PATVIRTINTA
Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. rugsėjo 28 d.
įsakymu Nr. V-1082
(Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. d.
įsakymo Nr.
redakcija)

VAIKŲ SVEIKATOS STEBĖSENOS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Vaikų sveikatos stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Informacijos tvarkymo taisyklės) tikslas – sudaryti sąlygas saugiai tvarkyti Vaikų sveikatos stebėsenos informacinės sistemos (toliau – Informacinė sistema) elektroninę informaciją ir užtikrinti kibernetinį saugumą.

2. Informacijos tvarkymo taisyklės parengtos vadovaujantis Saugos dokumentų turinio 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 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“ ir 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“.

3. Informacinės sistemos duomenų bazėje tvarkomi Informacinės sistemos duomenys, nurodyti Vaikų sveikatos stebėsenos informacinės sistemos nuostatų, patvirtintų Lietuvos Respublikos sveikatos apsaugos ministro 2015 m. birželio 22 d. įsakymu Nr. V-780 „Dėl Vaikų sveikatos stebėsenos informacinės sistemos nuostatų ir duomenų saugos nuostatų patvirtinimo“ (toliau – Informacinės sistemos nuostatai) 15–17 punktuose.

4. 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“, 8.1 ir 8.2 papunkčiais, Informacinėje sistemoje tvarkoma informacija, kuri priskiriama prie svarbios informacijos kategorijos.

5. Informacijos tvarkymo taisyklės privalomos Informacinės sistemos valdytojui, Informacinės sistemos tvarkytojui, Informacinės sistemos naudotojams, Informacinės sistemos administratoriui bei saugos įgaliotiniui. Už Informacijos tvarkymo taisyklių įgyvendinimo

organizavimą ir kontrolę atsako Informacinės sistemos saugos įgaliotinis. Už Informacinės sistemos elektroninės informacijos tvarkymą atsakingi:

5.1. Informacinės sistemos naudotojai, dirbantys Higienos institute, – už duomenų, nurodytų Informacinės sistemos nuostatų 17 punkte, tvarkymą;

5.2. Informacinės sistemos visuomenės sveikatos specialistai – už duomenų, nurodytų Informacinės sistemos nuostatų 15, 16 punktuose, tvarkymą;

5.3. Informacinės sistemos administratorius – už duomenų, nurodytų Informacinės sistemos nuostatų 15–17 punktuose, tvarkymą, už Informacinės sistemos administravimą, duomenų bazių atkūrimą ir priežiūrą, prieinamumo užtikrinimą, klasifikatorių tvarkymą.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

6. Kompiuterinės įrangos saugos priemonės turi atitikti reikalavimus:

6.1. Informacinės sistemos tarnybinės stotys ir kompiuterinė įranga turi įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį Informacinės sistemos tarnybinių stočių veikimą ne mažiau kaip 30 minučių;

6.2. Informacinės sistemos tarnybinėse stotyse ir Higienos instituto (toliau – Informacinės sistemos tvarkytojo) kompiuterizuotose darbo vietose įdiegta ir reguliariai atnaujinama virusų ir kenkėjiško kodo aptikimo ir šalinimo programinė įranga, skirta kompiuteriams ir laikmenoms tikrinti;

6.3. apsaugai naudojama programinė įranga automatiškai elektroniniu paštu informuoja Informacinės sistemos administratorių apie Informacinės sistemos tvarkytojo naudotojų kompiuterizuotas darbo vietas ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 12 valandų;

6.4. Informacinės sistemos neveikimo laikotarpis negali būti ilgesnis nei 12 valandų;

6.5. vidinių informacinės sistemos naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga. Informacinės sistemos saugos įgaliotinis turi parengti, su Informacinės sistemos valdytojo vadovu suderinti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti leistinos programinės įrangos sąrašą;

6.6. Informacinės sistemos techninė ir programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

6.7. svarbiausia kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima;

6.8. patekimas prie Informacinės sistemos naudotojų darbo vietų yra kontroliuojamas: stacionariais kompiuteriais, turinčiais prieigą prie Informacinės sistemos, galima naudotis tik Informacinės sistemos tvarkytojo patalpose;

6.9. prieiga prie Informacinės sistemos virtualių mašinų yra kontroliuojama prieigos teises suteikiant tik Informacinės sistemos administratoriui arba kitam įgaliotam asmeniui;

6.10. svarbiausia kompiuterinė įranga dubliuojama, jos techninė būklė nuolat stebima;

6.11. svarbiausios kompiuterinės įrangos gedimai registruojami elektroniniame žurnale. Už gedimų registravimą atsakingas Informacinės sistemos administratorius.

7. Sisteminės ir taikomosios programinės įrangos saugos priemonės turi atitikti reikalavimus:

7.1. Informacinės sistemos tarnybinėse stotyse ir Informacinės sistemos naudotojų kompiuteriuose naudojama tik legali, Informacinės sistemos funkcijoms vykdyti būtina programinė įranga;

7.2. operatyviai įdiegiami Informacinės sistemos tarnybinių stočių ir pagrindinio Informacinės sistemos tvarkytojo kompiuterizuotų darbo vietų kompiuterinės įrangos, operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

7.3. programinės įrangos diegimą, šalinimą ir konfigūravimą turi teisę atlikti tik Informacinės sistemos administratorius arba kitas įgaliotas asmuo;

7.4. Informacinės sistemos tarnybinėse stotyse įrašomi ir saugomi duomenys apie Informacinės sistemos tarnybinių stočių ir taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis Informacinės sistemos tarnybinėse stotyse, kitus saugai svarbius įvykius, nurodant naudotojo identifikatorių ir įvykio laiką. Šie duomenys analizuojami ne rečiau kaip kartą per savaitę;

7.5. fiksuojami Informacinės sistemos naudotojų, kuriems suteikta teisė tvarkyti Informacinės sistemos duomenis, veiksmai;

7.6. programinei įrangai testuoti naudojama atskira testavimo aplinka;

7.7. Informacinės sistemos tinkle įdiegtos automatinės įsilaužimo aptikimo sistemos;

7.8. pagrindinėse Informacinės sistemos tarnybinėse stotyse turi būti naudojamos vykdomo kodo kontrolės priemonės, automatiškai apribojančios ar informuojančios apie neautorizuoto programinio kodo vykdymą.

8. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės turi atitikti reikalavimus:

8.1. Informacinės sistemos tarnybinės stotys, Informacinės sistemos tvarkytojo naudotojų kompiuterizuotos darbo vietos ir kita kompiuterinė įranga, įjungta į elektroninės informacijos perdavimo tinklą, yra atskirta nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai reguliariai analizuojami;

8.2. viešaisiais ryšių tinklais perduodamos Informacinės sistemos elektroninės informacijos konfidencialumas užtikrinamas naudojant šifravimą, virtualų privatų tinklą (VPN), skirtines linijas, saugų elektroninių ryšių tinklą;

8.3. Informacinės sistemos programinė įranga apsaugota nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*);

8.4. Informacinės sistemos tinklo perimetro apsaugai naudojami filtrai, apsaugantys viešame ryšių tinkle naršančių Informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

8.5. prisijungimai viešaisiais ryšių tinklais prie Informacinės sistemos leidžiami tik iš nustatytų IP adresų;

8.6. nuotolinis prisijungimas prie informacinės sistemos turi būti vykdomas protokolu, skirtu duomenų šifravimui;

8.7. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę. Ugniasienės įvykių žurnalai (angl. *Logs*) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

8.8. viešaisiais ryšių tinklais perduodamos Informacinės sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualų privatų tinklą (angl. *virtual private network*), skirtines linijas, saugų elektroninių ryšių tinklą ar kitas priemones.

9. Patalpų ir aplinkos saugumo užtikrinimo priemonės turi atitikti reikalavimus:

9.1. patalpos atitinka priešgaisrinės saugos reikalavimus, yra gaisro gesinimo priemonės;

9.2. patalpos atskirtos nuo bendrojo naudojimo patalpų, asmenys, nesusiję su Informacinės sistemos tvarkymu, patekti į šias patalpas gali tik lydimi Informacinės sistemos administratoriaus;

9.3. veikia patekimo į patalpas kontrolės sistema;

9.4. patalpose naudojami nepertraukiamo elektros maitinimo šaltiniai;

9.5. patekimas į Informacinės sistemos tarnybinių stočių patalpas ir patalpas, kuriose saugomos atsarginės kopijos, turi būti kontroliuojamas šiose taisyklėse nustatyta tvarka.

10. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

10.1. Informacinės sistemos duomenų bazės veiksmų žurnale fiksuojami elektroninės informacijos pakeitimą atlikusio Informacinės sistemos naudotojo duomenys ir pakeitimo laikas;

10.2. kiekvienas naudotojas, prieš naudodamasis Informacine sistema, savo tapatybę patvirtina slaptažodžiu;

10.3. kiekvienam naudotojui Informacinėje sistemoje suteikiamos tik tiesioginėms pareigoms vykdyti būtinos teisės;

10.4. baigus darbą imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama, uždaroma programinė įranga, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą;

10.5. Informacinės sistemos naudotojui neatliekant jokių veiksmų Informacinėje sistemoje 15 minučių, Informacinės sistemos taikomoji programinė įranga automatiškai užsirakina ir naudotis Informacine sistema galima tik pakartotinai patvirtinus savo tapatybę;

10.6. Informacinės sistemos naudotojų darbo vietose naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (USB, CD/DVD ir kt.);

10.7. išorinėje duomenų laikmenoje teikiami asmens duomenys ir sveikatos asmens duomenys šifruojami arba naudojamos kitos saugos priemonės, užtikrinančios, kad asmens duomenys ir sveikatos asmens duomenys bus perduoti saugiai ir nebus galimybės tretiesiems asmenims jais pasinaudoti;

10.8. išoriniais duomenų perdavimo tinklais perduodami asmens duomenys ir sveikatos asmens duomenys šifruojami;

10.9. saugos atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip;

10.10. per metus turi būti užtikrintas Informacinės sistemos prieinamumas: ne mažiau kaip 96 proc. laiko visą parą.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

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

11.1. Informacinės sistemos duomenis įrašyti, keisti, atnaujinti ir naikinti turi teisę tik Informacinės sistemos naudotojai pagal nustatytas prieigos teises;

11.2. administravimo posistemyje tvarkomus duomenis įvesti, keisti, atnaujinti ar naikinti turi teisę tik Informacinės sistemos administratorius;

11.3. Informacinės sistemos duomenys įvedami, atnaujinami, keičiami ir naikinami Informacinės sistemos nuostatuose nustatyta tvarka;

11.4. duomenų įvedimas, pakeitimas, atnaujinimas ir naikinimas registruojami Informacinės sistemos duomenų bazės veiksmų žurnale, nurodant Informacinės sistemos naudotoją, prisijungimo datą, laiką ir atliktus veiksmus. Šie įrašai prieinami tik Informacinės sistemos administratoriui ir saugomi ne trumpiau nei 1 metus.

12. Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka:

12.1. Informacinės sistemos duomenų kopijos automatiniu būdu, esant aktyviai Informacinės sistemos duomenų bazei, daromos kiekvieną darbo dieną. Atsarginės Informacinės sistemos duomenų kopijos saugomos kitoje patalpoje nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota;

12.2. prarasti, iškraipyti ar sunaikinti Informacinės sistemos duomenys turi būti atkuriami iš Informacinės sistemos duomenų atsarginių kopijų. Už Informacinės sistemos duomenų atkūrimą iš atsarginių duomenų kopijų atsakingas paslaugų teikėjas, su kuriuo sudaryta Virtualių serverių nuomos sutartis. Nutraukus Virtualių serverių nuomos sutartį, už Informacinės sistemos duomenų atkūrimą iš atsarginių duomenų kopijų atsakingas Informacinės sistemos administratorius;

12.3. informacija apie elektroninės informacijos kopijavimą (kopijos įrašymo data ir laikas) automatiškai fiksuojama ir saugoma Informacinės sistemos tarnybinės stoties veiksmų žurnale.

13. Saugaus elektroninės informacijos perkėlimo ir teikimo susijusioms informacinėms sistemoms, elektroninės informacijos gavimo iš jų tvarka:

13.1. duomenys iš susijusių registrų ir informacinių sistemų gaunami ir jiems teikiami šių registrų ir informacinių sistemų valdytojų ir Informacinės sistemos tvarkytojo sudarytose duomenų teikimo ir gavimo sutartyse numatyta tvarka;

13.2. Informacinės sistemos duomenys kitai informacinei sistemai perduodami laikantis Informacinės sistemos nuostatuose, Informacinės sistemos saugos politiką įgyvendinančiuose dokumentuose nurodytų reikalavimų;

13.3. duomenų teikėjai duomenis Informacinei sistemai teikia Informacinės sistemos nuostatų nustatyta tvarka;

13.4. už duomenų, gaunamų iš susijusių registrų ir kitų informacinių sistemų, atnaujinimo procesą Informacinėje sistemoje yra atsakingas Informacinės sistemos administratorius.

14. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) nustatymo tvarka:

14.1. Informacinės sistemos naudotojai, pastebėję neteisėtos veiklos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai Informacinės sistemos administratoriui;

14.2. Informacinės sistemos administratorius apie saugos pažeidimus informuoja saugos įgaliotinį, imasi visų įmanomų veiksmų neteisėtai veiklai užkirsti bei išnagrinėja Informacinės sistemos duomenų bazės veiksmų žurnalo įrašus, siekiant nustatyti neteisėtos veiklos šaltinį, laiką ir veiksmus;

14.3. saugos įgaliotinis, gavęs pranešimą apie vykdomą neteisėtą veiklą, inicijuoja elektroninės informacijos saugos incidento valdymo veiksmus, kurie aprašyti Vaikų sveikatos stebėsenos informacinės sistemos veiklos tęstinumo valdymo plane.

15. Informacinės sistemos programinės ir techninės įrangos keitimo ir atnaujinimo (toliau – pokyčiai) tvarka:

15.1. visi pokyčiai (projektavimas, kūrimas, testavimas, diegimas) atliekami Informacinės sistemos tvarkytojo ir (ar) Informacinės sistemos valdytojo iniciatyva, sprendimą priima Informacinės sistemos valdytojas;

15.2. pokyčių projektavimą ir kūrimą atlieka Higienos instituto direktoriaus paskirti atsakingi darbuotojai arba įstatymų nustatyta tvarka pasirinkti paslaugų tiekėjai tam skirtoje kūrimo aplinkoje. Atsakomybė už pokyčių įgyvendinimo sprendimus nustatoma pokyčių projektavimo ir kūrimo dokumentacijoje;

15.3. prieš atliekant keitimus, kurių metu gali iškilti grėsmė Informacinės sistemos elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, visi pakeitimai turi būti išbandomi testavimo aplinkoje;

15.4. įgyvendinant pokyčius, kurių metu galimi Informacinės sistemos veikimo sutrikimai, Informacinės sistemos administratorius privalo ne vėliau kaip prieš vieną darbo dieną iki planuojamų pokyčių vykdymo pradžios informuoti (elektroniniu paštu, faksu ar kitomis priemonėmis) Informacinės sistemos naudotojus apie tokių darbų pradžią ir galimus sutrikimus;

15.5. atlikęs pokyčių testavimą arba jei testavimo darbų dėl programinių ir (ar) techninių priežasčių nebuvo galima atlikti, Informacinės sistemos administratorius gali pradėti įgyvendinti pokyčius;

15.6. jeigu testavimas sėkmingas, pokyčiai perkeliami į gamybinę aplinką;

15.7. visi pokyčiai registruojami ir prireikus apie tai informuojami Informacinės sistemos naudotojai;

15.8. Informacinės sistemos administratorius Informacinės sistemos naudotojams privalo pateikti visą reikalingą informaciją apie naudojimosi Informacine sistema pakitimus, kurie yra susiję su jų atliekamomis funkcijomis ir kurių atsiradimas susijęs su įvykdytais arba vykdomais pokyčiais;

15.9. Informacinė sistema turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones.

16. Nešiojamųjų kompiuterių naudojimo tvarka:

16.1. nešiojamieji kompiuteriai skirti savivaldybių visuomenės sveikatos biurų specialistams, tvarkantiems Informacinės sistemos duomenis, nurodytus Informacinės sistemos Nuostatų 15, 16 punktuose;

16.2. nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis;

16.3. nešiojamųjų kompiuterių nenaudojant, jie turi būti saugomi saugioje vietoje.

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

17. Reikalavimai Informacinei sistemai funkcionuoti reikalingoms paslaugoms (projektavimo, aptarnavimo ir priežiūros) ir jų teikėjams nustatomi šių paslaugų teikimo sutartyse.

18. Paslaugos teikėjas, teikiantis Virtualių serverių nuomos paslaugą, atsakingas už Informacinės sistemos kompiuterinės įrangos saugos priemonių įgyvendinimą, tarnybinių stočių patalpų ir aplinkos saugumą, rezervinių duomenų kopijų darymą ir duomenų atkūrimą jų praradimo atveju.

19. Informacinės sistemos administratorius suteikia prieigos prie Informacinės sistemos duomenų teisę (peržiūrėti Informacinės sistemos duomenis, atlikti užklausas Informacinėje sistemoje, vykdyti veiksmus su Informacinės sistemos duomenimis ir kt.), fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotiems asmenims paslaugų teikimo sutartyje nurodytam laikotarpiui jų nustatytoms funkcijoms atlikti.

20. Perkant paslaugas, darbus ar įrangą, susijusią su informacine sistema, pirkimo dokumentuose turi būti iš anksto nustatyta, kad paslaugos teikėjas turi užtikrinti atitiktį kibernetinio saugumo reikalavimams, nustatytiems 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“.

21. Prieš suteikiant trečiosioms šalims loginę arba fizinę prieigą prie Informacinės sistemos resursų, saugos įgaliotinis organizuoja trečiųjų šalių atstovų informavimą apie taikytinus informacijos saugumo reikalavimus ir atsakomybę.

22. Pasibaigus paslaugų teikimo sutartyje nurodytam laikotarpiui, Informacinės sistemos administratorius panaikina paslaugų teikėjo įgaliotų asmenų prieigos prie Informacinės sistemos programinių, techninių ir kitų resursų teisę ir apie tai juos informuoja.

_____