

# VŠĮ RESPUBLIKINĖS VILNIAUS PSICHIATRIJOS LIGONINĖS MINIMALŪS INFORMACIJOS SAUGOS IR KIBERNETINIO SAUGUMO REIKALAVIMAI TRETIESIEMS ASMENIMS (IŠORĖS ŠALIMS)

## 1. TAIKYMO SRITIS

1. Šie VšĮ Respublikinės Vilniaus psichiatrijos ligoninės (toliau – Bendrovė) minimalūs informacijos saugos ir kibernetinio saugumo reikalavimai Tretiesiems asmenims (išorės šalims) (toliau – Reikalavimai) taikomi visiems fiziniams ir juridiniams asmenims, su kuriais Bendrovė sudaro sutartis ir tokių sutarčių vykdymas apima Bendrovės informacijos saugumo reikalavimų įgyvendinimo užtikrinimą ir valdymą.

## 2. REIKALAVIMŲ PAGRINDAS IR OBJEKTAS

2. Reikalavimų pagrindas – tarp Bendrovės ir Trečiojo asmens sudaryta Sutartis bei Sutarties šalių pareiga užtikrinti informacijos saugos ir kibernetinio saugumo reikalavimų laikymąsi Sutarties vykdymo metu.

3. Reikalavimų objektas – Sutarties šalių teisės ir pareigos Bendrovės pavedimu / leidimu naudojant ir (ar) dirbant su Bendrovės informacija ir informacijos resursais.

## 3. VARTOJAMOS SĄVOKOS

4. Asmens duomenys – kaip jie apibrėžti Bendrojo duomenų apsaugo reglamento 4 straipsnio 1 dalyje, kuriuos Bendrovė pateikia Trečiajam asmeniui Sutarties vykdymui arba suteikia prieigą prie jų, laikantis šiuose Reikalavimuose nustatytų sąlygų.

5. „Būtina darbai“ – prieiga suteikiama tik prie minimalios ir atitinkamai veiklai, paslaugoms būtinos informacinės sistemos (infrastruktūros) ar jos dalies.

6. Informacinės sistemos (infrastruktūra) – Bendrovėje naudojamos informacinės sistemos ir jų infrastruktūra.

7. Tretieji asmenys (išorės šalys) – paslaugų teikėjai, partneriai, klientai, kiti asmenys turintys ar galintys turėti prieigą prie Bendrovės informacinių resursų.

8. Sutartis – Bendrovės ir Trečiojo asmens (išorės šalies) sudaryta sutartis, kurios vykdymas apima Bendrovės pavedimu / leidimu darbą su Bendrovės valdomomis informacinėmis sistemomis (infrastruktūra), Bendrovės informacija, ir kurioje yra nuoroda į šiuos Reikalavimus arba kai Reikalavimų taikymas tokiai Sutarčiai tarp Bendrovės ir Trečiojo asmens (išorės šalies) sutartas kitu būdu.

9. Kitos sąvokos Reikalavimuose suprantamos taip, kaip jos apibrėžtos ir vartojamos Sutartyje ir informacijos saugą ir kibernetinį saugumą reglamentuojančiuose teisės aktuose bei Bendrovės vidaus dokumentuose.

## 4. ATITIKTIES REIKALAVIMAI

10. Šie Reikalavimai apibrėžia minimalius informacijos saugos ir kibernetinio saugumo principus, kurie turi būti įvykdyti bet kokiomis sąlygomis pagal atitinkamą Sutartį su Bendrove, kurioje yra nuoroda į šiuos Reikalavimus.

11. Bendrovės prašymu leisti Bendrovės IT vadovui arba saugos įgaliotiniui atlikti informacijos saugos ir kibernetinio saugumo auditą ar kitus informacijos ir kibernetinio saugumo patikrinimo veiksmus bei pateikti visą reikalingą informaciją, kuri reikalinga patikrinti, - ar Trečiasis asmuo (išorės šalis) laikosi šių Reikalavimų ir taikomų aktualių informacijos saugos ir kibernetinio saugumo teisės aktų nurodymų; arba prašyti pateikti galiojančią Lietuvos standarto LST ISO/IEC 27001 sertifikata Tokio pobūdžio auditai atliekami Bendrovės lėšomis, ir juos turi atlikti tam teisę turintys subjektai.

12. Bendrovė pasilieka teisę atlikti Trečiojo asmens (išorės šalies) informacijos saugos ir kibernetinio saugumo vertinimą potencialių pažeidžiamumų nustatymui; arba prašyti pateikti galiojančią Lietuvos standarto LST ISO/IEC 27001 sertifikata.

13. Galimi, potencialūs ir tikėtini nukrypimai nuo Reikalavimų turi būti aiškiai įvardinti ir uždokumentuoti.

14. Priklausomai nuo prieigos prie informacinės sistemos (infrastruktūros) ir informacijos tipo gali būti taikomi papildomi techniniai ir organizaciniai reikalavimai nurodyti:

14.1. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarime 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“;

14.2. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarime Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

14.3. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakyme Nr. V-941 „Dėl Techninių valstybės registų (kadastrų), žinybinių registų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

14.4. Lietuvos standarte LST ISO/IEC 27001 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“.

## 5. NUOTOLINIO PRISIJUNGIMO REIKALAVIMAI

15. Įvertinus potencialias rizikas ir suteikus Trečiajam asmeniui (išorės šaliai) galimybę dirbti nuotolinėje kompiuterizuotoje darbo vietoje priklausančioje Trečiajam asmeniui (išorės šaliai) bei suteikiant nuotolinę prieigą prie Bendrovės informacinių sistemų (infrastruktūros) ir informacijos privaloma:

15.1. drausti nuotolinę prieigą, jeigu nenaudojama virtualaus privataus tinklo technologija VPN (angl. Virtual Private Network) arba alternatyvi, didesnį ar tą patį saugumą užtikrinanti technologija;

15.2. įsitikinti, kad informacinės sistemos ir infrastruktūra iš kurios jungiamasi per nuotolį, - yra saugi (atnaujinta operacinė sistema ir kita programinė įranga, įdiegta antivirusinė programinė įranga, įjungta ir sukonfigūruota ugniasienė ir t. t.);

15.3. užtikrinti savalaikę ir reguliarią prieigos teisių kontrolę;

15.4. vykdyti nuolatinį veiksmų stebėjimą ir kontrolę;

15.5. užtikrinti Bendrovės viešai neskelbtinos informacijos apsaugą techninėmis priemonėmis;

15.6. užtikrinti, kad nuotolinio prisijungimo ryšys būtų kontroliuojamas ir sutaptų su iš anksto tarpusavyje suderintais keliamais tikslais, kurie yra apibrėžti Sutartyje kaip sutarties objektas ar kuriuos nurodo Bendrovės įgaliotas atstovas, kreipdamasis į Trečiąjį asmenį žodžiu (tiesiogiai, telefonu ar pan.) ar raštu (paprastu ar elektroniniu laišku arba kitomis rašytinių pranešimų perdavimo elektroninėmis priemonėmis);

15.7. nuotolinio ryšio prisijungimas ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „Būtina darbui“ ir galiotų Sutarties galiojimo laikotarpiu arba kita Sutartyje nurodytą terminą.

16. Prisijungdamas nuotoline prieiga prie informacinių sistemų (infrastruktūros) naudotojas privalo patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone.

17. Bet kokia nesankcionuota nuotolinė prieiga prie Bendrovės informacinių sistemų (infrastruktūros) ir informacijos yra draudžiama.

## 6. SAUGUS PROGRAMINĖS ĮRANGOS KŪRIMAS

18. Trečiasis asmuo (išorės šalis) nustato, dokumentuoja ir įgyvendina iniciatyvas, atitinkančias bendrai priimtus informacijos saugos ir kibernetinio saugumo standartus bei praktiką, siekiant sukurti saugius programinės ar techninės įrangos kūrimo procesus. Tokios iniciatyvos turi užtikrinti informacijos saugos ir kibernetinį saugumą visuose plėtros etapuose: mokymuose, reikalavimų apibrėžimuose, dizaino kūrime, diegime, patvirtinime, išleidime ir priežiūroje.

19. Programinė įranga neturi turėti naudotojo paskyrų, slaptažodžių ar privačių / slaptų raktų, kurių negali pakeisti arba pašalinti įgaliotasis programinės įrangos galutinis vartotojas.

20. Programinė įranga neturi turėti jokių naudotojo paskyrų (individualių, bendrų, testavimo aplinkos), kurios nėra dokumentuotos (tai nereiškia, kad susijusių naudotojų prieigos duomenys turi būti atskleisti).

21. Trečiasis asmuo (išorės šalis) turi aktyviai imtis priemonių, kad būtų pagerinta programinės įrangos saugumo kokybė. Šios priemonės turi atitikti bendrai priimtus pramoninių procesų valdymo informacijos saugos ir kibernetinio saugumo standartus bei praktiką bei, jei tai techniškai įmanoma, apimti patikimumo bandymus, pažeidžiamumą valdymą ir programinio kodo saugumo testavimus (įskaitant statinio ar binarinio kodo analizę).

22. Trečiasis asmuo (išorės šalis), perkeliant vystomą programinę įrangą į darbinę aplinką, privalo užtikrinti kuriamo programinio kodo higieną (negali būti pavyzdinės imties duomenų ir scenarijaus kodo, nuorodų į nenaudojamas bibliotekas, derinimo kodo ir kitų naudotų įrankių).

23. Vystomos programinės įrangos kūrimo, testavimo ir darbinės aplinkos turi būti atskirtos.

24. Programinės įrangos naudotojams neturi būti rodomi vystomos programinės įrangos klaidų apie programinį kodą ar tarnybinės stoties pranešimai, jei tai Trečiojo asmens (išorės šalies) teikiamų paslaugų objektas.

## **7. MOKYMAI IR KVALIFIKACINIAI REIKALAVIMAI**

25. Bendrovė turi teisę įsitikinti Trečiojo asmens (išorės šalies) darbuotojų kvalifikacija prašydama pateikti atitinkamus įrodymus leidžiančius dirbti Bendrovės informacine sistema (infrastruktūra) ir informacija, kur tai yra būtina arba reikalaujama.
26. Trečiasis asmuo (išorės šalis) turi vykdyti savo darbuotojų informacijos saugos ir kibernetinio saugumo sąmoningumo ugdymo mokymus.

## **8. FIZINIS SAUGUMAS**

27. Trečiųjų asmenų (išorės šalių) atstovai ir jų transporto priemonės į Bendrovės teritorijas įleidžiami tik su Bendrovės leidimu, o gabenamas kroviny – su krovinių lydinčiais dokumentais.
28. Į Bendrovės teritoriją draudžiama įvežti / įnešti šiuos daiktus:
- 28.1. Lietuvos Respublikos ginklų ir šaudmenų kontrolės įstatyme įrašytus visų kategorijų ginklus, jų priedėlius ir šaudmenis ar jų imitacijas;
- 28.2. sprogstamus įtaisus ir sprogiąsias medžiagas ar jų imitacijas;
- 28.3. narkotikus ir narkotines medžiagas bei alkoholinius gėrimus;
- 28.4. kitus, atvirą liepsną naudojančius ar kibirkštį skleidžiančius / sukeliančius, pavojingus daiktus, išskyrus tiesioginiam darbui, kuriam išduotas atitinkamas leidimas, naudojamus įrankius ir prietaisus.
29. Už šių Reikalavimų nesilaikymą Trečiųjų asmenų (išorės šalių) atstovams gali būti atimta teisė lankytis Bendrovės teritorijose ir objektuose.

## **9. INFORMACIJOS SAUGA**

30. Bendrovės tvarkomi duomenys ir elektroninė informacija pagal konfidencialumą klasifikuojama į:
- 30.1. viešai neskelbtiną informaciją (asmens duomenys, tarnybinio naudojimo informacija, bendro naudojimo informacija);
- 30.2. viešą informaciją (be apribojimų skelbiama informacija).
31. Neskelbtinos informacijos perdavimas ir (ar) prieigos suteikimas Trečiajam asmeniui (išorės šaliai) leidžiamas tik pasirašius Bendrovės patvirtintą konfidencialumo susitarimą arba, jeigu konfidencialumo susitarimo nuostatos aptartos Sutartyje.

## **10. BENDRIEJI KIBERNETINIO SAUGUMO REIKALAVIMAI**

32. Trečiasis asmuo (išorės šalis) turi užtikrinti, kad bet kokios naujos technologijos, kuri diegiama / įdiegta Bendrovėje, saugumas yra pakankamas pagal Lietuvos standarto LST ISO/IEC 27001 reikalavimus arba, esant poreikiui, gauti Bendrovės sutikimą naudoti mažesnio saugumo technologijas, nei nurodyta minėtame standarte.
33. Kiekvienas informacinių sistemų (infrastruktūros) naudotojas ar administratorius turi būti unikalčiai atpažįstamas.
34. Informacinių sistemų (infrastruktūros) naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone.
35. Suteikiant laikinus slaptažodžius informacinių sistemų (infrastruktūros) naudotojams ar administratoriams, šie slaptažodžiai turi būti unikalūs kiekvienam naudotojui ar administratoriui ir perduodami saugiu būdu.
36. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo naudotojo ar administratoriaus vardo ir tik tuo atveju, jeigu naudotojas ar administratorius neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių naudotojui ar administratoriui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.
37. Visose informacinėse sistemose (infrastruktūroje), prieš pradėdant jas eksploatuoti, informacinių sistemų administratoriai privalo pakeisti standartinius (gamintojų) slaptažodžius į šiuos Reikalavimus atitinkančius slaptažodžius, jei tai Trečiojo asmens (išorės šalies) teikiamų paslaugų objektas.
38. Informacinių sistemų (infrastruktūros) įranga, patvirtinanti informacinių sistemų naudotojo ar administratoriaus tapatumą, turi drausti automatiškai išsaugoti slaptažodžius, jei tai Trečiojo asmens (išorės šalies) teikiamų paslaugų objektas.
39. Informacinių sistemų (infrastruktūros) naudotojams draudžiama suteikti administratoriaus teises, jei tai Trečiojo asmens (išorės šalies) teikiamų paslaugų objektas.

40. Informacinėse sistemose (infrastruktūroje) turi būti išjungiamos visos nereikalingos gamyklinės naudotojų paskyros (tame tarpe svečio paskyra), jei tai Trečiojo asmens (išorės šalies) teikiamų paslaugų objektas.
41. Prieiga prie Bendrovės informacinių išteklių ir informacijos turi būti suteikiama vadovaujantis principu „Būtina darbui“.

## 11. TREČIOJO ASMENS (IŠORĖS ŠALIES) ĮSIPAREIGOJIMAI

### 42. Trečiasis asmuo (išorės šalis) įsipareigoja:

- 42.1. dirbant su Bendrovės išduotais informaciniais resursais (kompiuteriais, informacijos laikmenomis, dokumentais, duomenimis ir informacija) vadovautis Bendrovės šiais Reikalavimais;
- 42.2. saugoti ir be Bendrovės išankstinio raštiško sutikimo neatskleisti tvarkomų asmens duomenų ir (ar) neskelbtinos informacijos jokiems kitiems asmenims ir gavėjams, išskyrus teisės aktais nustatytus atvejus;
- 42.3. atsakyti už visus Bendrovės informaciniams sistemoms (infrastruktūrai) žalingus veiksmus, kuriuos padarė Trečiojo asmens (išorės šalies) atstovai ir atlyginti žalingais veiksmais padarytos tiesioginės žalos atstatymo kaštus. Trečiasis asmuo (išorės šalis) neprisiima atsakomybės už Bendrovės eksploatacinius nuostolius, pelno netekimą, prestižo praradimą ir bet kokius kitus netiesioginius nuostolius bei jų padarinių žalą. Duomenų praradimas laikomas netiesioginiu nuostoliu.
- 42.4. užtikrinti Bendrovės elektroninės informacijos konfidencialumą bei vientisumą, savo veiksmais netrikdyti elektroninės informacijos prieinamumo.
- 42.5. naudoti tik tas prieigos prie informacinės sistemos (infrastruktūros) teises, kurios buvo suteiktos Bendrovės.
- 42.6. baigus darbą ar naudotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri apdorojama informaciniame sistemoje (infrastruktūroje), negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinės sistemos (infrastruktūros), įjungžiama ekrano užsklanda su slaptažodžiu.
- 42.7. naudotis tik tomis informacinės sistemos (infrastruktūros) funkcijomis ir tokia informacijos apimtimi prie kurios buvo suteikta prieiga;
- 42.8. būti pasitvirtinusi informacijos saugos ir kibernetinių incidentų valdymo bei veiklos tęstinumo planus ar kitą dokumentaciją, reglamentuojančią Trečiojo asmens (išorės šalies) darbuotojų veiksmus informacijos ir kibernetinių incidentų metu.
- 42.9. sužinojus apie informacijos saugos ir kibernetinio saugumo incidentą, kuris gali būti susijęs su Bendrovės informacinėmis sistemomis ir informacija, nedelsiant informuoti Bendrovės IT vadovą arba saugos įgaliotinį, pateikiant visą turimą informaciją apie incidentą.
- 42.10. užtikrinti, kad imsis pakankamų priemonių rizikoms, susijusioms su savo subrangovais, jų atliekamais darbais ir tiekimo grandine, suvaldyti.

### 43. Trečiajam asmeniui (išorės šaliai) draudžiama:

- 43.1. skenuoti Bendrovės informacines sistemas (infrastruktūrą), ieškant pažeidžiamumų ar kitais būdais stebėti Bendrovės informacinių sistemų (infrastruktūros) duomenų srautą, šių priemonių naudojimo nesuderinus su Bendrovės IT tarnybos vadovu arba saugos įgaliotiniu. Tokio suderinimo nereikia, jeigu šiame punkte išvardintos priemonės yra reikalingos tiesioginėms paslaugoms atlikti, kurios yra Sutarties objektas;
- 43.2. gerti, valgyti ir rūkyti šalia informacijos apdorojimo įrangos;
- 43.3. savavališkai keisti suteiktus tinklo parametrus (IP adresą ir pan.);
- 43.4. naudoti programas, kurios gali trikdyti Bendrovės informacinių sistemų (infrastruktūros) veikimą (skenavimo, blokavimo programas ir pan., prieš tai nesuderinus su Bendrove);
- 43.5. savarankiškai arba savavališkai keisti, remontuoti, taisyti Bendrovės išduotą programinę ir techninę įrangą;
- 43.6. naudoti Bendrovės išduotą programinę ir techninę įrangą Lietuvos Respublikos teisės aktais draudžiamai veiklai, šmeižikiško, įžeidžiančio, grasinamojo pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujantį veiklai, kompiuterių virusams, masinei piktybiškai informacijai siųsti ar kitiems tikslams, kurie gali pažeisti Bendrovės ar kitų asmenų teisėtus interesus;
- 43.7. diegti, saugoti, naudoti, kopijuoti ar platinėti nelegalią, autorines teises pažeidžiančią programinę įrangą.

## 12. ATSAKOMYBĖ IR GINČŲ SPRENDIMO TVARKA

44. Kiekvienas ginčas, nesutarimas ar reikalavimas, kylantis iš Reikalavimų ar susijęs su Reikalavimais, jų pažeidimu, nutraukimu bei galiojimu, turi būti sprendžiamas Sutartyje nustatyta tvarka.

45. Trečiasis asmuo (išorės šalis) yra atsakinga už visas būtinas priemones ir veiksmus, siekiant laikytis šių Reikalavimų bei kituose šiai sričiai taikomuose teisės aktuose nustatytų pareigų vykdymą.

46. Jeigu Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytos kontroliuojančios institucijos nustato informacijos saugos ir kibernetinio saugumo incidentą, kuris kilo dėl Trečiojo asmens (išorės šalies) veiksmų ar neveikimo vykdant Sutartį, ir Bendrovei skiriama piniginei sankcija, tai Trečiasis asmuo (išorės šalis) įsipareigoja Bendrovei pareikalavus atlyginti tokios sankcijos sumą ar jos dalį, kiek tai tiesiogiai susiję su Trečiojo asmens (išorės šalies) veiksmis ar neveikimu, vadovaujantis Sutartyje numatyta baudų sumokėjimo tvarka.

47. Už Trečiojo asmens (išorės šalies) pasitelktų Trečiųjų asmenų tinkamą Reikalavimų įgyvendinimą atsako Trečiasis asmuo (išorės šalis).

### **13. BAIGIAMOSIOS NUOSTATOS**

48. Šie Reikalavimai yra Sutarties neatsiejama dalis, kai tai numatyta Sutartyje arba, kai dėl šių Reikalavimų taikymo Bendrovė ir Trečiasis asmuo (išorės šalis) susitarė kitu būdu.

49. Reikalavimų galiojimas Trečiajam asmeniui (išorės šaliai) yra neatsiejamas nuo Sutarties galiojimo termino.

50. Bet kurios šių Reikalavimų sąlygos, nuostatos pripažinimas negaliojančia dėl prieštaravimo imperatyvioms teisės aktų nuostatoms atveju, sąlyga, nuostata keičiama, vadovaujantis Sutartyje nustatyta tvarka.

51. Šie Reikalavimai nėra atskirai pasirašomi, tvirtinami.