Suvestinė redakcija nuo 2022-07-01

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

Nauja redakcija nuo 2022-07-01:
Nr. T1-1871, 2022-06-06, paskelbta TAR 2022-06-06, i. k. 2022-12256

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, SVEIKATOS PRIEŽIŪROS TECHNOLOGIJŲ, SUSIJUSIŲ SU MEDICINOS PRIETAISAIS, VALDYMO INFORMACINĖS SISTEMOS IR LIETUVOS SVEIKATOS PRIEŽIŪROS SPECIALISTŲ KOMPETENCIJŲ PLATFORMOS 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, Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos ir Lietuvos sveikatos priežiūros specialistų kompetencijų platformos informacinės sistemos duomenų saugos nuostatus (pridedama).

2. S k i r i u Valstybinės akreditavimo sveikatos priežiūros veiklai tarnybos prie Sveikatos apsaugos ministerijos informacinės sistemos, Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos, Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos ir Lietuvos sveikatos priežiūros specialistų kompetencijų platformos informacinės sistemos saugos įgaliotinį – Duomenų ir dokumentų valdymo skyriaus patarėją Indrę Markauskienę.

3. 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 direktoriaus 2022 m. birželio 6 d. įsakymo Nr. T1-1871 redakcija)

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

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės akreditavimo sveikatos priežiūros veiklai tarnybos prie Sveikatos apsaugos ministerijos informacinės sistemos (toliau – VASPVT informacinė sistema), Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos (toliau – SPĮLIS), Sveikatos priežiūros technologijų, susijusių su medicinos prietaisais, valdymo informacinės sistemos (toliau – TechnoMedtas) ir Lietuvos sveikatos priežiūros specialistų kompetencijų platformos informacinės sistemos (toliau – Kompetencijų platforma) duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato šiose informacinėse sistemose tvarkomos elektroninės informacijos saugos (įskaitant kibernetinį saugumą) politiką, organizacinius ir techninius reikalavimus, reikalavimus personalui ir supažindinimo su saugos dokumentais principus.

2. Saugos nuostatuose vartojamos sąvokos atitinka teisės aktuose, nurodytuose šių Saugos nuostatų 12 punkte, vartojamas sąvokas.

3. Saugos nuostatais turi vadovautis VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos valdytojas, tvarkytojas, saugos įgaliotinis, duomenų valdymo įgaliotinis, administratorius ir šių informacinių sistemų naudotojai (toliau – naudotojai).

4. Elektroninės informacijos saugos užtikrinimo tikslai:

4.1. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

4.2. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

4.3. vykdyti elektroninės informacijos saugos incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

5. Elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. elektroninės informacijos saugos – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo – užtikrinimas;

5.2. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos kibernetinio saugumo užtikrinimas;

5.3. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos duomenims tvarkyti naudojamos techninės ir programinės įrangos kontrolė;

5.4. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos duomenų tvarkymo kontrolė;

5.5. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos veiklos tęstinumo užtikrinimas;

5.6. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos asmens duomenų apsauga;

5.7. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos naudotojų mokymas.

6. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos valdytoja ir asmens duomenų valdytoja – Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba prie Sveikatos apsaugos ministerijos (toliau - VASPVT) (A. Juozapavičiaus g. 9, LT-09311 Vilnius).

7. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos tvarkytoja – VASPVT (A. Juozapavičiaus g. 9, LT-09311 Vilnius).

8. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos ir asmens duomenų tvarkytoja – VASPVT (A. Juozapavičiaus g. 9, LT-09311 Vilnius).

9. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos valdytojas ir tvarkytojas atlieka šias funkcijas:

9.1. organizuoja VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos veiklą ir jai vadovauja;

9.2. tvirtina Saugos nuostatus, saugos politikos įgyvendinamuosius dokumentus, kitus dokumentus, susijusius su elektroninės informacijos sauga, ir jų pakeitimus;

9.3. priima sprendimą dėl VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

9.4. skiria VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos duomenų valdymo įgaliotinį, saugos įgaliotinį ir administratorių;

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

9.6. užtikrina saugos dokumentų ir kitų VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos valdytojo priimtų teisės aktų, susijusių su elektroninės informacijos sauga, tinkamą įgyvendinimą;

9.7. užtikrina nepertraukiamą VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos veiklą.

10. Saugos įgaliotinio funkcijos ir atsakomybė:

10.1. teikia VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos valdytojui siūlymus dėl:

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

10.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

10.1.3. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos saugos atitikties vertinimo atlikimo;

10.2. koordinuoja VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos elektroninės informacijos saugos incidentų tyrimą;

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

10.4. konsultuoja naudotojus VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos saugos klausimais;

10.5. atsako už VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos saugos politikos įgyvendinimo organizavimą;

10.6. organizuoja rizikos įvertinimą;

10.7. atlieka kitas Saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

11. Administratoriaus funkcijos ir atsakomybė:

11.1. įvertina, ar naudotojai yra pasirengę darbui;

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

11.3. administruoja ir užtikrina tinkamą VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos sudarančių komponentų (kompiuteriai, operacinės sistemos, duomenų bazių valdymo sistemos, taikomųjų programų sistemos, ugniasienės) veikimą, pažeidžiamų vietų ir saugos reikalavimų atitikties nustatymą;

11.4. informuoja saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia pasiūlymus dėl saugos užtikrinimo;

11.5. atsako už kompiuterių tinklo funkcionavimą;

11.6. atsako už VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos atsarginių duomenų kopijų darymą.

12. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos sauga užtikrinama vadovaujantis:

12.1. 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 (Bendrasis duomenų apsaugos reglamentas);

12.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

12.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

12.4. Lietuvos Respublikos valstybės informacinių išteklių įstatymu;

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

12.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas);

12.7. Techninių Valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas ir informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių Valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Techninių saugos reikalavimų aprašas);

12.8. Lietuvos standartais LST ISO / IEC 27001 ir LST ISO / IEC 27002, kitais Lietuvos ir tarptautiniais standartais, reglamentuojančiais informacijos saugą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d.

nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas) 10 punktu, VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos tvarkoma informacija priskiriama mažiausios svarbos elektroninės informacijos kategorijai.

14. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo 12.4 papunkčiu, VASPVT informacinės sistema, SPĮLIS, TechnoMedtas ir Kompetencijų platforma priskiriama ketvirtajai informacinių sistemų kategorijai.

15. Saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“ ir Nuostatų 12.8 papunktyje nurodytais standartais, ne rečiau kaip kartą per metus organizuoja VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos rizikos įvertinimą. Minėtą rizikos įvertinimą gali atlikti ir pats saugos įgaliotinis. Prireikus saugos įgaliotinis gali organizuoti neeilinį rizikos įvertinimą.

16. Rizikos vertinimo metu turi būti nustatomos grėsmės ir pažeidžiamumai, galintys turėti įtakos VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos saugai (kibernetiniam saugumui), nustatomos galimos grėsmių ir pažeidžiamumų poveikio vykdomai veiklai sritys, įvertinama pažeidimo grėsmių tikimybė ir galimos pasekmės, nustatomas rizikos lygis ir įvertinamos identifikuotos galimos grėsmės, kurios išdėstomos prioriteto tvarka pagal svarbą, kuri nustatoma atsižvelgiant į atliktą rizikos vertinimą. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos 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:

16.1. 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);

16.2. 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);

16.3. 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.

17. Atsižvelgdamas į rizikos įvertinimo ataskaitą, VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos 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.

18. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos 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.

19. Saugos užtikrinimo priemonės parenkamos, siekiant užtikrinti VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos veiklos tęstinumą, patiriant kuo mažiau išlaidų ir užtikrinant saugų informacinės sistemos darbą.

20. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos saugos atitikties vertinimas atliekamas vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių Valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“.

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

22. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos 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 nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

23. 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:

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

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

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

23.4. apsaugai naudojama programinė įranga privalo atsinaujinti ne rečiau kaip kartą per 16 valandų.

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

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

24.2. 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;

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

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

26. 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.

27. 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.

28. Stacionarūs, nešiojamieji naudotojų kompiuteriai ir mobilieji įrenginiai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos duomenys ir informacija. Stacionarūs, nešiojamieji kompiuteriai ir mobilieji įrenginiai, naudojimui ne VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos valdytojo patalpose, išduodami pasirašytinai.

29. Nešiojamuosiuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose turi būti naudojamas įjungimo slaptažodis.

30. Naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

31. Mobiliuosiuose įrenginiuose turi veikti apsauga, kad būtų galima išvengti neteisėtos prieigos prie duomenų, saugomų ir apdorojamų šiais įtaisais, pvz., naudojant įrenginio (išmaniojo telefono, planšetinio kompiuterio) atmintinės šifravimą ir tapatumo nustatymo priemones (PIN, slaptažodžiai, kriptografiniai raktai). Jei yra galimybė iš įrenginio prisijungti prie įstaigos informacinių sistemų, prisijungimai turi būti tinkamai sukonfigūruoti naudojant šifravimo priemones bei kitas technologijas, apsaugančias nuo galimybės pasinaudoti tokiu prisijungimu. Bet kuriuo atveju, įranga ir duomenų laikmenos neturėtų būti paliekamos be priežiūros viešose vietose ir neduodamos naudotis kitiems asmenims (pvz., vaikams).

32. Pagrindiniai atsarginių duomenų kopijų darymo ir atkūrimo reikalavimai:

32.1. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos atsarginės duomenų kopijos daromos automatiniu būdu kiekvieną dieną esant aktyviai VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos duomenų bazei;

32.2. kopijos įrašomos į informacijos kaupiklius, prie kurių priėjimą turi tik administratorius, jo nesant – administratorių pavaduojantis asmuo;

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

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

32.5. kopijų, iš kurių būtų galima atkurti duomenis, darymo ir saugojimo tvarka detaliai aprašyta VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos saugaus informacijos tvarkymo taisyklėse.

33. Informacinėse sistemose naudojamų svetainių saugos valdymo reikalavimai:

33.1. svetainių užkardos turi būti sukonfigūruotos taip, kad prie svetainių turinio valdymo sistemų (toliau – TVS) būtų galima jungtis tik iš vidinio informacinių sistemų tvarkytojo kompiuterinio tinklo arba nustatytų IP (angl. *Internet Protocol*) adresų;

33.2. turi būti pakeistos numatytos prisijungimo prie svetainių TVS ir administravimo skydų (angl. *Panel*) nuorodos (angl. *Default path*) ir slaptažodžiai;

33.3. turi būti užtikrinama, kad prie svetainių TVS ir administravimo skydų būtų galima jungtis tik naudojantis šifruotu ryšiu.

34. Tarnybinio el. pašto negalima naudoti didelių kiekių grafinių, audio bei video failų ar laiškų, nereikalingų tiesioginiam darbui ir nesusijusių su tarnybinių pareigų vykdymu, siuntimui.

35. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos valdytojo internetas ir el. paštas skirtas naudotis tik VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos valdytojo darbuotojams.

36. Išsiunčiamas bei gaunamas elektroninis paštas turi būti tikrinimas antivirusine programa, kuri turi būti nuolat atnaujinama.

37. El. pašto programa turi būti periodiškai atnaujinama, įdiegiamos jos gamintojo rekomenduojamos pataisos ar naujausia el. pašto programos versija.

38. Naudotojams draudžiama atidarinėti neaiškios kilmės gautų elektroninių laiškų priedus – ypač su vykdomųjų bylų išplėtimais (exe, scr, com, pif, vbs, bat, cmd, dll ir pan.). Jei įtartinas priedas gautas iš patikimo siuntėjo – būtina susisiekti su siuntėju (pageidautina – ne el. paštu) prieš bandant šį priedą atidaryti.

39. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos valdytojo patalpose belaidžiu tinklu nesinaudojama.

40. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos elektroninės informacijos saugos priemonės turi užtikrinti ir kitus Techninių saugos reikalavimų aprašo 5 punkte ir Kibernetinio saugumo reikalavimų apraše nurodytus reikalavimus, taikomus ketvirtosios kategorijos informacinėms sistemoms.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

41. 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.

42. Saugos įgaliotinis turi išmanyti saugos užtikrinimo principus, darbą su kompiuterių tinklais, turėti darbo su operacinėmis sistemomis, taikomosiomis programomis patirties. Savo darbe turi vadovautis Saugos nuostatų 12 punkte nurodytais teisės aktais.

43. Administratorius turi išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugą, išmanyti elektroninės informacijos saugos užtikrinimo principus. Administratorius privalo būti susipažinęs su duomenų bazių administravimo ir priežiūros pagrindais. Savo darbe turi vadovautis Saugos nuostatų 12 punkte nurodytais teisės aktais.

44. Naudotojai privalo turėti pagrindinius darbo kompiuteriu įgūdžius, būti susipažinę su šiais Saugos nuostatais, kitais saugos politiką reglamentuojančiais dokumentais bei teisės aktais, reglamentuojančiais asmens duomenų tvarkymą.

45. Saugos įgaliotinis ne rečiau kaip kartą per metus inicijuoja naudotojų mokymą elektroninės informacijos saugos ir kibernetinio saugumo klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problematiką.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

46. Naudotojų supažindinimą su šiais Saugos nuostatais bei kitais saugos politiką reglamentuojančiais dokumentais vykdo saugos įgaliotinis. Su minėtais dokumentais naudotojai supažindinami dokumentų valdymo sistemoje „Kontora“. Pakartotinai su minėtais dokumentais naudotojai supažindinami iš esmės pasikeitus saugos dokumentams.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

47. VASPVT informacinės sistemos, SPĮLIS, TechnoMedtas ir Kompetencijų platformos duomenų valdymo įgaliotinis, 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

2.
Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba prie Sveikatos apsaugos ministerijos, Įsakymas
Nr. T1-1871, 2022-06-06, paskelbta TAR 2022-06-06, i. k. 2022-12256
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