PATVIRTINTA
Greitosios medicinos pagalbos
tarnybos generalinio direktoriaus
2026 m. liepos 24 d. įsakymu Nr. V-491

GREITOSIOS MEDICINOS PAGALBOS TARNYBOS
KIBERNETINIO SAUGUMO VADOVAS
PAREIGYBĖS APRAŠYMAS NR. 23P-42

<...>

II SKYRIUS
SPECIALŪS REIKALAVIMAI ŠIAS PAREIGAS EINANČIAM DARBUOTOJUI

4. Darbuotojas, einantis šias pareigas, turi atitikti šiuos specialius reikalavimus:

4.1. *Būti įgijęs:*

4.1.1. aukštojo mokslo kvalifikaciją, įgytą baigus universitetines studijas ne žemesnį nei bakalauro kvalifikacinį laipsnį arba jai lygiavertę aukštojo mokslo kvalifikaciją;

4.1.2. ne mažesnę kaip 2 (dvejų) metų patirtį IT / kibernetinio saugumo srityje;

4.1.3. *CISM sertifikatą;*

4.1.4. *Nacionalinio kibernetinio saugumo centro Informacijos saugumo vadovo kursų pažymėjimą*.

4.2. *Mokėti* anglų kalbą C1 lygiu.

4.3. *Gebėti* formuoti saugumo strategiją, valdyti informacijos saugos rizikas, valdyti kibernetinius incidentus, rengti auditus, koordinuoti techninių ir organizacinių saugumo priemonių diegimą,

4.4. *Žinoti*:

4.4.1. ISO 27001, NIST, CSF bei kitus standartus;

4.4.2. Bendrąjį duomenų apsaugos reglamento;

4.4.3. TIS2 direktyvos reikalavimus.

4.5. Turėti bazinę kompiuterinio raštingumo kvalifikaciją, vadovaujantis Visuotinio kompiuterinio raštingumo standartu, patvirtintu Lietuvos Respublikos švietimo ir mokslo ministro 2004 m. gruodžio 14 d. įsakymu Nr. ISAK-2016.

4.6. Išmanyti dokumentų rengimo taisykles, mokėti sklandžiai dėstyti mintis raštu ir žodžiu, rengti išvadas ir pasiūlymus, tvarkomuosius, organizacinius dokumentus.

III SKYRIUS
ŠIAS PAREIGAS EINANČIO DARBUOTOJO FUNKCIJOS

5. Šias pareigas einantis darbuotojas vykdo šias funkcijas:

5.1. užtikrina kad Tarnyba atitiktų teisės aktų ir reguliacinių standartų reikalavimus;

5.2. rengia ir įgyvendina organizacijos kibernetinio saugumo strategiją, saugumo politiką ir kitas procedūras;

5.3. organizuoja kibernetinio saugumo incidentų aptikimą, reagavimą ir koordinavimą su atsakingomis institucijomis;

5.4. užtikrina Tarnybos informacijos, kritinės IT infrastruktūros saugumą ir veiklos tęstinumą;

5.5.koordinuoja veiklas, skirtas informacijos ir kibernetinių rizikų mažinimui bei su tuo susijusių finansinių nuostolių prevencijai;

5.6. organizuoja darbuotojų mokymus ir skatina kibernetinio saugumo sąmoningumą;

5.7. kuria ir įgyvendina informacijos saugumo programas, apimančias politikas, standartus, gaires ir procedūras;

5.8. reguliariai peržiūri informacijos saugumo politikų ir kt. dokumentus, atkreipdamas dėmesį į naujas grėsmes bei teisės aktų reikalavimus;

5.9. koordinuoja su IT ir kitais skyriais saugumo kontrolių įgyvendinimą;

5.10. kuria Tarnybos reagavimo į informacijos saugumo incidentus planą ir jį prižiūri;

5.11. vadovauja incidentų valdymo komandai incidentų metu;

5.12. užtikrina, kad Tarnybos informacijos saugumo praktikos atitiktų teisės aktų reikalavimus;

5.13. koordinuoja pasirengimą vidaus bei išorės saugumo auditams;

5.14. užtikrina, kad visos saugumo audito metu užfiksuotos neatitiktys būtų pašalintos;

5.15. bendradarbiauja su reguliavimo institucijomis ir nacionaliniais kibernetinio saugumo centrais, siekdamas užtikrinti atitiktį reikalavimams ir stiprinti organizacijos kibernetinį saugumą;

5.16. pagal savo kompetenciją vykdo kitus su kibernetiniu saugumu susijusius generalinio direktoriaus pavedimus;

5.17. tvarko asmens duomenis vadovaudamasis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu.

<...>