

**VIEŠOJI ĮSTAIGA
JŪRININKŲ POLIKLINIKA**

TVIRTINU
Direktorius

Saulius Dabravalskis

**ADMINISTRACIJA
KIBERNETINIO SAUGUMO VADOVO PAREIGINIAI NUOSTATAI**

I. BENDROJI DALIS

1. Bendrieji reikalavimai kibernetinio saugumo vadovo pareigybei:
- 1.1. Kibernetinio saugumo vadovas yra darbuotojas, atsakingas už VŠĮ Jūrininkų poliklinikos (toliau – Įstaiga) kibernetinio saugumo politikos formavimą, įgyvendinimą, priežiūrą ir tobulinimą, taip pat už Įstaigos tinklų ir informacinių sistemų saugumo užtikrinimą;
- 1.2. Kibernetinio saugumo vadovas savo veikloje užtikrina atitiktį Lietuvos Respublikos kibernetinio saugumo įstatymui, kitiems Lietuvos Respublikos teisės aktams, Europos Sąjungos teisės aktams (įskaitant TIS2 direktyvos nuostatas), Nacionalinio kibernetinio saugumo centro (NKSC) metodikoms ir nurodymams
- 1.3. Kibernetinio saugumo vadovu dirbti priimamas asmuo turi turėti bent 2 metų patirtį IT, kibernetinio saugumo ar tinklų ir informacinių sistemų srityje arba atitinkamą aukštojo mokslo diplomą, tarptautinį saugumo sertifikatą (pvz., CISSP, CISM, CEH, ISO 27001 Lead Auditor) arba būti išklauses Nacionalinio kibernetinio saugumo centro (NKSC) patvirtintus mokymus ir išlaikęs egzaminą.
- 1.4. prieš pradėdamas dirbti ir vėliau pagal reikalavimus turi pasitikrinti sveikatą;
- 1.5. dirbdamas vadovaujasi Lietuvos Respublikos įstatymais, teisės aktais, Jūrininkų poliklinikos direktoriaus įsakymais, vidaus tvarkos ir vidaus darbo tvarkos taisyklėmis, saugos ir sveikatos darbe instrukcijomis, civilinės saugos instrukcijomis, priešgaisrinės saugos instrukcijomis, pareiginiiais nuostatais, kitais norminiais dokumentais susijusiais su jo atliekamu darbu.
- 1.6. Kibernetinio saugumo vadovas tiesiogiai pavaldus direktoriui.

II. KVALIFIKACINIAI REIKALAVIMAI

2. Kibernetinio saugumo vadovas turi žinoti, išmanyti ir mokėti:
- 2.1. Lietuvos Respublikos kibernetinio saugumo įstatymą ir susijusius teisės aktus;
- 2.2. TIS2 direktyvos reikalavimus;
- 2.3. kibernetinio saugumo rizikų valdymo principus;
- 2.4. tinklų ir informacinių sistemų saugumo pagrindus;
- 2.5. kibernetinių incidentų valdymo procesus;
- 2.6. organizacijos veiklos tęstinumo ir atkūrimo po incidentų principus;
- 2.7. asmens duomenų apsaugos (BDAR) reikalavimus;
- 2.8. vidaus kontrolės ir rizikų valdymo sistemas;
- 2.9. informacinių sistemų architektūrą ir saugos priemones;
- 2.10. analizuoti kibernetinio saugumo rizikas ir teikti išvadas;
- 2.11. valdyti incidentus ir krizes;

- 2.12. dirbti kompiuteriu, naudotis biuro programomis, saugumo valdymo ir stebėsenos sistemomis;
- 2.13. bendradarbiauti su išorinėmis institucijomis ir audito subjektais.

III. PAREIGOS

3. Kibernetinio saugumo vadovas:

Bendrosios pareigos:

- 3.1. tinkamai ir laiku vykdyti darbo sutartyje ir šiuose pareiginiuose nuostatuose nustatytas pareigas;
- 3.2. veikti savarankiškai pagal savo kompetenciją ir atsakyti už savo veiksmus teisės aktų nustatyta tvarka;
- 3.3. laikytis vidaus tvarkos ir vidaus darbo tvarkos taisyklių;
- 3.4. vykdyti saugos ir sveikatos darbe, priešgaisrinės ir civilinės saugos, elektrosaugos taisyklių reikalavimus;
- 3.5. dalyvauti bendruose Įstaigos darbuotojų bei administracijos susirinkimuose;
- 3.6. nuolat tobulinti profesinę kvalifikaciją kibernetinio saugumo srityje;
- 3.7. Vadovas gali būti atsakingas ne tik už bendrą Įstaigos saugumą, bet ir vykdyti konkrečių tinklų ar informacinių sistemų apsaugą, kaip numatyta įstatyme (Saugos įgaliojimo funkcijų vykdymas).

Kibernetinio saugumo politikos ir valdymo srityje:

- 3.8. yra atsakingas už tai, kad Įstaiga atitiktų Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nurodytus reikalavimus, susijusius su informacijos apsauga, rizikų valdymu ir reagavimu į incidentus. Užtikrinta, kad Įstaigos kibernetinio saugumo priemonės atitiktų teisės aktų, NKSC rekomendacijų ir gerosios praktikos reikalavimus;
- 3.9. organizuoja kibernetinio saugumo rizikų identifikavimą, vertinimą ir valdymą;
- 3.10. teikia įstaigos vadovui pasiūlymus dėl kibernetinio saugumo stiprinimo, investicijų ir prioritetų;
- 3.11. dalyvauja Įstaigos strateginiame planavime, integruodamas kibernetinio saugumo aspektus;
- 3.12. užtikrina, kad kibernetinis saugumas būtų integruotas į naujų informacinių sistemų, paslaugų ar procesų diegimą;

Tinklų ir informacinių sistemų saugumo srityje

- 3.13. koordinuoja tinklų ir informacinių sistemų saugumo priemonių diegimą ir priežiūrą;
- 3.14. užtikrina prieigos teisių valdymą, autentifikavimo ir autorizavimo priemonių taikymą;
- 3.15. kontroliuoja atsarginių kopijų darymo, saugojimo ir atkūrimo procesus;
- 3.16. užtikrina veiklos tęstinumo ir atkūrimo po kibernetinių incidentų planų parengimą, testavimą ir atnaujinimą;
- 3.17. dalyvauja atliekant informacinių sistemų saugumo vertinimus, testavimus ir auditus;

Kibernetinių incidentų valdymo srityje

- 3.18. organizuoja pasirengimą kibernetiniams incidentams;
- 3.19. koordinuoja reagavimą į kibernetinius incidentus ir vos neįvykusius incidentus;
- 3.20. užtikrina incidentų registravimą, analizę, dokumentavimą ir pasekmių šalinimą;
- 3.21. teisės aktų nustatyta tvarka teikia pranešimus apie kibernetinius incidentus Nacionaliniam kibernetinio saugumo centrui;
- 3.22. bendradarbiauja su NKSC, policija, Valstybine duomenų apsaugos inspekcija ir kitomis institucijomis;
- 3.23. organizuoja incidentų priežasčių analizę.

Mokymų, informacijos sklaidos ir vidaus kontrolės srityje

- 3.24. organizuoja darbuotojų mokymus ir informuotumo didinimą kibernetinio saugumo klausimais;
- 3.25. dalyvauja rengiant metinius mokymų ir kvalifikacijos tobulinimo planus;
- 3.26. konsultuoja darbuotojus ir vadovybę kibernetinio saugumo klausimais;
- 3.27. dalyvauja vidaus kontrolės sistemos diegimo, įgyvendinimo ir tobulinimo procesuose;

Turto ir informacijos apsaugos srityje

- 3.29. užtikrina jam patikėto materialiojo ir nematerialiojo turto saugumą;
- 3.30. kontroliuoja, kad informacinės sistemos ir duomenys būtų naudojami teisėtai, saugiai ir efektyviai;
- 3.31. užtikrina informacijos konfidencialumą, vientisumą ir prieinamumą;
- 3.32. organizuoja neatitiktį registravimą ir korekcinį veiksmų taikymą.

IV. TEISĖS

- 4. Kibernetinio saugumo vadovas turi teisę:
 - 4.1. naudotis Įstaigos turima informacija;
 - 4.2. gauti iš Įstaigos struktūrinių padalinių visą informaciją, reikalingą pareigoms vykdyti;
 - 4.3. dalyvauti pasitarimuose, komisijų ir darbo grupių veikloje;
 - 4.4. teikti pasiūlymus Įstaigos vadovui dėl kibernetinio saugumo organizavimo ir gerinimo;
 - 4.5. inicijuoti saugumo priemonių diegimą ir pakeitimus;
 - 4.6. naudotis darbuotojams nustatytomis socialinėmis ir kvalifikacijos kėlimo garantijomis;
 - 4.7. gauti darbui reikalingas technines ir organizacines priemones;
 - 4.8. gauti darbui būtinas darbo ir apsaugos bei kitas priemones;

V. ATSAKOMYBĖ

- 5. Kibernetinio saugumo vadovas atsako už:
 - 5.1. šių pareiginių nuostatų reikalavimų vykdymą.
 - 5.2. žalą, padarytą įstaigai dėl savo kaltės ar neatsargumo, padarytas klaidas, aplaidumą, netinkamą pareigų vykdymą, kompetencijos viršijimą kibernetinio saugumo vadovas atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

Susipažinau ir įsipareigoju vykdyti : _____
(darbuotojo vardas, pavardė, parašas)

Data _____