PATVIRTINTA

Viešosios įstaigos Vilniaus miesto

klinikinės ligoninės direktoriaus

2022 m. balandžio 15 d. įsakymu Nr.V1-114/22(1.1)

**VMKL INFORMACINĖS SISTEMOS**

 **NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS**

**I SKYRIUS**

**Bendrosios nuostatos**

1. Viešosios įstaigos Vilniaus miesto klinikinė ligoninė (toliau – VMKL) valdomos ir tvarkomos informacinės sistemos (toliau – IS) naudotojų administravimo taisyklės (toliau – Taisyklės) reglamentuoja VMKL IS naudotojų ir IS administratorių įgaliojimus, teises, pareigas, prieigos prie elektroninės informacijos principus, saugaus elektroninės informacijos teikimo IS naudotojams kontrolės tvarką.

2. Taisyklėse vartojamos sąvokos:

2.1. **Išorinis IS naudotojas** – su IS valdytoju arba IS tvarkytoju (-ais) tarnybos ar darbo santykiais nesusijęs asmuo, kuris IS veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudoja ir (ar) tvarko elektroninę informaciją.

2.2. **Vidinis IS naudotojas** – IS naudotojas, tarnybos ar darbo santykiais susijęs su IS valdytoju arba IS tvarkytoju.

2.3. Kitos 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“.

3. Taisyklės taikomos visiems IS naudotojams, IS administratoriams ir IS tvarkytojo (-jų) saugos įgaliotiniams.

4. Prieigos prie elektroninės informacijos principai:

4.1. IS naudotojų ir IS administratorių prieiga prie elektroninės informacijos grindžiama būtinumo žinoti principu. Šis principas reiškia, kad IS naudotojams ir IS administratoriams prieiga suteikiama tik prie tos elektroninės informacijos, kuri reikalinga vykdant tiesioginę jų veiklą. Tvarkyti elektroninę informaciją gali tik tie IS naudotojai ir IS administratoriai, kuriems Taisyklių III skyriuje nustatyta tvarka suteiktos prieigos prie elektroninės informacijos teisės ir priemonės (identifikavimo priemonės, slaptažodžiai ar kitos tapatybės nustatymo priemonės ir panašiai);

4.2. IS naudotojų ir IS administratorių prieigos prie elektroninės informacijos lygmuo grindžiamas mažiausios privilegijos principu. Šis principas reiškia, kad turi būti suteikiamos tik minimalios IS naudotojų ir IS administratorių tiesioginei veiklai vykdyti reikalingos prieigos teisės bei organizacinėmis ir techninėmis priemonėmis užtikrinama minimalių prieigos teisių naudojimo kontrolė (pavyzdžiui, privilegijuotos prieigos teisės neturi būti naudojamos veiklai, kuriai atlikti pakanka žemesnio lygio prieigos teisių, ir panašiai);

4.3. pareigų atskyrimo principas. Šis principas reiškia, kad IS naudotojui, IS administratoriui ar jų grupei negali būti pavesta atlikti ar kontroliuoti visų pagrindinių elektroninės informacijos tvarkymo ar IS priežiūros funkcijų, IS naudotojams negali būti suteikiamos IS administratoriaus teisės, IS priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą IS administratoriaus paskyrą, kuria naudojantis negalima atlikti kasdienių IS naudotojo funkcijų, IS kūrimo, modernizavimo funkcijos turi būti atskirtos nuo IS priežiūros funkcijų ir panašiai;

4.4. pareigų rotacijos principas. Šis principas reiškia, kad IS administratoriui negali būti pavesta nuolat atlikti tas pačias IS administratoriaus funkcijas. Siekiant išvengti subjektyviai tyčinių ir (arba) subjektyviai netyčinių rizikos veiksnių, IS tvarkytojai pagal galimybes turi užtikrinti IS administratorių rotaciją.

**II SKYRIUS**

**is naudotojų IR is administratorių įgaliojimai, teisės ir pareigos**

5. IS naudotojų (išskyrus pacientus) ir IS administratorių įgaliojimai, teisės ir pareigos tvarkant elektroninę informaciją ir prieigos prie elektroninės informacijos lygiai nustatomi pagal IS nuostatus, elektroninės informacijos teikimo sutartis, IS naudotojų ir IS administratorių pareiginius nuostatus bei kitus teisės aktus, reglamentuojančius IS veiklą ir IS elektroninės informacijos tvarkymą.

6. IS naudotojų – pacientų įgaliojimai, teisės ir pareigos tvarkant elektroninę informaciją ir prieigos prie elektroninės informacijos lygiai nustatomi IS naudojimo susipažinimo formose.

7. IS naudotojų (išskyrus pacientus) ir IS administratorių įgaliojimai, teisės ir pareigos tvarkant elektroninę informaciją:

7.1. turi teisę tvarkyti VMKL IS elektroninę informaciją tik atlikdami savo tiesiogines funkcijas;

7.2. gali naudotis tik tomis VMKL IS funkcijomis ir VMKL IS tvarkoma elektronine informacija, prie kurių prieiga jiems suteikta Taisyklių III skyriuje nustatyta tvarka;

7.3. privalo rūpintis IS ir jose tvarkomos elektroninės informacijos sauga ir kibernetiniu saugumu, tvarkyti elektroninę informaciją vadovaudamiesi IS veiklą reglamentuojančiais teisės aktais ir elektroninės informacijos teikimo sutartyse ar IS naudojimo licencijose nustatytais reikalavimais ir sąlygomis, savo veiksmais nepažeisti elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo, laikytis bendrųjų etikos ir moralės principų;

7.4. kilus įtarimui, kad slaptažodis galėjo būti atskleistas, IS naudotojai turi nedelsdami slaptažodį pakeisti ir / ar pranešti VMKL Informacinių technologijų skyriaus vedėjui ar VMKL IS administratoriui;

7.5. apie VMKL IS sutrikimus, neįprastą veikimą, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, esamus arba galimus informacijos saugumo reikalavimų pažeidimus bei kitų VMKL IS naudotojų nederamus veiksmus ar nusikalstamos veiklos požymių IS naudotojai turi nedelsdami pranešti VMKL Informacinių technologijų skyriaus vedėjui ar VMKL IS administratoriui;

7.7. apie VMKL IS techninės įrangos gedimus IS naudotojai turi nedelsdami pranešti VMKL IS administratoriui bei privalo leisti jam imtis veiksmų gedimui įvertinti ir jį pašalinti;

7.8. atsako už visus neteisėtus veiksmus, kuriuos atliko tvarkydami VMKL IS elektroninę informaciją ar administruodami VMKL IS informacinius išteklius.

8. IS naudotojams ir IS administratoriams draudžiama:

8.1. perduoti savo prisijungimo prie VMKL IS duomenis kitiems asmenims;

8.2. prisijungti prie VMKL IS naudojant ne savo prisijungimo duomenimis;

8.3. naudoti elektroninę informaciją kitokiais tikslais, nei būtina vykdant tiesiogines darbo funkcijas, savavališkai rinkti, tvarkyti, perduoti, saugoti, naikinti, pakeisti ar kitaip naudoti VMKL IS elektroninę informaciją;

8.4. atskleisti VMKL IS tvarkomą informaciją ar bet kokiu kitu būdu leisti su ja susipažinti tokios teisės neturintiems asmenims;

8.5. sudaryti sąlygas pasinaudoti VMKL IS technine ir programine įranga tokios teisės neturintiems asmenims;

8.6. naudotis svetimais ištekliais (kopijuoti, trinti, kurti ir naudotis programomis ir duomenimis be išteklių savininko žinios ir sutikimo, jungtis prie svetimų kompiuterių, sistemų, duomenų bazių ir kitų vietų be atitinkamo leidimo);

8.7. savavališkai diegti VMKL IS programinės įrangos pakeitimus ir naujas versijas neturint tam suteiktos teisės. IS naudotojai neturi teisės keisti IS administratoriaus nustatytų operacinės sistemos, taikomosios programinės įrangos, techninės įrangos tvarkyklių bei konfigūracijos nustatymo duomenų;

8.8. instaliuoti ir naudoti programinę įrangą, kuri yra nesusijusi su darbo užduotimis arba yra skirta asmeniniams poreikiams;

8.9. naudoti programinę įrangą, kuri apsunkina ar trikdo VMKL IS techninės ir programinės įrangos veikimą arba kuri nesusijusi su tiesioginiu darbu (tinklo skenavimo programos, tinklo blokavimo programos, muzikos ir/ar filmų, žaidimų siuntimosi programos, internetinės TV ir/ar radijo programos, pokalbių programos, nuotraukų ir vaizdo apsikeitimo programos ir pan.);

8.10. be tiesioginio vadovo leidimo išsinešti VMKL IS techninę įrangą iš VMKL patalpų, išskyrus tuos atvejus kai tai būtina darbo funkcijoms atlikti;

8.11. atlikti bet kokius kitus neteisėtus VMKL IS tvarkymo veiksmus;

8.12. VMKL IS priemones, įskaitant suteiktas darbo tikslais elektroninio pašto paskyras, naudoti veiklai, kuri yra neteisėta pagal Lietuvos Respublikos teisės aktus.

9. IS administratorių prieigos prie IS lygiai ir juose taikomi saugos reikalavimai:

9.1. IS administratoriai IS ir jų komponentus gali pasiekti naudodamiesi tiesiogine, vietinio tinklo arba nuotoline prieiga. IS administratorių prieiga ir jos lygiai kontroliuojami per fizinius (įeigos kontrolės sistemos, barjerai ir kita) ir loginius (užkardos, domeno valdikliai ir kita) prieigos taškus. Kontrolės priemonės turi būti taikomos visuose IS sandaros sluoksniuose (kompiuterinis tinklas, platformos ar operacinės sistemos, duomenų bazės ir taikomųjų programų sistemos);

9.2. IS administratoriams prieiga prie IS komponentų, elektroninės informacijos ir teisė atlikti elektroninės informacijos tvarkymo veiksmus (elektroninės informacijos skaitymas, kūrimas, atnaujinimas, šalinimas, IS naudotojų informacijos, prieigos teisių redagavimas ir pan.) suteikiama pagal šias IS administratorių grupes, remiantis Taisyklių 4 punkte nustatytais prieigos prie elektroninės informacijos principais:

9.2.1. koordinuojančiam administratoriui pagal kompetenciją gali būti suteikta prieiga prie visų IS komponentų ir jų sąrankos;

9.2.2. IS naudotojų administratoriams suteikiama prieiga prie IS naudotojų prieigos teisių valdymo sistemų;

9.2.3. IS komponentų administratoriams pagal kompetenciją suteikiama prieiga prie kompiuterių, operacinių sistemų, duomenų bazių ir jų valdymo sistemų, taikomųjų programų sistemų, užkardų, įsilaužimų aptikimo ir prevencijos sistemų, elektroninės informacijos perdavimo tinklų, duomenų saugyklų, bylų serverių ir kitos techninės ir programinės įrangos bei jų sąrankos;

9.2.4. IS saugos administratoriams suteikiama prieiga prie IS pažeidžiamumų skenavimo, IS stebėsenos ir saugos atitikties nustatymo ir įvertinimo, saugos informacijos ir įvykių stebėjimo, apsaugos nuo elektroninės informacijos nutekinimo priemonių, kitos saugos užtikrinimo įrangos ir kitų priemonių, kuriomis atliekamas informacinių sistemų pažeidžiamų vietų nustatymas, saugumo reikalavimų atitikties nustatymas ir stebėsena. Saugos administratoriai turi teisę gauti prieigą ir prie kitų IS komponentų, jeigu tai būtina jų funkcijoms, susijusioms su saugumo reikalavimų atitikties nustatymu ir stebėsena, atlikti.

9.3. IS administratoriams suteikiamos tokios prieigos teisės, su kuriomis jie negali atlikti IS naudotojų funkcijų, išskyrus tuos atvejus, kai tai tiesiogiai susiję su IS administratorių vykdomomis funkcijomis;

9.4. Jei IS administratoriai pagal savo darbo funkcijas turi atlikti ir IS naudotojų funkcijas, jiems sukuriamos atskiros paskyros – IS naudotojo rolei ir IS administratoriaus rolėms atlikti.

**III skyrius**

**SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO IS NAUDOTOJAMS KONTROLĖS TVARKA**

10. Už IS naudotojų ir IS administratorių registravimą ir išregistravimą atsakingi informacinių sistemų naudotojų administratoriai. Už Taisyklių 13 punkte nurodytos informacijos, reikalingos IS naudotojų ir IS administratorių registravimo ir išregistravimo veiksmams atlikti, pateikimą IS naudotojų administratoriams atsakingi IS naudotojų ir IS administratorių tiesioginiai vadovai.

11. IS naudotojai ir IS administratoriai registruojami arba išregistruojami IS posistemiuose ir komponentuose atitinkamai suteikiant jiems prieigos prie IS teises arba jas panaikinant.

12. Vidinio IS naudotojo tapatybė gali būti nustatoma naudojantis VMKL tam tikslui naudojama specializuota autentifikavimo programine įranga arba IS vidinėmis autentifikavimo priemonėmis.

13. IS naudotojų ir IS administratorių registravimo ir išregistravimo tvarka:

13.1. IS naudotojų administratorius prieigos teises suteikia arba pakeičia gavęs IS naudotojo ar IS administratoriaus tiesioginio vadovo rašytinį prašymą, suderintą su savo organizacijoje paskirtais IS ir (arba) elektroninės informacijos savininkais (angl. *System Owner/Data Owner*);

13.2. teisė tvarkyti elektroninę informaciją gali būti suteikiama tik įsitikinus, kad IS naudotojas arba IS administratorius yra pasirašęs pasižadėjimą saugoti duomenų ir informacijos paslaptį ir pasirašytinai susipažinęs su saugos dokumentais ar jų santrauka ir sutikęs laikytis jų reikalavimų;

13.3. IS naudotojų administratorius prieigos teises sustabdo nedelsdamas, gavęs VMKL Personalo skyriaus kompetentingo darbuotojo pateiktą informaciją apie tai, kad teisės aktų nustatytais atvejais IS naudotojas ar IS administratorius nušalinamas nuo darbo (pareigų), neatitinka teisės aktuose nustatytų IS naudotojo ar IS administratoriaus kvalifikacinių reikalavimų, praranda patikimumą, yra nėštumo ir gimdymo (motinystės) ar vaiko priežiūros atostogose ir pan.;

13.4. administratorius prieigos teises panaikina gavęs VMKL Personalo skyriaus kompetentingo darbuotojo pateiktą informaciją apie IS naudotojo ar IS administratoriaus darbo (tarnybos) santykių pasibaigimą. IS naudotojų administratorius prieigos teises turi panaikinti paskutinę IS naudotojo ar IS administratoriaus darbo dieną, tačiau ne vėliau kaip iki darbo (tarnybos) dienos pabaigos. Priverstinio darbo (tarnybos) santykių nutraukimo atveju ir kitais atvejais, kai yra rizika, kad IS naudotojas ar IS administratorius gali atlikti tyčinius veiksmus (pakeisti ar sunaikinti elektroninę informaciją, sutrikdyti elektroninės informacijos perdavimą informacinių technologijų duomenų perdavimo tinklais, pažeisti IS saugumą, įvykdyti vagystę ir kita), prieigos teisės turi būti panaikintos nedelsiant;

13.5. tiesioginiai IS naudotojų ir IS administratorių vadovai kartu su savo organizacijoje paskirtais IS ir (arba) elektroninės informacijos savininkais ne rečiau kaip kartą per metus arba keičiantis IS naudotojo ar IS administratoriaus pareigoms ar funkcijoms turi peržiūrėti šiems darbuotojams suteiktas teises, įvertinti jų atitiktį vykdomoms funkcijoms. Tiesioginiai IS naudotojų ir IS administratorių vadovai turi parengti rašytinį prašymą dėl prieigos teisių vidiniam IS naudotojui ar IS administratoriui pakeitimo, jeigu suteiktos prieigos teisės neatitinka vykdomų funkcijų.

14. Išoriniai IS naudotojai prie IS jungiasi naudodamiesi VMKL tam tikslui naudojama specializuota autentifikavimo programine įranga arba IS vidinėmis autentifikavimo priemonėmis. Išoriniai IS naudotojai gali naudotis tik išorinio informacinių sistemų naudotojo paskyromis.

15. IS naudotojų ir IS administratorių paskyrų kontrolės priemonės:

15.1. paskyrų galiojimas turi būti laikinai sustabdomas, kai IS naudotojas nesinaudoja IS ilgiau kaip 60 darbo dienų, o IS administratorius – 30 darbo dienų);

15.2. IS tvarkytojai turi patvirtinti asmenų, kuriems suteiktos IS naudotojo ir IS administratoriaus teisės prisijungti prie IS, sąrašai periodiškai (ne rečiau kaip kartą per pusmetį) peržiūrimi IS tvarkytojų saugos įgaliotinių savo organizacijose. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais IS administratorius nušalinamas nuo darbo (pareigų);

15.3. IS naudotojų administratorius ne rečiau kaip kas 3 mėnesius patikrina IS naudotojų ir ne rečiau kaip kas 2 mėnesius patikrina IS administratorių paskyras. Apie nepatvirtintas IS naudotojų ir administratorių paskyras pranešama VMKL IS saugos įgaliotiniui;

15.4. nereikalingos ar nenaudojamos IS naudotojų ir IS administratorių paskyros turi būti blokuojamos nedelsiant ir ištrinamos praėjus audito duomenų saugojimo terminui, nustatytam IS saugaus elektroninės informacijos tvarkymo taisyklėse.

16. Kiekvienas IS naudotojas ir IS administratorius turi būti IS unikaliai atpažįstamas. IS naudotojo ir IS administratoriaus identifikacija turi būti pagrįsta naudotojo vardu, naudotojo kodu arba kita identifikacijos priemone, vienareikšmiškai apibrėžiančia IS naudotoją ar IS administratorių.

17. IS naudotojas ir IS administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita autentiškumo patvirtinimo priemone. IS administratorių tapatumui patvirtinti turi būti naudojamos dviejų veiksnių tapatumo patvirtinimo priemonės, jeigu IS komponentai palaiko tokį funkcionalumą.

18. IS naudotojų ir IS administratorių slaptažodžių, jų sudarymo, galiojimo trukmės ir keitimo bendrieji reikalavimai:

18.1. slaptažodį turi sudaryti trijų grupių iš galimų keturių (didžiosios ir mažosios raidės, skaičiai bei specialūs ženklai) simboliai;

18.2. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, vardas, pavardė, gimimo data, šeimos narių vardai, prisijungimo vardas, gyvenamosios vietos adresas ar jo sudedamosios dalys, telefono numeris ir kita);

18.3. draudžiama slaptažodžius atskleisti tretiesiems asmenims;

18.4. kilus įtarimui dėl slaptažodžio konfidencialumo pažeidimo, slaptažodis turi būti nedelsiant pakeistas;

18.5. IS dalys, atliekančios nuotolinio prisijungimo tapatybės nustatymą, turi neleisti išsaugoti slaptažodžių;

18.6. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius turi būti ne didesnis nei 3 kartai. Viršijus leistiną mėginimų įvesti teisingą slaptažodį skaičių, paskyra automatiški užrakinama. Atrakinti paskyra gali tik IS naudotojų administratorius. Apie IS naudotojų paskyrų užsirakinimą automatiškai turi būti informuojamas IS naudotojas ir IS administratorius;

18.7. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais;

18.8. IS tvarkytojo saugos įgaliotinio sprendimu laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo naudotojo vardo ar identifikavimo kodo, jei IS naudotojas ar IS administratorius neturi galimybių iššifruoti gauto užšifruoto slaptažodžio arba nėra techninių galimybių IS naudotojui ar IS administratoriui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

21. Specialieji reikalavimai IS naudotojų slaptažodžiams:

21.1. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;

21.2. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

21.3. keičiant slaptažodį IS neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

21.4. pirmojo prisijungimo prie IS metu IS turi automatiškai inicijuoti laikino slaptažodžio pakeitimą.

22. Specialieji IS administratorių slaptažodžių reikalavimai:

22.1. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

22.2. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

22.3. keičiant slaptažodį IS neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

22.4. draudžiama IS techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti nedelsiant pakeisti ir atitikti IS administratorių slaptažodžiams taikomus reikalavimus.

23. Nuotolinis IS naudotojų prisijungimas prie IS turi būti vykdomas naudojant patikimus elektroninės informacijos šifravimo protokolus.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_