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

SVEIKATOS PRIEŽIŪROS ĮSTAIGOS INFORMACINĖS SISTEMOS PAVYZDINĖS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Sveikatos priežiūros įstaigos (toliau – SPĮ) valdomos ir tvarkomos informacinės sistemos (toliau – IS) naudotojų administravimo taisyklės (toliau – Taisyklės) reglamentuoja SPĮ 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 licencijose (susipažinimo formose).

7. IS naudotojai ir IS administratoriai 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 arba susipažinimo formose nustatytais reikalavimais ir sąlygomis, savo veiksmais nepažeisti elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo.

8. IS naudotojai ir IS administratoriai turi teises naudotis tik tais IS ištekliais, kurios jiems buvo suteiktos Taisyklių III skyriuje nustatyta tvarka.

9. IS naudotojai ir IS administratoriai, pastebėję Duomenų saugos nuostatuose, Taisyklėse ir kituose IS saugos dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos ir (ar) kibernetinio saugumo užtikrinimo priemones, privalo nedelsdami kreiptis į SPĮ informacinių technologijų pagalbos tarnybą ar kitą kompetentingą padalinį arba asmenį, atliekantį informacinių technologijų pagalbos tarnybos funkcijas.

10. Jeigu IS tvarkytojo saugos įgaliotinis nebuvo informuotas apie Taisyklių 9 punkte nurodytus pažeidimus, apie tai informuojamas kitas kompetentingas padalinys arba asmuo, atliekantis informacinių technologijų pagalbos tarnybos funkcijas. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią IS saugą ir (ar) kibernetinį saugumą, IS tvarkytojo saugos įgaliotinis apie tai turi pranešti IS valdytojo vadovui ir kompetentingoms institucijoms, tiriančioms elektroninių ryšių tinklų, elektroninės informacijos saugos ir kibernetinius incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos ar kibernetiniais incidentais.

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

11.1. 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);

11.2. 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 Duomenų saugos nuostatuose nustatytas IS administratorių grupes, remiantis Taisyklių 4 punkte nustatytais prieigos prie elektroninės informacijos principais;

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

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

11.5. 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;

11.6. 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.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO IS NAUDOTOJAMS KONTROLĖS TVARKA

12. Už IS naudotojų ir IS administratorių registravimą ir išregistravimą atsakingi informacinių sistemų naudotojų administratoriai. Už Taisyklių 15 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.

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

14. Vidinio IS naudotojo tapatybė gali būti nustatoma naudojantis Valstybės informacinių išteklių sąveikumo platformos (toliau – VIISP) ar kitomis autentifikavimo priemonėmis.

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

14.2. 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*);

14.3. 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;

14.4. IS naudotojų administratorius prieigos teises sustabdo nedelsdamas, gavęs už žmogiškųjų išteklių valdymą atsakingo IS valdytojo, IS tvarkytojo padalinio arba kito kompetentingo padalinio arba 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.;

14.5. administratorius prieigos teises panaikina gavęs už žmogiškųjų išteklių valdymą atsakingo IS valdytojo, IS tvarkytojo padalinio arba kito kompetentingo padalinio arba 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;

14.6. 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.

15. Išoriniai IS naudotojai prie IS jungiasi naudodamiesi VIISP arba kitomis asmenų autentifikavimo priemonėmis. Išoriniai IS naudotojai gali naudotis tik išorinio informacinių sistemų naudotojo paskyromis.

16. IS naudotojų ir IS administratorių paskyrų kontrolės priemonės:

16.1. paskyrų galiojimas turi būti laikinai sustabdomas, kai vidinis IS naudotojas nesinaudoja IS ilgiau kaip __ dienų (IS administratorius – __ dienų);

16.2. 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);

16.3. turi būti naudojamos IS naudotojų paskyrų kontrolės priemonės ir administratorių paskyrų kontrolės priemonės, kurios atliktų paskyrų patikrinimą ir apie nepatvirtintas IS naudotojų ir administratorių paskyras praneštų IS tvarkytojo saugos įgaliotiniui. Apie nepatvirtintas administratorių paskyras turi būti pranešama nedelsiant;

16.4. 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.

17. 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.

18. Sudarant IS naudotojo ar IS administratoriaus identifikatorių didžiosios ir mažosios raidės neturi būti skiriamos.

19. 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.

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

20.1. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;

20.2. 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);

20.3. draudžiama slaptažodžius atskleisti tretiesiems asmenims;

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

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

20.6. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius turi būti ne didesnis nei __ kartai. Viršijus leistiną mėginimų įvesti teisingą slaptažodį skaičių, paskyra turi užsirakinti ir neleisti identifikuotis ne trumpiau nei __ minučių. Apie IS naudotojų paskyrų užsirakinimą automatiškai turi būti informuojamas IS administratorius;

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

20.8. 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 __ simboliai;

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

21.3. keičiant slaptažodį IS neturi leisti sudaryti slaptažodžio iš buvusių __ 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 __ simbolių;

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

22.3. keičiant slaptažodį IS neturi leisti sudaryti slaptažodžio iš buvusių __ 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.

_____