Suvestinė redakcija nuo 2015-08-18 iki 2017-11-20

Įsakymas paskelbtas: Žin. 2011, Nr. 124-5916, i. k. 1112250ISAK000V-889

LIETUVOS RESPUBLIKOS
SVEIKATOS APSAUGOS MINISTRO
Į S A K Y M A S

DĖL ELEKTRONINĖS SVEIKATOS PASLAUGŲ IR BENDRADARBIAVIMO INFRASTRUKTŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2011 m. spalio 7 d. Nr. V-889
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ 7.1 papunkčiu, 11 ir 19 punktais:

Preambulės pakeitimai:
Nr. V-927, 2015-08-10, paskelbta TAR 2015-08-17, i. k. 2015-12343

1. T v i r t i n u Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatus (pridedama).

2. N u s t a t a u, kad:

2.1. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos pagrindinio tvarkytojo valstybės įmonės Registrų centro direktorius per 3 mėnesius nuo Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatų patvirtinimo paskiria Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos vyriausiąjį saugos įgaliotinį;

2.2. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos pagrindinis tvarkytojas valstybės įmonė Registrų centras per 6 mėnesius nuo Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatų patvirtinimo parengia ir pateikia Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos valdytojui tvirtinti Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos veiklos tęstinumo valdymo plano ir Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos naudotojų administravimo taisyklių projektus.

3. P a v e d u įsakymo vykdymą kontroliuoti viceministrui pagal veiklos sritį.

Punkto pakeitimai:
Nr. V-927, 2015-08-10, paskelbta TAR 2015-08-17, i. k. 2015-12343

SVEIKATOS APSAUGOS MINISTRAS RAIMONDAS ŠUKYS

SUDERINTA

Lietuvos Respublikos vidaus reikalų ministerijos
2011-08-01 raštu Nr. 1D-5307 (3)

SUDERINTA
Valstybės įmonės Registrų centro
2011-07-26 raštu Nr. (1.1.5.)s-3231

PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. spalio 7 d. įsakymu Nr. V-889
(Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. rugpjūčio 10 d. įsakymo Nr. V-927 redakcija)

ELEKTRONINĖS SVEIKATOS PASLAUGŲ IR BENDRADARBIAVIMO INFRASTRUKTŪROS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos (toliau – informacinė sistema) duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja informacinės sistemos duomenų saugos politiką, nustato organizacines, technines, programines, teisines ir kitas priemones, užtikrinančias saugų informacinės sistemos duomenų tvarkymą.

2. Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ ir kituose teisės aktuose vartojamas sąvokas ir jų apibrėžimus.

3. Elektroninės informacijos saugumo užtikrinimo tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti informacinės sistemos duomenis, užtikrinti elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei tinklo įrangos funkcionavimą. Informacinės sistemos duomenų saugai užtikrinti kompleksiškai naudojamos administracinės, techninės ir programinės priemonės, padedančios įgyvendinti reagavimo, atsakomybės, elektroninės informacijos saugos suvokimo kėlimo ir saugos priemonių projektavimo ir diegimo principus.

4. Elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. paciento asmens ir ypatingų sveikatos duomenų, registracijos ir siuntimų konsultuoti, tirti, gydyti duomenų konfidencialumo, vientisumo ir prieinamumo užtikrinimas naudojant technines, organizacines ir teisines priemones:

4.1.1. duomenų konfidencialumas užtikrinamas techninėmis ir organizacinėmis priemonėmis ribojant priėjimą prie asmens duomenų ir ypatingų asmens duomenų; priėjimas suteikiamas tik teisėtiems informacinės sistemos tvarkytojams ir naudotojams, kurių tapatybė yra nustatyta, ir tik prie duomenų, būtinų informacinės sistemos naudotojo veiklos funkcijoms vykdyti; supažindinant administratorius ir naudotojus su konfidencialaus asmens duomenų tvarkymo principais;

4.1.2. duomenų ar sistemos vientisumas užtikrinamas valdant teisėtą duomenų ar sistemos keitimą, kontroliuojant duomenų įvedimą, stebint ir reaguojant į galimą neteisėtą duomenų ar sistemos keitimą ar sunaikinimą; atsakingi už duomenų įvedimą ar keitimą sistemos administratoriai ir naudotojai supažindinami su klaidų ir vientisumo pažeidimo nustatymo ir koregavimo metodais ir tvarkų aprašais;

4.1.3. duomenų ar sistemos prieinamumas užtikrinamas organizacinėmis ir technologinėmis priemonėmis valdant informacinę sistemą, jos elementų ar duomenų keitimus, naudojant perteklines ar alternatyvias informacinių sistemų ir duomenų tinklų technologines priemones, atliekant informacinės sistemos atkūrimo plano bandymus ir veiklos tęstinumo valdymo plano bandymus;

4.2. kitos prioritetinės kryptys:

4.2.1. administracinių saugaus darbo su duomenimis, asmens duomenimis ir ypatingais asmens duomenimis priemonių įgyvendinimas ir kontrolė (informacinės sistemos duomenų gavėjų ir teikėjų, informacinės sistemos tvarkytojų teisių, įpareigojimų, atsakomybės ribų, detalių informacinės sistemos elektroninės informacijos tvarkymo ir administravimo taisyklių nustatymas);

4.2.2. technologinė elektroninės informacijos apdorojimo priemonių (informacinės sistemos tarnybinių stočių saugojimo patalpų, tarnybinių stočių, elektroninės informacijos perdavimo įrangos, programinės įrangos) apsauga;

4.3. Informacinės sistemos veiklos tęstinumo užtikrinimas;

4.4. asmens duomenų apsauga;

4.5. naudotojų mokymas.

5. Informacinės sistemos valdytoja – Lietuvos Respublikos sveikatos apsaugos ministerija (toliau – Sveikatos apsaugos ministerija), buveinės adresas: Vilniaus g. 33, LT-01506 Vilnius.

6. Informacinės sistemos tvarkytojai – valstybės įmonė Registrų centras (toliau – Registrų centras) (pagrindinis informacinės sistemos tvarkytojas), buveinės adresas: Vinco Kudirkos g. 18-3, 03105 Vilnius, ir sveikatinimo veiklą vykdančios įstaigos (toliau – sveikatinimo įstaigos).

7. Informacinės sistemos valdytojo funkcijos ir atsakomybė:

7.1. rengia ir tvirtina informacinės sistemos duomenų saugos politiką įgyvendinančius teisės aktus;

7.2. kontroliuoja, kaip laikomasi informacinės sistemos duomenų saugos politiką įgyvendinančių dokumentų ir kitų teisės aktų, reglamentuojančių informacinės sistemos duomenų tvarkymo teisėtumą ir saugos valdymą, reikalavimų;

7.3. priima sprendimus dėl informacinės sistemos techninių ir programinių priemonių, būtinų informacinės sistemos duomenų saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

7.4. prižiūri, kaip laikomasi informacinės sistemos duomenų ir elektroninės informacijos saugos reikalavimų;

7.5. nagrinėja informacinės sistemos tvarkytojų pasiūlymus dėl informacinės sistemos saugos tobulinimo ir priima dėl jų sprendimus;

7.6. priima sprendimą atlikti informacinės sistemos informacinių technologijų saugos reikalavimų atitikties vertinimą;

7.7. vykdo kitas informacinės sistemos duomenų saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose informacinės sistemos duomenų tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas;

7.8. atsako už informacinės sistemos duomenų tvarkymo, teikimo ir (ar) gavimo teisėtumą ir saugą.

8. Pagrindinio informacinės sistemos tvarkytojo – Registrų centro – funkcijos:

8.1. rengia informacinės sistemos duomenų saugos politiką įgyvendinančių teisės aktų projektus;

8.2. teikia savo ir apibendrintus kitų informacinės sistemos tvarkytojų pateiktus pasiūlymus informacinės sistemos valdytojui, kaip tobulinti informacinės sistemos saugą;

8.3. užtikrina tinkamą informacinės sistemos valdytojo priimtų teisės aktų ir rekomendacijų įgyvendinimą;

8.4. užtikrina nepertraukiamą informacinės sistemos veikimą ir elektroninės informacijos saugą, taip pat saugų elektroninės informacijos perdavimą kompiuterių tinklais (automatiniu būdu);

8.5. užtikrina informacinės sistemos sąveiką su kitomis informacinėmis sistemomis ir registrais;

8.6. Informacinės sistemos valdytojui pavedus, skiria saugos įgaliotinį;

8.7. skiria administratorius, vykdančius informacinės sistemos administravimo funkcijas.

9. Informacinės sistemos tvarkytojų – sveikatinimo įstaigų – funkcijos:

9.1. užtikrina tinkamą informacinės sistemos valdytojo priimtų teisės aktų ir rekomendacijų įgyvendinimą sveikatinimo įstaigose;

9.2. nustato darbo organizavimo principus ir tvarką, kurie užtikrina saugų informacinės sistemos duomenų ir elektroninės informacijos tvarkymą sveikatinimo įstaigose;

9.3. užtikrina, kad informacinė sistema sveikatinimo įstaigose būtų tvarkoma vadovaujantis Informacinės sistemos nuostatais, Saugos nuostatais ir kitais informacinės sistemos duomenų saugos politiką įgyvendinančiais dokumentais;

9.4. kiekviena sveikatinimo įstaiga skiria saugos įgaliotinį;

9.5. kiekviena sveikatinimo įstaiga skiria administratorius, vykdančius informacinės sistemos administravimo funkcijas savo įstaigoje;

9.6. teikia pasiūlymus pagrindiniam informacinės sistemos tvarkytojui, kaip tobulinti informacinės sistemos saugą.

10. Informacinės sistemos tvarkytojų vadovai atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir informacinės sistemos duomenų saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

11. Pagrindinio informacinės sistemos tvarkytojo saugos įgaliotinio funkcijos ir atsakomybė:

11.1. koordinuoja sveikatinimo įstaigų saugos įgaliotinių veiklą;

11.2. rengia duomenų saugos politiką įgyvendinančių dokumentų projektus;

11.3. teikia informacinės sistemos valdytojo vadovui pasiūlymus dėl:

11.3.1. duomenų saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

11.3.2. informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo;

11.4. teikia pagrindinio informacinės sistemos tvarkytojo vadovui pasiūlymus dėl administratorių paskyrimo ir reikalavimų jiems nustatymo;

11.5. koordinuoja elektroninės informacijos saugos incidentų tyrimą, išskyrus atvejus, kai šią funkciją atlieka informacijos saugos darbo grupė;

11.6. kasmet organizuoja kasmetinius ir prireikus neeilinius informacinės sistemos rizikos vertinimus;

11.7. teikia administratoriams privalomus vykdyti nurodymus ir pavedimus dėl informacinės sistemos saugos politikos įgyvendinimo;

11.8. supažindina administratorius su informacinės sistemos duomenų saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, taip pat su atsakomybe už šiuose dokumentuose nustatytų reikalavimų nesilaikymą;

11.9. periodiškai inicijuoja darbuotojų (išskyrus sveikatinimo įstaigų naudotojus) supažindinimą su informacijos sauga, siųsdamas priminimus ir konsultuodamas elektroniniu paštu;

11.10. atsako už informacinės sistemos duomenų saugos politikos įgyvendinimo organizavimą;

11.11. atsako už informacinės sistemos saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams;

11.12. vykdo kitas informacinės sistemos duomenų saugos politiką įgyvendinančiuose dokumentuose ir kituose teisės aktuose, reglamentuojančiuose informacinės sistemos duomenų tvarkymo teisėtumą ir saugos valdymą, priskirtas funkcijas.

12. Sveikatinimo įstaigos saugos įgaliotinio funkcijos ir atsakomybė:

12.1. įgyvendina informacinės saugos reikalavimus sveikatinimo įstaigoje;

12.2. teikia sveikatinimo įstaigos vadovui pasiūlymus dėl administratorių paskyrimo ir reikalavimų jiems nustatymo;

12.3. supažindina sveikatinimo įstaigos naudotojus ir administratorius su Saugos nuostatais ir informacinės sistemos duomenų saugos politiką įgyvendinančiais dokumentais, kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, taip pat su atsakomybe už juose nurodytų reikalavimų nesilaikymą;

12.4. informuoja pagrindinio informacinės sistemos tvarkytojo saugos įgaliotinį apie saugos dokumentų pažeidimus, nusikalstamos veikos požymius;

12.5. periodiškai inicijuoja sveikatinimo įstaigos naudotojų, administratorių supažindinimą su informacijos sauga, informuoja juos informacijos saugos klausimais, siųsdamas priminimus ir konsultuodamas elektroniniu paštu;

12.6. vykdo pagrindinio informacinės sistemos tvarkytojo saugos įgaliotinio pavedimus dėl informacinės sistemos duomenų saugos.

13. Sveikatinimo įstaigos saugos įgaliotinis informacinės sistemos saugos klausimais yra atskaitingas informacinės sistemos tvarkytojo saugos įgaliotiniui.

14. Informacinės sistemos priežiūrą atlieka administratoriai: kompiuterių tinklų administratorius, tarnybinių stočių administratorius, duomenų bazių administratorius ir naudotojų administratorius. Pagal einamas pareigas ir prieigos prie informacinės sistemos lygį:

14.1. kompiuterių tinklų administratorius atlieka šias funkcijas:

14.1.1. užtikrina kompiuterių tinklų veikimą;

14.1.2. projektuoja kompiuterių tinklus;

14.1.3. diegia, konfigūruoja ir aptarnauja kompiuterių tinklų aktyviąją įrangą;

14.1.4. užtikrina kompiuterių tinklų saugumą;

14.2. tarnybinių stočių administratorius atlieka šias funkcijas:

14.2.1. užtikrina tarnybinių stočių veikimą;

14.2.2. konfigūruoja tarnybinių stočių tinklo prieigą;

14.2.3. kuria ir administruoja tarnybinių stočių naudotojų registracijos į tarnybines stotis duomenis;

14.2.4. stebi ir analizuoja tarnybinių stočių veiklą;

14.2.5. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

14.2.6. diegia tarnybinių stočių programinės įrangos atnaujinimus;

14.2.7. užtikrina tarnybinių stočių saugą;

14.3. duomenų bazių administratorius atlieka šias funkcijas:

14.3.1. užtikrina duomenų bazių veikimą;

14.3.2. tvarko duomenų bazių programinę įrangą;

14.3.3. konfigūruoja duomenų bazių kompiuterių tinklo aplinką;

14.3.4. kuria ir administruoja duomenų bazių naudotojų registracijos į duomenų bazes duomenis;

14.3.5. kuria ir atkuria atsargines elektroninės informacijos kopijas;

14.3.6. stebi duomenų bazes ir optimizuoja jų funkcionavimą;

14.4. naudotojų administratorius atlieka šias funkcijas:

14.4.1. administruoja naudotojų duomenis;

14.4.2. tvarko naudotojų klasifikatorius;

14.4.3. analizuoja naudotojų veiksmų registracijos žurnalų įrašus.

15. Administratoriai, vykdydami informacinės sistemos priežiūrą, yra atsakingi už tinkamą Saugos nuostatuose nustatytų funkcijų vykdymą.

16. Informacinės sistemos duomenys tvarkomi ir jų sauga užtikrinama vadovaujantis:

16.1. Lietuvos Respublikos sveikatos sistemos įstatymu;

16.2. Lietuvos Respublikos sveikatos priežiūros įstaigų įstatymu;

16.3. Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymu;

16.4. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

16.5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

16.6. Lietuvos Respublikos kibernetinio saugumo įstatymu;

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

16.8. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas);

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

16.10. Bendraisiais reikalavimais organizacinėms ir techninėms asmens duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“ (toliau – Bendrieji reikalavimai organizacinėms ir techninėms asmens duomenų saugumo priemonėms);

16.11. Lietuvos standartais LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“;

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

16.13. kitais teisės aktais, kuriais reglamentuojamas elektroninės informacijos tvarkymo teisėtumas, informacinės sistemos valdytojo ir tvarkytojų veikla ir elektroninės informacijos saugos valdymas.

17. Saugos nuostatai privalomi visiems naudotojams, saugos įgaliotiniams ir administratoriams.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

18. Informacinėje sistemoje tvarkoma elektroninė informacija priskirtina ypatingos svarbos elektroninės informacijos kategorijai, vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 4.1.1 ir 4.1.5 papunkčių nuostatomis.

19. Informacinė sistema priskiriama pirmajai kategorijai, vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 5.1 papunkčio nuostatomis, atsižvelgiant į pagrindiniame valstybės registre apdorojamos elektroninės informacijos svarbos kategoriją.

20. Informacinės sistemos asmens duomenų tvarkymas automatiniu būdu priskirtinas antrajam saugumo lygiui, vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms 11.3 papunkčio nuostatomis.

21. Pagrindinio informacinės sistemos tvarkytojo saugos įgaliotinis, vadovaudamasis Lietuvos Respublikos vidaus reikalų ministerijos išleistu metodiniu leidiniu „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacinės technologijos. Saugumo metodai“ grupės standartais, kasmet organizuoja informacinės sistemos rizikos vertinimą, o prireikus ir neeilinį šios rizikos vertinimą.

22. Informacinės sistemos rizikos įvertinimas įforminamas rizikos įvertinimo ataskaitoje. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius

turėti įtakos informacijos saugai. Informacinės sistemos rizikos įvertinimo ataskaita pateikiama informacinės sistemos valdytojo vadovui.

23. Svarbiausi rizikos veiksniai yra šie:

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

23.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacinės sistemos duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymas, saugumo pažeidimai, vagystės ir kita);

23.3. 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.

24. Atsižvelgdamas į rizikos įvertinimo ataskaitą, informacinės sistemos valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

25. Pagrindinio informacinės sistemos tvarkytojo saugos įgaliotinis ne rečiau kaip vieną kartą per metus organizuoja informacinių technologijų saugos atitikties vertinimą, kurio metu:

25.1. įvertinama, ar informacinės sistemos duomenų saugos politiką įgyvendinantys dokumentai atitinka realią informacijos saugos situaciją;

25.2. inventorizuojama informacinės sistemos techninė ir programinė įranga;

25.3. patikrinama ne mažiau kaip 10 procentų atsitiktinai parinktų naudotojų kompiuterinių darbo vietų, visose tarnybinėse stotyse įdiegtos programos ir jų sąranga;

25.4. įvertinama naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;

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

26. Atlikus informacinių technologijų saugos atitikties vertinimą, pagrindinio informacinės sistemos tvarkytojo saugos įgaliotinis rengia ir teikia informacinės sistemos valdytojui vertinimo ataskaitą.

27. Atsižvelgdamas į informacinių technologijų saugos atitikties vertinimo ataskaitą, pagrindinio informacinės sistemos tvarkytojo saugos įgaliotinis prireikus parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinės sistemos valdytojo vadovas.

28. Patvirtintų informacinės sistemos duomenų saugos politiką įgyvendinančių dokumentų ir jų pakeitimų kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo jų patvirtinimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) 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 (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, (toliau – Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatai) nustatyta tvarka.

29. Techninės, programinės ir organizacinės informacinės sistemos elektroninės informacijos saugos priemonės pasirenkamos atsižvelgiant į informacinės sistemos valdytojo turimus resursus, vadovaujantis šiais priemonių parinkimo principais:

29.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

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

29.3. kur galima, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

30. Informacinės sistemos informacinių technologijų saugos atitikties vertinimą ne rečiau kaip kartą per trejus metus turi atlikti nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai.

31. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano, saugos atitikties vertinimo ataskaitos ir pastebėtų trūkumų šalinimo plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

32.1. tarnybinėse stotyse ir kompiuterinėse darbo vietose su „Microsoft Windows“ operacine sistema privalo būti įdiegta centralizuotai valdoma apsaugai naudojama programinė įranga nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos ir kt.);

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

32.3. kompiuterinėse darbo vietose turi būti įdiegtos priemonės, leidžiančios riboti USB jungties ir kito tipo laikmenų naudojimą;

32.4. apsaugai naudojama programinė įranga turi atsinaujinti ne rečiau kaip kartą per 24 valandas;

32.5. apsaugai naudojama programinė įranga turi automatiškai elektroniniu paštu informuoti atsakingus darbuotojus apie kompiuterines darbo vietas ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 24 valandas;

32.6. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

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

33.1. naudojama tik legali programinė įranga;

33.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

33.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka tik tarnybinių stočių administratorius.

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

34.1. kompiuterių tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, „DOS“ ir „DDOS“ atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

34.2. visas duomenų srautas į ir iš interneto yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

34.3. naudojamos turinio filtravimo sistemos;

34.4. naudojamos aplikacijų kontrolės sistemos.

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

35.1. nuotolinis prisijungimas prie informacinės sistemos galimas:

35.1.1. iš virtualių darbo vietų „PCoIP“ protokolu. Nutolusiame kompiuteryje įdiegiama speciali programinė įranga „Vmware view client“ ir jungiamasi per specializuotą tarnybinę stotį (securitysrv.kada.lt) naudojant HTTPS protokolą;

35.1.2. naudojantis „IPSec“ (angl. *Internet Protocol Security*) protokolų rinkiniu ir jungiantis kaip „IPSec“ programiniam klientui;

35.1.3. naudojant šifruotą komandinės eilutės protokolą „SSH“ (angl. *Secure shell*). Šia galimybe gali būti pasinaudota tik informacinės sistemos administravimo tikslais;

35.2. prieiga prie informacinės sistemos yra ribojama ugniasienėmis;

35.3. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų valstybės institucijų, naudojami saugūs ryšio kanalai. Informacijai perduoti gali būti naudojamas Saugus valstybinis duomenų perdavimo tinklas;

35.4. teikti ir (ar) gauti elektroninę informaciją automatiniu būdu galima tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas – naudojami saugūs ryšio kanalai (VPN).

36. Nešiojamieji kompiuteriai, jei juose yra įdiegta informacinės sistemos naudotojo darbo vietos programinė įranga, gali būti išnešami iš įstaigos, kuriai priskirta naudotojo darbo vieta, patalpų tik vadovaujantis įstaigos direktoriaus įsakymu patvirtintu kompiuterių ir programinės įrangos ir informacinių resursų naudojimo darbo vietose tvarkos aprašu. Šiuo atveju naudotojas asmeniškai Lietuvos Respublikos teisės aktų nustatyta tvarka atsako už kompiuterio duomenų saugojimo laikmenose esančių informacinės sistemos duomenų saugą.

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

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

37.2. atsarginės kopijos daromos magnetinėse laikmenose;

37.3. atsarginės kopijos magnetinėse laikmenose daromos reguliariai, kiekvieną darbo dieną;

37.4. sukurta atsarginė kopija pažymima specialia ženklinimo etikete, kurioje nurodoma kopijavimo data, kopiją padariusio asmens duomenys (pareigos, vardas, pavardė), duomenų katalogai;

37.5. kiekvienos savaitės paskutinės atsarginės kopijos ženklinimo etiketėje papildomai nurodoma, kad tai yra savaitinė kopija;

37.6. kiekvieno mėnesio paskutinės atsarginės kopijos ženklinimo etiketėje papildomai nurodoma, kad tai yra mėnesinė kopija;

37.7. kiekvienų metų paskutinės atsarginės kopijos ženklinimo etiketėje papildomai nurodoma, kad tai yra metinė kopija;

37.8. atsargines dokumentų kopijas turi teisę daryti tik pagrindinio informacinės sistemos tvarkytojo administratorius, kurio pareigybės aprašyme numatyta ši funkcija;

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

37.10. atsarginės kopijos magnetinėje laikmenoje saugomos pagrindinio informacinės sistemos tvarkytojo duomenų kopijų archyve. Už jų atidavimą saugoti atsako pagrindinio informacinės sistemos tvarkytojo administratorius, vykdantis dokumentų kopijavimo funkciją;

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

37.12. informacinės sistemos duomenų atsarginės kopijos turi būti daromos automatiškai. Jas atkurti turi teisę tik pagrindinio informacinės sistemos tvarkytojo administratorius;

37.13. bandomieji elektroninės informacijos atkūrimai iš mėnesio atsarginių kopijų vykdomi kartą per mėnesį, o vieną kartą metuose daromas metų kopijos atkūrimas;

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

38. Užtikrinant techninius saugos reikalavimus, kurie keliami ypatingai svarbios elektroninės informacijos prieinamumui, turi būti numatyta rezervinė pagrindinė kompiuterinė ir programinė įranga bei infrastruktūra.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

39. Saugos įgaliotiniai privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis informacinės sistemos duomenų saugos politiką įgyvendinančiais dokumentais, standartais ir kitais duomenų tvarkymą reglamentuojančiais Lietuvos Respublikos ir Europos Sąjungos teisės aktais bei būti susipažinę su esminiais informacinės sistemos duomenų saugos reikalavimais, turėti reikiamą kvalifikaciją saugos politikai įgyvendinti.

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

41. Administratoriai privalo išmanyti informacijos saugos principus, mokėti užtikrinti jų saugą, administruoti ir prižiūrėti duomenų bazes, turi būti susipažinę su informacinės sistemos duomenų saugos politiką įgyvendinančiais dokumentais, darbo saugos taisyklėmis. Administratoriai privalo gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų diagnostiką ir šalinimą, išmanyti elektroninės informacijos saugos užtikrinimo principus.

42. Naudotojai privalo turėti pagrindinius darbo su kompiuteriu įgūdžius, mokėti tvarkyti duomenis, turi būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą; pasirašę pasižadėjimą saugoti asmens duomenų paslaptį; nuolat kelti savo kvalifikaciją

kvalifikacijos kėlimo kursuose, saugaus darbo su duomenimis seminaruose ir mokymuose; gilinti kompiuterines žinias ir būti susipažinę su informacinės sistemos duomenų saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, įgyvendinančiais informacinės sistemos duomenų saugos politiką.

43. Saugos įgaliotiniai administratoriams ir naudotojams periodiškai, bet ne rečiau kaip kartą per dvejus metus organizuoja mokymus elektroninės informacijos saugos klausimais, įvairiais būdais primena apie saugumo problemas (pvz., pranešimai elektroniniu paštu, naujų darbuotojų instruktavimas ir pan.).

V SKYRIUS
NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

44. Naudoti informacinės sistemos duomenis gali tik tie asmenys, kurie yra susipažinę su Saugos nuostatais, informacinės sistemos duomenų saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugumą, taip pat su atsakomybe už šiuose dokumentuose nustatytų reikalavimų nesilaikymą ir raštiškai sutikę laikytis šių teisės aktų reikalavimų.

45. Už naudotojų supažindinimą su Saugos nuostatais, informacinės sistemos duomenų saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, taip pat su atsakomybe už šiuose dokumentuose nustatytų reikalavimų nesilaikymą yra atsakingi saugos įgaliotiniai.

46. Saugos nuostatai ir informacinės sistemos duomenų saugos politiką įgyvendinantys dokumentai skelbiami naudotojams pasiekiamoje interneto svetainėje.

47. Pakartotinis supažindinimas su Saugos nuostatais ir informacinės sistemos duomenų saugos politiką įgyvendinančiais dokumentais yra vykdomas elektroniniu paštu šiems dokumentams pasikeitus.

48. Naudotojai, administratoriai ir saugos įgaliotiniai, pažeidę Saugos nuostatų, informacinės sistemos duomenų saugos politiką įgyvendinančių dokumentų ir saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

Priedo pakeitimai:
Nr. V-927, 2015-08-10, paskelbta TAR 2015-08-17, i. k. 2015-12343

Pakeitimai:

1.
Lietuvos Respublikos sveikatos apsaugos ministerija, Įsakymas
Nr. V-927, 2015-08-10, paskelbta TAR 2015-08-17, i. k. 2015-12343
Dėl Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. spalio 7 d. įsakymo Nr. V-889 „Dėl Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo