Suvestinė redakcija nuo 2020-01-01 iki 2022-06-30

Įsakymas paskelbtas: TAR 2015-07-13, i. k. 2015-11260

VALSTYBINĖS AKREDITAVIMO SVEIKATOS PRIEŽIŪROS VEIKLAI TARNYBOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL VALSTYBINĖS AKREDITAVIMO SVEIKATOS PRIEŽIŪROS VEIKLAI TARNYBOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS INFORMACINĖS SISTEMOS, SVEIKATOS PRIEŽIŪROS ĮSTAIGŲ LICENCIJAVIMO INFORMACINĖS SISTEMOS IR SVEIKATOS PRIEŽIŪROS TECHNOLOGIJŲ, SUSIJUSIŲ SU MEDICINOS PRIETAISAIS, VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2015 m. birželio 29 d. Nr. T1-1024
Vilnius

Vadovaudamasi Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi, 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 ir 13, 19 punktais:

1. T v i r t i n u Valstybinės akreditavimo sveikatos priežiūros veiklai tarnybos prie Sveikatos apsaugos ministerijos informacinės sistemos, Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos bei Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos duomenų saugos nuostatus (pridedama).

2. P r i p a ž į s t u netekusiu galios Valstybinės akreditavimo sveikatos priežiūros veiklai tarnybos prie Sveikatos apsaugos ministerijos (toliau – VASPVT) direktoriaus 2010 m. birželio 14 d. įsakymą Nr. T1-498 „Dėl Valstybinės akreditavimo sveikatos priežiūros veiklai tarnybos prie Sveikatos apsaugos ministerijos informacinės sistemos bei Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais.

3. S k i r i u VASPVT informacinės sistemos, Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos bei Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos saugos įgaliotinį – Informacinių technologijų skyriaus vedėją Liną Nausėdienę.

4. P a v e d u:

4.1. VASPVT Teisės ir bendrųjų reikalų skyriui per 6 mėnesius nuo VASPVT informacinės sistemos, Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos bei Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo dienos parengti, suderinti ir pateikti tvirtinti:

4.1.1. VASPVT informacinės sistemos, Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos bei Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių projektą;

4.1.2. VASPVT informacinės sistemos, Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos bei Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos veiklos tęstinumo valdymo plano projektą;

4.1.3. VASPVT informacinės sistemos, Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos bei Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos naudotojų administravimo taisyklių projektą.

5. P a s i l i e k u sau įsakymo vykdymo kontrolę.

Direktoriaus pavaduotoja,
laikinai vykdanti direktoriaus funkcijas Ramunė Vaitkevičienė

PATVIRTINTA
Valstybinės akreditavimo
sveikatos priežiūros veiklai tarnybos
prie Sveikatos apsaugos ministerijos
direktoriaus 2015 m. birželio 29 d.
įsakymu Nr. T1-1024

VALSTYBINĖS AKREDITAVIMO SVEIKATOS PRIEŽIŪROS VEIKLAI TARNYBOS PRIE SVEIKATOS APSAUGOS MINISTERIJOS INFORMACINĖS SISTEMOS, SVEIKATOS PRIEŽIŪROS ĮSTAIGŲ LICENCIJAVIMO INFORMACINĖS SISTEMOS IR SVEIKATOS PRIEŽIŪROS TECHNOLOGIJŲ, SUSIJUSIŲ SU MEDICINOS PRIETAISAIS, VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės akreditavimo sveikatos priežiūros veiklai tarnybos prie Sveikatos apsaugos ministerijos (toliau – VASPVT) informacinės sistemos, Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos (toliau – SPĮLIS) bei Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos (toliau – TechnoMedTas) duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato šiose informacinėse sistemose tvarkomos elektroninės informacijos saugos tikslus, duomenų saugos užtikrinimo prioritetines kryptis, saugų elektroninės informacijos valdymą, organizacinius, techninius ir personalui keliamus reikalavimus, naudotojų supažindinimo su saugos dokumentais principus, apibrėžia duomenų saugos politiką.

2. Šiuose Saugos nuostatuose vartojamos sąvokos atitinka teisės aktuose, nurodytuose šių Saugos nuostatų 10 punkte, vartojamas sąvokas.

3. Šiais Saugos nuostatais turi vadovautis VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojas, VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas tvarkytojas, VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas saugos įgaliotinis (toliau – saugos įgaliotinis), VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas administratorius (toliau – administratorius) ir VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas naudotojai (toliau – naudotojai).

4. Informacijos saugos tikslai:

4.1. informacijos vientisumo, konfidencialumo, prieinamumo užtikrinimas;

4.2. kompiuterizuotų darbo vietų pakankamo saugos lygio įdiegimas ir palaikymas;

4.3. tinkamo kompiuterinės, programinės ir ryšių įrangos funkcionavimo užtikrinimas;

4.4. kompiuterinio ryšio, priimant ir perduodant informaciją elektroniniu paštu, patikimumo ir saugos užtikrinimas.

5. Informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas duomenims tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

5.2. VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas duomenų tvarkymo kontrolė;

5.3. veiklos tęstinumo užtikrinimas;

5.4. asmens duomenų apsauga.

6. VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojas ir tvarkytojas yra VASPVT, A. Juozapavičiaus g. 9, LT-09311 Vilnius.

Punkto pakeitimai:
Nr. T1-2063, 2019-12-31, paskelbta TAR 2019-12-31, i. k. 2019-21806

7. VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojo ir tvarkytojo funkcijos:

7.1. priima sprendimus dėl VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas techninių ir programinių priemonių įsigijimo, įdiegimo ir modernizavimo;

7.2. priima sprendimą dėl VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

7.3. atsako už elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugą;

7.4. tvirtina Saugaus elektroninės informacijos tvarkymo taisykles, Informacinės sistemos veiklos tęstinumo valdymo planą bei Informacinės sistemos naudotojų administravimo taisykles;

7.5. prižiūri saugos dokumentų reikalavimų įgyvendinimą;

7.6. skiria saugos įgaliotinį ir administratorių;

7.7. užtikrina, kad naudotojai laikytųsi Saugos nuostatuose ir saugos politiką įgyvendinančiuose teisės aktuose nurodytų reikalavimų;

7.8. kontroliuoja, kad Registras būtų tvarkomas vadovaujantis Lietuvos Respublikos įstatymais, šiais Saugos nuostatais ir kitais teisės aktais.

8. Saugos įgaliotinio funkcijos ir atsakomybė:

8.1. teikia VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojui siūlymus dėl:

8.1.1. administratoriaus paskyrimo (saugos įgaliotinis negali atlikti administratoriaus funkcijų);

8.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

8.1.3. VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas saugos atitikties vertinimo atlikimo;

8.2. koordinuoja VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas saugos incidentų tyrimą;

8.3. teikia administratoriui privalomus vykdyti nurodymus bei pavedimus, susijusius su saugos politikos įgyvendinimu;

8.4. organizuoja rizikos įvertinimą;

8.5. konsultuoja naudotojus VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas saugos klausimais;

8.6. atsako už VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas saugos politikos įgyvendinimo organizavimą;

8.7. atlieka kitas Saugos nuostatuose bei kituose teisės aktuose nustatytas funkcijas.

9. Administratoriaus funkcijos ir atsakomybė:

9.1. įvertina, ar naudotojai yra pasirengę darbui;

9.2. suteikia teisę naudotojams naudotis elektronine informacija paskirtoms funkcijoms atlikti;

9.3. administruoja ir užtikrina tinkamą VASPVT informacinę sistemą, SPĮLIS ir TechnoMedTas sudarančių komponentų (kompiuteriai, operacinės sistemos, duomenų bazių valdymo sistemos, taikomųjų programų sistemos, ugniasienės) veikimą, pažeidžiamų vietų ir saugos reikalavimų atitikties nustatymą;

9.4. informuoja saugos įgaliotinį apie saugos incidentus ir teikia pasiūlymus dėl saugos užtikrinimo;

9.5. atsako už kompiuterių tinklo funkcionavimą;

9.6. atsako už VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas atsarginių duomenų kopijų darymą.

10. VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas duomenys tvarkomi ir jų sauga užtikrinama vadovaujantis:

10.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

10.2. Lietuvos Respublikos valstybės informacinių išteklių įstatymu;

10.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

10.4. 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 – Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716);

10.5. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (OL 2016 L 119, p.1);

Papunkčio pakeitimai:

Nr. T1-2063, 2019-12-31, paskelbta TAR 2019-12-31, i. k. 2019-21806

10.6. Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos nuostatais, patvirtintais VASPVT direktoriaus 2015 m. kovo 31 d. įsakymu Nr. T1-537 „Dėl Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos nuostatų patvirtinimo“;

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

10.8. Bendraisiais reikalavimais organizacinėms ir techninėms 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 duomenų saugumo priemonėms patvirtinimo“;

10.9. 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“;

Papunkčio pakeitimai:

Nr. T1-2063, 2019-12-31, paskelbta TAR 2019-12-31, i. k. 2019-21806

10.10. Lietuvos standartais LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, reguliuojantys saugų informacinių sistemų duomenų tvarkymą;

10.11. kitais teisės aktais, reglamentuojančiais VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas duomenų tvarkymo teisėtumą bei VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas duomenų saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

11. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo (toliau – Aprašas), patvirtinto Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, 4.3 papunkčiu, VASPVT informacinėje sistemoje, SPĮLIS ir TechnoMedTas tvarkoma informacija priskiriama žinybinės svarbos elektroninės informacijos kategorijai.

12. Vadovaujantis Aprašo 5.2 papunkčiu, VASPVT informacinė sistema, SPĮLIS ir TechnoMedTas priskiriamos trečiai informacinių sistemų kategorijai.

13. Asmens duomenys VASPVT informacinėje sistemoje, SPĮLIS ir TechnoMedTas tvarkomi vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (OL 2016 L 119, p.1) (toliau – Reglamentas) ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu.

Punkto pakeitimai:

Nr. T1-2063, 2019-12-31, paskelbta TAR 2019-12-31, i. k. 2019-21806

14. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus, ne rečiau kaip kartą per metus organizuoja VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas rizikos įvertinimą. Minėtą rizikos įvertinimą gali atlikti ir pats saugos įgaliotinis. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą.

15. VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojo vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausieji rizikos veiksniai yra šie:

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

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

15.3. 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.

16. Atsižvelgdamas į rizikos įvertinimo ataskaitą, VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

17. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

Punkto pakeitimai:

Nr. T1-2063, 2019-12-31, paskelbta TAR 2019-12-31, i. k. 2019-21806

18. Saugos užtikrinimo priemonės parenkamos, siekiant užtikrinti VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas veiklos tęstinumą, patiriant kuo mažiau išlaidų ir užtikrinant saugų informacinės sistemos darbą.

19. VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas saugos atitikties vertinimas atliekamas vadovaujantis 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“.

20. Atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojo vadovas.

21. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

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

22.1. kompiuterinėse darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai atnaujinamos automatiniu būdu;

22.2. turi būti naudojamos priemonės, nuolat ieškančios ir blokuojančios kenksmingą programinę įrangą, veikiančią sisteminiuose kataloguose esančiose rinkmenose tarnybinėje stotyje ir visuose kompiuterių tinklo kompiuteriuose;

22.3. turi būti naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų;

22.4. apsaugai naudojama programinė įranga privalo atsinaujinti ne rečiau kaip kartą per 24 valandas.

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

23.1. nuotolinis prisijungimas galimas tik administratoriaus suteiktais unikaliais prisijungimo vardais ir slaptažodžiais naudojant virtualų privatų tinklą (VPN) arba nuotolinį darbalaukį (RDC);

23.2. kompiuterių tinklo tarnybinės stotys bei kiekvienas kompiuterių tinklui priklausantis kompiuteris privalo turėti užkardą, ribojančią priėjimą iš išorės bei duomenų srautus į išorę. Turi būti draudžiama naudoti interneto ryšį visoms programoms, kurios gali visiškai atlikti savo funkcijas ir be internetinio ryšio su išore. Visi nenaudojami prievadai turi būti užblokuoti;

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

23.4. duomenys kopijose šifruojami.

24. Naudotojams draudžiama patiems diegti bet kokią programinę įrangą. Draudimą kontroliuoja tarnybinės stoties operacinė sistema. Programinę įrangą, reikalingą naudotojo funkcijoms vykdyti, diegia ir prižiūri administratorius.

25. Neteisėtų programų įdiegimo (apeinant operacinės sistemos apsaugos mechanizmus) paiešką bent kartą per mėnesį atlieka administratorius. Nuolat turi būti stebimas interneto srautas,

siekiant aptikti ir išaiškinti galimus neleistinus, ne su naudotojų funkcijomis susijusius didelius duomenų srautus, apkraunančius ne mažiau kaip 20 proc. interneto ryšio resurso.

26. Turi būti galimybė reguliuoti atskirų interneto sričių pasiekiamumą tiek pagal interneto sričių vardus, tiek pagal fizinius adresus. Reguliavimą kontroliuoja administratorius, blokuodamas potencialiai pavojingas interneto sritis.

27. Nešiojamuosius VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas naudotojų kompiuterius, skirtus VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas elektroninei informacijai tvarkyti, išnešti iš VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas valdytojo patalpų yra griežtai draudžiama.

28. Pagrindiniai atsarginių duomenų kopijų darymo ir atkūrimo reikalavimai:

28.1. VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas atsarginės duomenų kopijos daromos automatiniu būdu kiekvieną dieną esant aktyviai registro duomenų bazei;

28.2. kopijos įrašomos į keičiamus informacijos kaupiklius (kompaktinius diskus, magnetines juostas ar kitas duomenų kopijų saugojimo laikmenas) ir saugomos seife, prieinamame tik administratoriui, jo nesant – administratorių pavaduojančiam asmeniui;

28.3. atsarginės duomenų kopijos turi būti saugomos kitose patalpose, atskirai nuo tarnybinių stočių;

28.4. prireikus duomenis atkurti turi teisę tik administratorius ar jį pavaduojantis asmuo;

28.5. kopijų, iš kurių būtų galima atkurti duomenis, darymo ir saugojimo tvarka detaliai aprašyta VASPVT informacinės sistemos, SPĮLIS ir TechnoMedTas saugaus informacijos tvarkymo taisyklėse.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

29. 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, arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

30. Saugos įgaliotinis turi išmanyti saugos užtikrinimo principus, darbą su kompiuterių tinklais, turėti darbo su operacinėmis sistemomis, taikomosiomis programomis patirties. Savo darbe turi vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais.

31. Administratorius turi išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugą. Administratorius privalo būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais.

32. Naudotojai privalo turėti pagrindinius darbo kompiuteriu įgūdžius, būti susipažinę su šiais Saugos nuostatais bei kitais saugos politiką reglamentuojančiais dokumentais.

33. Naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veiklos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti saugos įgaliotiniui.

34. Saugos įgaliotinis ne rečiau kaip kartą per metus inicijuoja naudotojų mokymą informacijos saugos klausimais, įvairiais būdais informuoja juos apie informacijos saugos problematiką.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

35. Naudotojų supažindinimą su šiais Saugos nuostatais bei kitais saugos politiką reglamentuojančiais dokumentais vykdo saugos įgaliotinis. Su minėtais dokumentais naudotojai supažindinami pasirašytinai. Pakartotinai su minėtais dokumentais naudotojai supažindinami iš esmės pasikeitus saugos dokumentams ir (arba) padažnėjus elektroninės informacijos saugos incidentų.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

36. Saugos įgaliotinis, administratorius ir naudotojai, pažeidę šių Saugos nuostatų reikalavimus, atsako teisės aktų nustatyta tvarka.

Pakeitimai:

1.
Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba prie Sveikatos apsaugos ministerijos, Įsakymas
Nr. T1-2063, 2019-12-31, paskelbta TAR 2019-12-31, i. k. 2019-21806
Dėl Valstybinės akreditavimo sveikatos priežiūros veiklai tarnybos prie Sveikatos apsaugos ministerijos direktoriaus 2015 m. birželio 29 d. įsakymo Nr. T1-1024 „Dėl Valstybinės akreditavimo sveikatos priežiūros veiklai tarnybos prie Sveikatos apsaugos ministerijos informacinės sistemos, Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos ir Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo