PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro
2021 m. rugpjūčio 30 d. įsakymu Nr.V-1959

SVEIKATOS PRIEŽIŪROS ĮSTAIGOS INFORMACINĖS SISTEMOS PAVYZDINĖS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Sveikatos priežiūros įstaigos (toliau – SPĮ) valdomos ir tvarkomos informacinės sistemos (toliau – IS) saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Taisyklės) tikslas – nustatyti elektroninės informacijos tvarkymo, techninius ir kitus elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus.

2. Taisyklėse vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas).

3. IS tvarkoma elektroninė informacija ir jos grupių sąrašas nurodomi SPĮ IS nuostatuose (toliau – Nuostatai), (pateikiamos nuorodos į konkrečius IS nuostatų punktus, kuriuose yra nurodyta IS tvarkoma elektroninė informacija).

4. Už IS esančios elektroninės informacijos, priskirtos _____ (įrašoma SPĮ IS duomenų saugos nuostatuose (toliau – Duomenų saugos nuostatai) nurodyta elektroninės informacijos svarbos kategorija) svarbos elektroninės informacijos kategorijai, tvarkymą yra atsakingi IS naudotojai ir IS administratoriai.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

5. Kompiuterinės įrangos saugos priemonės:

5.1. turi būti įdiegtos ir veikti automatizuotos įsibrovimo aptikimo sistemos, kurios stebėtų IS gaunamą ir išsiunčiamą duomenų srautą bei vidinį srautą tarp svarbiausių tinklo paslaugų;

5.2. _____ (įrašomos kitos naudojamos kompiuterinės įrangos saugos priemonės).

6. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

6.1. programinė įranga turi būti prižiūrima ir atnaujinama laikantis gamintojo reikalavimų ir rekomendacijų;

6.2. _____ (įrašomos kitos naudojamos sisteminės ir taikomosios programinės įrangos saugos priemonės.

7. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

7.1. kompiuterių tinklas turi būti atskirtas nuo viešųjų elektroninių ryšių tinklų (interneto) naudojant ugniasienes, automatinę įsilaužimų aptikimo ir prevencijos įrangą, atkirtimo nuo paslaugos, dedikuoto atkirtimo nuo paslaugos įrangą;

7.2. _____ (įrašomos kitos naudojamos elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės).

8. IS naudojamų svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumo ir kontrolės priemonės:

8.1. turi būti įgyvendinti atpažinties, tapatumo patvirtinimo ir naudojimosi IS saugumo ir kontrolės reikalavimai, nustatyti IS naudotojų administravimo taisyklėse;

8.2. _____ (įrašomos kitos naudojamos IS naudojamų svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumo ir kontrolės priemonės).

9. Pagrindinio IS tvarkytojo patalpų ir aplinkos saugumo užtikrinimo priemonės:

9.1. turi būti įrengta patalpų apsaugos signalizacija, kurios signalai turi būti persiunčiami patalpas saugančiai saugos tarnybai;

9.2. _____ (įrašomos kitos pagrindinio IS tvarkytojo patalpų ir aplinkos saugumo užtikrinimo priemonės).

10. Kitų (galimų) IS tvarkytojų patalpų ir aplinkos saugumo užtikrinimo priemonės:

10.1. visose patalpose, kuriose yra IS naudotojų ir IS techninė įranga, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

10.2. _____ (įrašomos kitos kitų (galimų) IS tvarkytojų patalpų ir aplinkos saugumo užtikrinimo priemonės).

11. Kitos priemonės, naudojamos IS elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti:

11.1. audito įrašų administravimas ir saugojimas: _____ (nurodoma, kokie duomenys yra kaupiami audito įrašuose (veiksmas, data, laikas, IP adresas etc.), taip pat nurodomos kitos priemonės, užtikrinančios audito įrašų administravimą ir saugojimą);

11.2. saugaus naudojimosi belaidžiu tinklu saugumo priemonės: _____ (nurodomos kitos saugaus naudojimosi belaidžiu tinklu saugumo priemonės).

12. IS veikimo užtikrinimas:

12.1. IS vienkartinis neveikimo (dėl incidentų, profilaktinių darbų, plėtros darbų ir kt.) laikotarpis negali būti ilgesnis nei __ val.;

12.2. IS prieinamumas turi būti užtikrintas ne mažiau kaip __ proc. laiko visą parą (IS neprieinamumo bendra trukmė per metus valandomis – iki __ val.).

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

13. Saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka:

13.1. elektroninė informacija į IS gali būti įvedama, joje keičiama, atnaujinama ir naikinama tik Taisyklių, Nuostatų, Duomenų saugos nuostatų ir kitų teisės aktų, reglamentuojančių IS veiklą ir elektroninės informacijos tvarkymą, nustatyta tvarka;

13.2. elektroninė informacija gali būti tvarkoma pagal IS naudotojams ir IS administratoriams suteiktas prieigos teises ir tik turint teisėtą tikslą ir pagrindą;

13.3. visi IS naudotojų veiksmai registruojami Taisyklių __ papunktyje nustatyta tvarka;

13.4. IS naudotojui neatliekant jokių veiksmų __ minučių, IS taikomoji programinė įranga turi užsirakinti, kad toliau naudotis IS galima būtų tik pakartotinai atlikus savo tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

13.5. baigus darbą ar IS naudotojui pasitraukus iš darbo vietos, turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo IS, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai ar jų kopijos darbo vietoje turi būti padedami į pašaliniams asmenims neprieinamą vietą;

13.6. IS turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo, patikimumo tikrinimo ir informavimo apie klaidas priemones.

14. Atsarginių elektroninės informacijos kopijų darymas, saugojimas, elektroninės informacijos atkūrimo iš atsarginių elektroninės informacijos kopijų išbandymas vykdomas vadovaujantis IS tvarkytojo tvirtinamais atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių elektroninės informacijos kopijų tvarkos aprašais, kuriuose nurodomi atsakingi už duomenų kopijų darymą, apsaugą, saugojimo kontrolę ir duomenų atkūrimą iš atsarginių duomenų kopijų asmenys, kas kiek laiko yra atliekami atkūrimo iš atsarginių kopijų bandymai, kur saugomos kopijos ir kaip užtikrinamas jų konfidencialumas (šifravimas ar fizinės saugos priemonės), kopijų darymo būdas (angl. *full backup, incremental, differential*). Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių elektroninės informacijos kopijų tvarka gali būti nurodoma ir šiame dokumente.

15. Elektroninė informacija perkeliama ir teikiama susijusiems registrams ir (ar) kitoms informacinėms sistemoms ir iš jų gaunama vadovaujantis Nuostatuose nustatyta tvarka ir sąlygomis.

16. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo, perdavimo ar kitokios neteisėtos veiklos (toliau – neteisėta veikla) nustatymo tvarka:

16.1. siekiant nustatyti, ar su IS elektronine informacija nėra vykdoma neteisėta veikla, visi elektroniniuose įvykių žurnaluose saugomi įrašai turi būti analizuojami ne rečiau kaip kartą per savaitę, taip pat nurodomas asmuo, atsakingas už įvykių žurnalų analizę. Siekiant nustatyti, ar su IS elektronine informacija nėra vykdoma neteisėta veikla, visi elektroniniuose įvykių žurnaluose saugomi įrašai turi būti analizuojami ne rečiau kaip kartą per savaitę, taip pat nurodomas asmuo, atsakingas už įvykių žurnalų analizę;

16.2. IS naudotojai, pastebėję Taisyklėse, Duomenų saugos nuostatuose, Taisyklėse, SPĮ IS veiklos tęstinumo valdymo plane nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo priemones, įvykius ar veiką, atitinkančią kibernetinio ar elektroninės informacijos saugos incidento požymius, arba apie tai gavę informacijos iš kitų informacijos šaltinių, privalo nedelsdami pranešti apie tai administratoriui, IS tvarkytojo saugos įgaliotiniui arba, jeigu IS tvarkytojo organizacijoje įsteigta informacinių technologijų pagalbos tarnyba, šiai tarnybai;

16.3. IS tvarkytojo saugos įgaliotinis, įtaręs, kad su elektronine informacija, tvarkoma IS, vykdoma neteisėta veikla, inicijuoja elektroninės informacijos saugos ir kibernetinių incidentų valdymo procedūras.

17. IS programinės ir techninės įrangos keitimo, IS pokyčių valdymo tvarka nustatoma SPĮ IS pokyčių valdymo tvarkos apraše. IS pokyčių valdymo tvarka gali būti išdėstyta ir šiame dokumente.

18. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių (toliau kartu – mobilieji įrenginiai) naudojimo tvarka:

18.1. jeigu prie IS jungiamasi per IS infrastruktūroje esančius tarpinius įrenginius, šie įrenginiai turi atitikti šiuos reikalavimus: _____ (įrašomi reikalavimai, kurie turi būti užtikrinami, jeigu prie IS jungiamasi per IS infrastruktūroje esančius tarpinius įrenginius);

18.2. jeigu prie IS iš mobiliųjų įrenginių jungiamasi tiesiogiai, turi būti įgyvendinti šie reikalavimai:

18.2.1. mobiliesiems įrenginiams, naudojamiems IS valdytojo ar IS tvarkytojo patalpose, esantiems vidiniame IS tvarkytojo kompiuterių tinkle, taikomi tokie patys elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai kaip ir stacionariesiems kompiuteriams;

18.2.2. _____ (įrašomi kiti reikalavimai, kurie turi būti užtikrinami, jeigu prie IS iš mobiliųjų įrenginių jungiamasi tiesiogiai).

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

19.1. elektroninei informacijai teikti ir (ar) gauti gali būti naudojamas Saugus valstybinis duomenų perdavimo tinklas;

19.2. _____ (įrašomi kiti metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą).

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINEI SISTEMAI FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

20. IS funkcionuoti reikalingų paslaugų, darbų ir (ar) įrangos tiekėjas (toliau – tiekėjas) turi atitikti IS veiklą reglamentuojančių teisės aktų, standartų, Taisyklių reikalavimus ir paslaugų teikimo, darbų atlikimo ar įrangos tiekimo pirkimo dokumentuose iš anksto nustatomus tiekėjo kompetencijos, patirties, teikiamų paslaugų, atliekamų darbų ar tiekiamos įrangos reikalavimus.

21. Perkant paslaugas, darbus ar įrangą, susijusius su IS, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi būti nustatoma, kad tiekėjas užtikrina atitiktį Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, nustatytiems reikalavimams. Perkamos paslaugos, darbai ar įranga, susiję su IS, turi atitikti teisės aktų ir standartų, kuriais vadovaujamasi užtikrinant IS elektroninės informacijos saugą ir kibernetinį saugumą, reikalavimus, kurie iš anksto nustatomi paslaugų teikimo, darbų atlikimo ar įrangos tiekimo pirkimo dokumentuose.

22. Tiekėjas, vykdydamas sutartinius įsipareigojimus, turi įgyvendinti tinkamas organizacines ir technines priemones, skirtas IS ir jose tvarkomai elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

23. Tiekėjui prieiga prie IS gali būti suteikiama tik pasirašius sutartį, kurioje turi būti nustatytos tiekėjo teisės, pareigos, prieigos prie informacinių sistemų lygiai ir sąlygos, elektroninės informacijos saugos, kibernetinio saugumo, konfidencialumo reikalavimai ir atsakomybė už jų nesilaikymą. IS saugos įgaliotinis turi supažindinti tiekėją su suteiktos prieigos IS saugos ir kibernetinio saugumo reikalavimais ir sąlygomis. IS saugos administratorius yra atsakingas už prieigos prie IS tiekėjui suteikimą ir panaikinimą pasirašius sutartį, pasibaigus sutarties su tiekėju galiojimo terminui ar kitais sutartyje nurodytais prieigos prie IS panaikinimo atvejais.

24. Tiekėjui suteikiamas tik toks prieigos prie IS lygmuo, kuris yra būtinas sutartyje nustatytiems įsipareigojimams vykdyti. Tiekėjo paskirti specialistai turi pasirašyti konfidencialumo pasižadėjimus.

25. Iškilus poreikiui, siekiant įsitikinti, ar tinkamai vykdoma sutartis, laikomasi elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų, IS tvarkytojas turi teisę atlikti tiekėjo teikiamų paslaugų stebėseną ir auditą, suteikti galimybę atlikti auditą trečiosioms šalims.

26. Tiekėjas privalo nedelsdamas informuoti IS tvarkytoją apie sutarties vykdymo metu pastebėtus elektroninės informacijos saugos ar kibernetinius incidentus, pastebėtas neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos ir (ar) kibernetinio saugumo užtikrinimo priemones, elektroninės informacijos saugos ir (ar) kibernetinio saugumo reikalavimų nesilaikymą, nusikalstamos veikos požymius, saugumo spragas, pažeidžiamumus, kitus svarbius saugai įvykius.

27. IS tvarkytojas su interneto paslaugų teikėju (-ais) turi būti sudaręs sutartis dėl apsaugos nuo IS elektroninių paslaugų trikdymo taikymo (angl. *denial of service*), reagavimo į elektroninės informacijos saugos ir kibernetinius incidentus įprastomis darbo valandomis ir po darbo valandų, nepertraukiamo interneto paslaugos teikimo ir interneto paslaugos sutrikimų registravimo 24 valandas per parą, 7 dienas per savaitę.

_____