

PATVIRTINTA

Lietuvos Respublikos sveikatos apsaugos
ministro 2010 m. balandžio 21 d.

įsakymu Nr. V-308

(Lietuvos Respublikos sveikatos apsaugos
ministro 2014 m. d.

įsakymo Nr. redakcija)

**LIETUVOS RESPUBLIKOS PROFESINIŲ LIGŲ VALSTYBĖS REGISTRO SAUGAUS
ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS**

**I SKYRIUS
BENDROSIOS NUOSTATOS**

1. Lietuvos Respublikos profesinių ligų valstybės registro saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Informacijos tvarkymo taisyklės) tikslas – sudaryti sąlygas saugiai tvarkyti Lietuvos Respublikos profesinių ligų valstybės registro (toliau – Registras) elektroninę informaciją.

2. Registro duomenų bazėje tvarkomi ir kaupiami Registro objektų duomenys, nurodyti Lietuvos Respublikos profesinių ligų valstybės registro nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 1994 m. lapkričio 30 d. nutarimu Nr. 1198 „Dėl profesinių ligų sąrašo ir Lietuvos Respublikos profesinių ligų valstybės registro bei jo nuostatų“ (toliau – Registro nuostatai) 15 punkte.

3. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo 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 Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ 4.2. papunkčiu, Registre tvarkoma elektroninė informacija priskiriama antrai elektroninės informacijos svarbos kategorijai.

4. Informacijos tvarkymo taisyklės privalomos Registro naudotojams, Registro valdytojui, Registro tvarkytojui, Registro administratoriui bei saugos įgaliotiniui. Už Informacijos tvarkymo taisyklių įgyvendinimo organizavimą ir kontrolę atsako Registro saugos įgaliotinis. Už Registro elektroninės informacijos tvarkymą atsakingi:

4.1. Registro naudotojai, dirbantys Higienos institute – už duomenų, nurodytų Registro nuostatų 15 punkte tvarkymą;

4.2. Registro administratorius – už Registro administravimą, duomenų bazių atkūrimą ir priežiūrą, prieinamumo užtikrinimą, klasifikatorių tvarkymą.

5. Informacijos tvarkymo taisyklėse vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše ir Saugos dokumentų turinio gairių apraše, patvirtintuose 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“, Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose 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“, Registro nuostatuose, Lietuvos Respublikos profesinių ligų valstybės registro duomenų saugos nuostatuose,

patvirtintuose Lietuvos Respublikos sveikatos apsaugos 2009 m. spalio 8 d. įsakymu Nr. V-850 „Dėl Lietuvos Respublikos profesinių ligų valstybės registro duomenų saugos nuostatų patvirtinimo“ (toliau – Registro duomenų saugos nuostatai), kituose Lietuvos Respublikos įstatymuose ir teisės aktuose.

II SKYRIUS

TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

6. Vadovaujantis Higienos instituto, paslaugų gavėjo, ir VĮ Registrų centro, paslaugų teikėjo, 2014 m. sausio 20 d. virtualių serverių nuomos sutartimi Nr. SGS-11 (toliau – Virtualių serverių nuomos sutartis), Registro programinė įranga patalpinta VĮ Registrų centro tarnybinių stočių patalpose. Paslaugos teikėjas atsakingas už Registro kompiuterinės įrangos saugos priemonių įgyvendinimą, tarnybinių stočių patalpų ir aplinkos saugumą, rezervinių duomenų kopijų darymą ir duomenų atkūrimą jų praradimo atveju.

7. Kompiuterinės įrangos saugos priemonės:

7.1. Registro tarnybinės stotys ir kompiuterinė įranga turi įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį Registro tarnybinių stočių veikimą 2,5 val.;

7.2. Registro tarnybinėse stotyse ir Higienos instituto (toliau – Registro tvarkytojo) kompiuterizuotose darbo vietose įdiegta ir reguliariai atnaujinama virusų ir kenkėjiško kodo aptikimo ir šalinimo programinė įranga, skirta kompiuteriams ir laikmenoms tikrinti. Už Registro naudotojų, dirbančių kitose įstaigose, kompiuterių apsaugą nuo kenksmingos programinės įrangos atsako tų įstaigų vadovų paskirti atsakingi asmenys;

7.3. apsaugai naudojama programinė įranga automatiškai elektroniniu paštu informuoja Registro administratorių apie Registro tvarkytojo naudotojų kompiuterizuotas darbo vietas ir tarnybines stotis, kuriose apsaugos sistema netinkamai funkcionuoja, yra išjungta arba neatsinaujino per 24 valandas;

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

7.5. prieiga prie Registro virtualių mašinų yra kontroliuojama prieigos teisės suteikiant tik Registro administratoriui arba kitam įgaliotam asmeniui;

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

7.6. svarbiausios kompiuterinės įrangos gedimai registruojami elektroniniame žurnale. Už gedimų registravimą atsakingas Registro administratorius;

7.7. svarbiausia kompiuterinė įranga dubliuota ir jos techninė būklė nuolat stebima.

8. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

8.1. Registro tarnybinėse stotyse ir Registro naudotojų kompiuteriuose naudojama tik legali, Registro funkcijoms vykdyti būtina programinė įranga;

8.2. operatyviai įdiegiami Registro tarnybinių stočių ir pagrindinio Registro tvarkytojo kompiuterizuotų darbo vietų kompiuterinės įrangos, operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai. Už Registro naudotojų, dirbančių kitose įstaigose, kompiuterių operacinių sistemų apsaugą atsako įstaigų, kuriose jie dirba, vadovų paskirti atsakingi darbuotojai;

8.3. programinės įrangos diegimą, šalinimą ir konfigūravimą turi teisę atlikti tik Registro administratorius arba kitas įgaliotas asmuo;

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

8.5. fiksuojami Registro naudotojų, kuriems suteikta teisė tvarkyti Registro duomenis, veiksmai;

8.6. programinės įrangos testavimui naudojama atskira testavimo aplinka;

8.7. Registro informacinės sistemos tinkle įdiegtos automatinės įsilaužimo aptikimo sistemos.

9. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

9.1. Registro tarnybinės stotys, Registro 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;

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

9.3. Registro 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);

9.4. Registro tinklo perimetro apsaugai naudojami filtrai, apsaugantys viešame ryšių tinkle naršančių Registro naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

9.5. prisijungimai viešaisiais ryšių tinklais prie Registro sistemos leidžiami tik iš nustatytų IP adresų.

10. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

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

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

10.3. kiekvienam naudotojui Registro 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, įjungžiama ekrano užsklanda su slaptažodžiu, dokumentai padedami į pašaliniams asmenims neprieinamą vietą;

10.5. Registro naudotojui neatliekant jokių veiksmų Registre, Registro taikomoji programinė įranga automatiškai užsirakina ir naudotis Registru galima tik pakartotinai patvirtinus savo tapatybę;

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

III SKYRIUS

SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

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

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

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

11.3. Registro duomenys įvedami, atnaujinami, keičiami ir naikinami turint teisėtą pagrindą;

11.4. duomenų įvedimas, pakeitimas, atnaujinimas ir naikinimas registruojami Registro duomenų bazės veiksmų žurnale, nurodant Registro naudotoją, prisijungimo datą, laiką ir atliktus veiksmus. Šie įrašai prieinami tik Registro 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. už Registro duomenų ir virtualių serverių kopijų darymą atsakingas paslaugų teikėjas, su kuriuo sudaryta Virtualių serverių nuomos sutartis. Nutraukus Virtualių serverių nuomos sutartį, už Registro duomenų ir virtualių serverių kopijų darymą atsakingas Registro administratorius;

12.2. Registro duomenų kopijos automatiškai būdu daromos reguliariai, kartą per parą. Kartą per savaitę daromos atsarginės Registro duomenų kopijos, kurios saugomos kitoje patalpoje nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota;

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

12.4. informacija apie elektroninės informacijos kopijavimą (kopijos įrašymo data ir laikas) automatiškai fiksuojama ir saugoma Registro 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 Registro tvarkytojo sudarytose duomenų teikimo ir gavimo sutartyse numatyta tvarka;

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

13.3. duomenų teikėjai duomenis Registrui teikia Registro nuostatų nustatyta tvarka;

13.4. už duomenų, gaunamų iš susijusių registrų ir kitų informacinių sistemų, atnaujinimo procesą Registre yra atsakingas Registro administratorius.

14. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

14.1. Registro naudotojai, pastebėję duomenų neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai Registro administratoriui;

14.2. Registro administratorius apie saugos pažeidimus informuoja saugos įgaliotinį, imasi visų įmanomų veiksmų neteisėtai veiklai užkirsti bei išnagrinėja Registro 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 Lietuvos Respublikos profesinių ligų valstybės registro veiklos testinimo valdymo plane.

15. Registro programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

15.1. Registro programinės ir techninės įrangos keitimai atliekami Registro tvarkytojo ir/ar Registro valdytojo iniciatyva, sprendimą priima Registro valdytojas;

15.2. pakeitimų projektavimą ir kūrimą atlieka atsakingi asmenys arba įstatymų nustatyta tvarka pasirinkti paslaugų tiekėjai;

15.3. prieš atliekant keitimus, kurių metu gali iškilti grėsmė Registro duomenų konfidencialumui, vientisumui ar pasiekiamumui, visi pakeitimai turi būti išbandomi testavimo aplinkoje;

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

15.5. Registro tvarkytojas Registro naudotojams, dirbantiems kitose įstaigose, privalo pateikti visą reikalingą informaciją apie naudojimosi Registru pasikeitimus, atsiradusius po programinės ar techninės įrangos keitimo arba atnaujinimo.

16. Registro pokyčių (toliau – pokyčiai) valdymo tvarka:

16.1. visi pokyčiai (projektavimas, kūrimas, testavimas, diegimas) atliekami Registro tvarkytojo ir / ar Registro valdytojo iniciatyva;

16.2. pokyčių projektavimą ir kūrimą atlieka atsakingi asmenys arba įstatymų nustatyta tvarka pasirinkti paslaugų tiekėjai;

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

16.4. atlikus Registro pokyčių testavimą arba, jei testavimo darbų dėl programinių ir (ar) techninių priežasčių nebuvo galima atlikti, Registro administratorius gali pradėti įgyvendinti pokyčius;

16.5. jeigu testavimas sėkmingas, pokyčiai perkeliama į gamybinę aplinką;

16.6. visi pokyčiai registruojami ir prireikus apie tai informuojami Registro naudotojai;

16.7. Registro administratorius Registro naudotojams privalo pateikti visą reikalingą informaciją apie naudojimosi Registru pakitimus, kurie yra susiję su jų atliekamomis funkcijomis ir kurių atsiradimas susijęs su įvykdytais arba vykdomais pokyčiais.

17. Nešiojamųjų kompiuterių naudojimo tvarka:

17.1. nešiojamaisiais kompiuteriais turi teisę naudotis tik Registro naudotojai ir Registro administratorius darbinėms funkcijoms atlikti;

17.2. nešiojamieji kompiuteriai turi būti atskirti nuo viešojo interneto tinklo užkarda;

17.3. nešiojamuosiuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis;

17.4. baigus darbą ar pasitraukiant iš darbo vietos Registro naudotojai privalo imtis priemonių, kad su Registro duomenimis negalėtų susipažinti pašaliniai asmenys (atsijungti nuo Registro, įjungti ekrano užsklandą su slaptažodžiu);

17.5. siekiant apsaugoti nešiojamuosiuose kompiuteriuose sukauptus Registro duomenis, turi būti daromos atsarginės duomenų kopijos išorinėse duomenų laikmenose;

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

IV SKYRIUS

REIKALAVIMAI, KELIAMİ REGISTRUI FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

18. Reikalavimai Registrui funkcionuoti reikalingoms paslaugoms (projektavimo, aptarnavimo ir priežiūros) ir jų teikėjams nustatomi šių paslaugų teikimo sutartyse.

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

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

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