektroninės informacijos tvarkymą, saugojimą bei sunaikinimą.

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 duomenų saugą nustato Informacinės sistemos duomenų saugos nuostatai ir kiti saugos politiką įgyvendinantys dokumentai, kurie rengiami, derinami ir tvirtinami Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ nustatyta tvarka.

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

TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos duomenų saugos nuostatų (toliau – Saugos nuostatai) tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos (toliau – Informacinė sistema) duomenis.

2. Saugos nuostatai apibrėžia Informacinės sistemos saugos politiką, kuri įgyvendinama Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėmis, Informacinės sistemos veiklos tęstinumo valdymo planu ir Informacinės sistemos naudotojų administravimo taisyklėmis (toliau – saugos politiką įgyvendinantys dokumentai). Saugos nuostatai ir saugos politiką įgyvendinantys dokumentai kartu vadinami saugos dokumentais.

3. Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarime Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180, kituose teisės aktuose bei Lietuvos Respublikos standartuose LST ISO/IEC 27002:2009 ir LST ISO/IEC 27001:2006.

4. Informacinės sistemos duomenų saugos tikslai:

4.1. informacijos patikimumo, vientisumo, konfidencialumo, prieinamumo ir saugumo užtikrinimas;

4.2. kompiuterizuotų darbo vietų tinkamo saugumo lygio įdiegimas ir palaikymas;

4.3. nuolatinis vietinio kompiuterių tinklo funkcionavimo užtikrinimas bei saugumo stebėsena;

4.4. tinkamo kompiuterinės, programinės ir tinklo įrangos funkcionavimo ir saugumo užtikrinimas.

5. Informacinės sistemos duomenų saugai užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo, atsakomybės, elektroninės informacijos saugos lygio kėlimo, saugos priemonių projektavimo ir diegimo principus.

6. Informacijos saugumo užtikrinimo prioritetinės kryptys:

6.1. Informacinės sistemos perduodamų duomenų konfidencialumo užtikrinimas;

6.2. Informacinės sistemos perduodamų duomenų vientisumo užtikrinimas;

6.3. Informacinės sistemos duomenų prieinamumo užtikrinimas;

6.4. Informacinės sistemos veiklos tęstinumo užtikrinimas.

7. Informacinės sistemos valdytoja yra Lietuvos Respublikos sveikatos apsaugos ministerija (adresas: Vilniaus g. 33, LT-01506, Vilnius).

8. Informacinės sistemos tvarkytojas yra Higienos institutas (adresas: Didžioji g. 22, Vilnius, LT-01128).

9. Saugos nuostatų reikalavimai taikomi Informacinės sistemos valdytojui, Informacinės

sistemos tvarkytojui, Informacinės sistemos saugos įgaliotiniams, Informacinės sistemos administratoriams ir Informacinės sistemos naudotojams.

10. Informacinės sistemos valdytojo vadovas vykdo šias funkcijas:

10.1. organizuoja Informacinės sistemos veiklą ir jai vadovauja;

10.2. tvirtina dokumentus, susijusius su Informacinės sistemos sauga;

10.3. priima sprendimą dėl Informacinės sistemos informacinių technologijų atitikties Saugos reikalavimams vertinimo atlikimo;

10.4. pagal kompetenciją rengia ir tvirtina dokumentus, susijusius su Informacinės sistemos tvarkymu ir duomenų sauga, ir prižiūri, kaip jų laikomasi;

10.5. atsako už informacijos tvarkymo Informacinėje sistemoje teisėtumą ir duomenų saugą.

11. Informacinės sistemos tvarkytojo vadovas vykdo šias funkcijas:

11.1. teikia siūlymus Informacinės sistemos valdytojai dėl Informacinės sistemos eksploatavimui, priežiūrai ir plėtrai skirtų techninių, programinių priemonių įsigijimo, organizuoja jų įdiegimą ir modernizavimą, pagal kompetenciją atlieka Informacinės sistemos techninės, programinės įrangos priežiūros ir tobulinimo darbus;

11.2. užtikrina Informacinės sistemos sąveiką su kitomis informacinėmis sistemomis;

11.3. užtikrina duomenų bazių techninę priežiūrą ir užtikrina nepertraukiamą Informacinės sistemos veikimą;

11.4. pavedus valdytojui skiria Informacinės sistemos saugos įgaliotinį ir paveda jam organizuoti ir kontroliuoti saugos dokumentų įgyvendinimą Informacinėje sistemoje;

11.5. pavedus valdytojui skiria Informacinės sistemos duomenų valdymo įgaliotinį;

11.6. pavedus valdytojui skiria Informacinės sistemos administratorių ir paveda jam užtikrinti Informacinės sistemos kompiuterinės įrangos ir Informacinės sistemos naudotojų kompiuterizuotų darbo vietų saugų funkcionavimą, administruoti Informacinės sistemos duomenų bazę saugos dokumentų ir kitų teisės aktų nustatyta tvarka;

11.7. Informacinės sistemos tvarkytojo ir Informacinės sistemos duomenų gavėjų sutarčių dėl duomenų teikimo nustatyta tvarka automatiškai teikia Informacinės sistemos duomenis duomenų gavėjams bei užtikrina duomenų saugą iki duomenys pasiekia duomenų gavėją sutartyse numatytomis sąlygomis ir tvarka;

11.8. užtikrina Informacinėje sistemoje tvarkomų duomenų saugą;

11.9. užtikrina Informacinės sistemos naudotojų darbo vietose naudojamų administracinių, techninių ir programinių priemonių, užtikrinančių duomenų saugą, diegimą ir priežiūrą;

11.10. atlieka kitas Saugos nuostatų, Saugos reikalavimų, Informacinės sistemos nuostatų ir kitų teisės aktų nustatytas funkcijas.

12. Informacinės sistemos saugos įgaliotinis, įgyvendindamas elektroninės informacijos saugą Informacinėje sistemoje, vykdo šias funkcijas:

12.1. teikia Informacinės sistemos tvarkytojo vadovui pasiūlymus dėl:

12.1.1. Informacinės sistemos administratoriaus skyrimo ir reikalavimų administratoriui nustatymo;

12.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

12.1.3. Informacinės sistemos informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo.

12.2. teikia informacinės sistemos valdytojo vadovui pasiūlymus dėl saugos dokumentų priėmimo, keitimo;

12.3. įgyvendina Informacinės sistemos duomenų saugą, vadovaudamasis Saugos reikalavimais;

12.4. organizuoja elektroninės informacijos saugos incidentų Informacinės sistemos tyrimą;

12.5. pagal kompetenciją teikia Informacinės sistemos administratoriui privalomus vykdyti nurodymus ir pavedimus;

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

12.7. atsako už Informacinės sistemos saugos dokumentų reikalavimų vykdymą;

12.8. periodiškai organizuoja Informacinės sistemos naudotojų mokymą elektroninės saugos

klausimais, reguliariai jiems primena saugos problemas (elektroniniu paštu, parengia atmintines naujai priimtiems darbuotojams ir pan.);

12.9. koordinuoja elektroninės informacijos saugos incidentų, įvykusių informacinėje sistemoje, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

12.10. kasmet organizuoja visų informacinių sistemų rizikos įvertinimą;

12.11. atlieka kitas Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

13. Informacinės sistemos administratorius vykdo šias funkcijas:

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

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

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

13.4. atlieka Informacinės sistemos sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, elektroninės informacijos perdavimu 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.

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

15. Teisės aktai, kuriais vadovaujamasi tvarkant Informacinę sistemą, joje tvarkomus duomenis ir užtikrinant jų saugumą:

15.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

15.2. Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimas Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“;

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

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

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

15.6. Lietuvos standartai LST ISO/IEC 27002:2009, LST ISO/ IEC 27001:2006 bei kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys informacijos saugumą;

15.7. Saugos nuostatai ir kiti teisės aktai, reglamentuojantys elektroninės informacijos saugą valstybės institucijose.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

16. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, 4.3 papunkčiu, Informacinėje sistemoje tvarkoma elektroninė informacija priskiriama žinybinės svarbos elektroninės informacijos kategorijai. Elektroninės informacijos priskyrimo žinybinės svarbos kategorijai kriterijai:

16.1. gali padaryti žalą vieno ar kelių fizinių ar juridinių asmenų teisėtiems interesams;

16.2. gali turėti neigiamų padarinių institucijos veiklai;

16.3. gali sukelti kitų neigiamų padarinių institucijai.

17. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.3 papunkčiu, Informacinė sistema priskiriama trečiosios kategorijos informacinėms sistemoms – Informacinėje sistemoje tvarkoma žinybinės svarbos elektroninė informacija.

18. Informacinės sistemos saugos priemonės parenkamos įvertinus galimus rizikos veiksnius Informacinės sistemos duomenų 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, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, kasmet organizuoja Informacinės sistemos rizikos vertinimą. Prireikus Informacinės sistemos saugos įgaliotinis gali organizuoti neeilinį Informacinės sistemos rizikos vertinimą. Informacinės sistemos saugos įgaliotinį paskyrusio valdytojo vadovo rašytiniu pavedimu Informacinės sistemos rizikos vertinimą gali atlikti pats Informacinės sistemos saugos įgaliotinis.

21. Informacinės sistemos rizikos vertinimo metu atliekamos šios veiklos:

21.1. Informacinę sistemą sudarančių išteklių inventorizacija;

21.2. rizikos veiksnių įtakos Informacinei sistemai vertinimas;

21.3. liekamosios rizikos vertinimas.

22. Informacinės sistemos rizikos įvertinimo 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 (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, fiziniai informacijos technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

22.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis Informacinės sistemos duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

22.3. nenugalima jėga (*force majeure*).

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

24. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

24.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

24.2. informacijos saugos priemonės diegimo kainos adekvatumas saugomos informacijos vertei;

24.3. turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

25. Siekiant užtikrinti Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, Informacinių technologijų saugos atitikties vertinimo metodikos nustatyta tvarka Informacinės sistemos saugos įgaliotinis kasmet, iki gruodžio 30 d., organizuoja Informacinės sistemos informacinių technologijų saugos reikalavimų atitikties vertinimą, kurio metu:

25.1. įvertinama informacijos saugos atitiktis saugos dokumentams;

25.2. inventorizuojama Informacinės sistemos techninė ir programinė įranga;

25.3. patikrinama ne mažiau kaip 10 proc. atsitiktinai parinktų Informacinės sistemos naudotojų kompiuterizuotų darbo vietų, Informacinės sistemos tarnybinėse stotyse įdiegtos programos ir jų sąranka;

25.4. patikrinama (įvertinama) Informacinės sistemos naudotojams suteiktų teisių atitiktis jų vykdomoms funkcijoms;

25.5. įvertinamas pasirengimas užtikrinti Informacinės sistemos veiklos tęstinumą įvykus elektroninės informacijos saugos incidentui.

26. Atlikus Informacinės sistemos informacinių technologijų saugos reikalavimų atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus Informacinės sistemos valdytojo vadovas.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

27. Prieigos prie Informacinės sistemos užtikrinimo metodai ir priemonės:

27.1. teisė dirbti su konkrečia elektronine informacija suteikiama konkrečiam Informacinės sistemos naudotojui;

27.2. pasibaigus darbo santykiams, Informacinės sistemos naudotojo teisė naudotis Informacinės sistemos duomenimis turi būti panaikinta, Informacinės sistemos naudotojo veiklos tyrimo metu teisė dirbti su konkrečia elektronine informacija turi būti ribojama ar sustabdoma;

27.3. ribojama Informacinės sistemos naudotojo teisė manipuliuoti duomenimis.

28. Informacinės sistemos naudotojų darbo vietose veikia programinė įranga, skirta kovai su kenksminga programine įranga, automatiškai atnaujinama ne rečiau kaip kas 7 paras.

29. Programinės įrangos, ribojančios programinės įrangos, nesusijusios su Informacinės sistemos veikla ar Informacinės sistemos naudotojų funkcijomis, naudojimo reikalavimai:

29.1. Informacinės sistemos naudotojams leidžiama naudoti tik legalią programinę įrangą;

29.2. periodiškai, ne rečiau kaip kartą per 6 mėnesius, turi būti tikrinama, ar nenaudojama nelegali programinė įranga; rasta nelegali programinė įranga turi būti nedelsiant pašalinta;

29.3. tarnybinėse stotyse, Informacinės sistemos naudotojų kompiuteriuose privalo būti naudojama reguliariai ne rečiau kaip kartą per parą automatiškai atnaujinama programinė įranga, skirta apsaugai nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.).

30. Informacinės sistemos objektų duomenims saugiai rinkti, apdoroti, kaupti, saugoti, naikinti ir teikti Informacinėje sistemoje turi būti taikomos šios programinės ir techninės įrangos naudojimą ribojančios pagrindinės priemonės:

30.1. Informacinės sistemos naudotojams prieiga prie Informacinės sistemos duomenų suteikiama tik užsiregistravus (įvedus Informacinės sistemos naudotojo vardą ir slaptažodį) arba naudojant elektroninio parašo kvalifikuotą sertifikatą. Informacinės sistemos administratorius (-iai) savo tapatybę turi patvirtinti slaptažodžiu, kuriam keliami aukštesni (nei Informacinės sistemos naudotojų slaptažodžiams) reikalavimai arba naudojant elektroninio parašo kvalifikuotą sertifikatą;

30.2. Informacinės sistemos naudotojų prieigos valdymas apibrėžtas Informacinės sistemos naudotojų administravimo taisyklėse;

30.3. Informacinės sistemos naudotojas, baigęs darbą, turi imtis priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungti nuo Informacinės sistemos, įjungti ekrano užsklandą su slaptažodžiu, dokumentus padėti į pašaliniams asmenims neprieinamą vietą;

30.4. naudojamos ugniasienės;

30.5. tarnybinėse stotyse ir darbo vietose naudojama antivirusinė programinė įranga, turinti realaus laiko apsaugą ir nuolat (kartą per parą) automatiškai atsinaujinanti;

30.6. programinėmis priemonėmis registruojamos Informacinėje sistemoje esančios informacijos užklausos, pakeitimai, juos atlikusio Informacinės sistemos naudotojo tapatybė ir pakeitimų atlikimo laikas.

31. Pagrindiniai atsarginių kopijų darymo ir atkūrimo reikalavimai:

31.1. duomenų saugai užtikrinti daromos pagrindinės duomenų bazės atsarginės duomenų kopijos;

31.2. atsarginės kopijos diskinėse laikmenose daromos reguliariai, kiekvieną darbo dieną;

31.3. sukurtai atsarginei kopijai nurodoma kopijavimo data;

31.4. kiekvienos savaitės paskutinei atsarginei kopijai papildomai nurodoma, kad tai yra savaitinė kopija;

31.5. kiekvieno mėnesio paskutinei atsarginei kopijai papildomai nurodoma, kad tai yra mėnesinė kopija;

31.6. kiekvienų metų paskutinei atsarginei kopijai papildomai nurodoma, kad tai yra metinė kopija;

31.7. atsargines dokumentų kopijas turi teisę daryti tik Informacinės sistemos administratorius (-iai), kurio (-ių) pareigybės aprašyme numatyta ši funkcija;

31.8. darant (padarius) atsargines kopijas, būtina užtikrinti kopijų kokybę;

31.9. atsarginės kopijos saugomos specializuotos tarnybinės stoties diskinėse laikmenose;

31.10. atsarginės metinės kopijos saugomos 10 metų nuo jų sukūrimo dienos. Atsarginės mėnesinės kopijos saugomos 1 metus nuo jų sukūrimo dienos;

31.11. Informacinės sistemos duomenų atsarginės kopijos turi būti daromos automatiškai. Jas atkurti turi teisę tik Informacinės sistemos administratorius;

31.12. periodiškai (ne rečiau 1 kartą per metus) atliekami elektroninės informacijos atkūrimo iš Informacinės sistemos duomenų atsarginių kopijų bandymai;

31.13. kopijų, iš kurių būtų galima atkurti Informacinės sistemos duomenis, darymo ir saugojimo tvarka turi būti detaliai aprašyta Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

32. Nešiojamuose kompiuteriuose Informacinės sistemos programinė įranga nebus diegiama ir duomenys lokaliai nebus saugomi, o Informacine sistema bus naudojamasi per interneto naršyklę.

33. Apsauga nuo galimų tyčinių Informacinės sistemos naudotojų veiksmų:

33.1. nustatomi Informacinės sistemos naudotojų vaidmenys ir jiems priskiriami konkretūs leidžiami atlikti veiksmai;

33.2. ribojama Informacinės sistemos naudotojo teisė manipuliuoti duomenimis;

33.3. Informacinės sistemos naudotojo teisės suteikiamos ir sustabdomos įstaigos, kurioje dirba naudotojas, vadovo prašymu;

33.4. visi Informacinės sistemos naudotojo prisijungimai prie Informacinės sistemos registruojami Informacinės sistemos prisijungimų žurnale ir saugomi 3 metus;

33.5. visi pakeitimai duomenų bazėje yra registruojami elektroniniame žurnale;

33.6. įdiegiama programinė įranga, registruojanti į atskirą žurnalą sistemoje Informacinės sistemos administratoriaus atliekamus veiksmus duomenų bazėje.

34. Informacinės sistemos programiniai kodai privalo būti apsaugoti nuo atskleidimo neturintiems teisės su jais susipažinti asmenims.

35. Informacinės sistemos telekomunikacinio tinklo apsaugos priemonės:

35.1. tinklo segmentavimas;

35.2. prieigos kontrolės sąrašai (ACL);

35.3. „statefull“ ugniasienė; tinklo išorinis perimetras apsaugotas interneto prieigos maršruto parinktuvu ir ugniasiene. Išoriniam perimetrui apsaugoti naudojamas statinis 7 lygmens pagal OSI modelį paketų ir „statefull“ (sekantis paketų būsenas) filtravimas;

35.4. tinklo adresų transliavimas (NAT/PAT);

35.5. pagrindinė Informacinės sistemos duomenų pateikimo prieiga yra duomenų perdavimas duomenų perdavimo kanalu, panaudojant saugų HTTPS protokolą. Informacinės sistemos naudotojai identifikuojami ir jiems suteikiamos teisės pagal jam suteiktą naudotojo vardą ir slaptažodį. Kaip papildoma priemonė, ribojanti prisijungimą prie Informacinės sistemos, yra interneto protokolo (angl. IP) adresų filtravimas.

36. Informacinės sistemos duomenys, perduodami ne per Informacinės sistemos tvarkytojui priklausančias duomenų perdavimo linijas, privalo būti šifruojami.

37. Saugos dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) po rizikos analizės ar informacinių technologijų saugos atitikties vertinimo atlikimo arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Prireikus saugos dokumentai turi būti tikslinami ir derinami su Vidaus reikalų ministerija.

38. Informacinės sistemos duomenų gavimo automatiniu būdu iš kitų informacinių sistemų tvarka nustatoma duomenų teikimo sutartyse.

39. Informacinės sistemos saugai užtikrinti turi būti apribota fizinė prieiga prie informacinės sistemos tarnybinių stočių (atskiros rakinamos patalpos arba rakinama spinta), patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų.

40. Informacinei sistemai administruoti naudojamas tarnybinių stočių operacines sistemas, techninę ir programinę įrangą, reikalingą Informacinės sistemos naudotojo funkcijoms vykdyti, diegia ir prižiūri tik Informacinės sistemos administratorius (-iai).

41. Informacinės sistemos programinę įrangą diegti ar atnaujinti gali tik Informacinės sistemos administratorius (-iai) ar Informacinės sistemos tvarkytojo įgalioti asmenys.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

42. Informacinės sistemos saugos įgaliotinis turi išmanyti informacijos saugos užtikrinimo principus, savo darbe vadovautis Saugos dokumentais, Informacinių technologijų saugos atitikties vertinimo metodika ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, standartais ir kitais dokumentais, reglamentuojančiais Informacinės sistemos duomenų tvarkymą, sugebėti prižiūrėti Informacinės sistemos saugos politikos įgyvendinimą. Informacinės sistemos administratorius privalo išmanyti Informacinės sistemos informacijos saugos politikos principus, darbą su duomenų perdavimo tinklais, mokėti užtikrinti jų saugą, taip pat administruoti ir prižiūrėti informacines sistemas, turi būti susipažinęs su šiais saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais saugos dokumentais.

43. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

44. Informacinės sistemos naudotojai turi turėti naudojimosi kompiuteriu įgūdžių, mokėti tvarkyti Informacinės sistemos duomenis Informacinės sistemos nuostatų nustatyta tvarka, būti susipažinę su šiais Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais saugos dokumentais.

45. Informacinės sistemos naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių ar netinkamai veikiančių Informacinės sistemos duomenų saugos priemonių, nedelsdami privalo apie tai pranešti Informacinės sistemos administratoriui.

46. Informacinės sistemos administratorius apie Saugos nuostatų 45 punkte nurodytus pažeidimus informuoja Informacinės sistemos saugos įgaliotinį. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią Informacinės sistemos saugą (jos konfidencialumą, vientisumą ar prieinamumą), Informacinės saugos įgaliotinis apie tai turi pranešti kompetentingoms institucijoms.

47. Informacinės sistemos naudotojų informacijos saugos mokymai ir žinių atnaujinimas atliekamas kasmet. Už tai atsakingas saugos įgaliotinis.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

48. Tvarkyti Informacinės sistemos duomenis gali tik įgalioti Informacinės sistemos naudotojai, susipažinę su saugos dokumentais ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų.

49. Už Informacinės sistemos naudotojų supažindinimą su saugos dokumentais, kitais teisės aktais, nurodytais Saugos nuostatų 15 punkte, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, atsakomybę už saugos dokumentų nuostatų pažeidimus, informacijos saugos mokymą ir žinių atnaujinimą atsako Saugos įgaliotinis.

50. Tvarkyti Informacinės sistemos duomenis gali tik įgalioti Informacinės sistemos naudotojai, susipažinę su saugos dokumentais ir raštu sutikę laikytis saugos dokumentuose nustatytų reikalavimų. Saugos įgaliotinis raštu informuoja Informacinės sistemos naudotojus apie saugos dokumentų priėmimą, pakeitimą ar pripažinimą netekusiais galios.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

51. Informacinės sistemos valdytojas, Informacinės sistemos tvarkytojas, Informacinės sistemos Saugos įgaliotinis, Informacinės sistemos administratorius ir Informacinės sistemos naudotojai, pažeidę šių Saugos nuostatų ir kitų saugų informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

_____