

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKA

I. BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų (toliau – TIS) kibernetinio saugumo politika (toliau – Politika) yra pagrindinis VšĮ Skuodo pirminės sveikatos priežiūros centras (toliau – Įstaiga) kibernetinio saugumo valdymo dokumentas, kuris apibrėžia kibernetinio saugumo tikslus, teisės aktų ir standartų, reglamentuojančių kibernetinį saugumą, reikalavimus, atsakingų asmenų funkcijas ir atsakomybes, įsipareigojimus darbuotojams ir trečiosioms šalims ir kita.

2. Politikos tikslas – užtikrinti kibernetinį saugumą, kuris apima tris pagrindinius aspektus:

2.1. Konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo;

2.2. Vientisumą – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;

2.3. Prieinamumą – užtikrinimą, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti Įstaigos veiklą.

3. Kibernetinis saugumas grindžiamas kibernetinio saugumo principais, kurie numatyti Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje.

4. Politikoje vartojamos sąvokos:

4.1. **Atitikties vertinimas** – Įstaigos atitikties Kibernetinio saugumo įstatymo, Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ bei šios Politikos ir jos įgyvendinimą reglamentuojančių kibernetinio saugumo dokumentų reikalavimams vertinimas;

4.2. **Rizikos vertinimas** – rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal Įstaigos TIS rizikos vertinimo ir valdymo tvarką;

4.3. **Kibernetinio saugumo vadovas** – Įstaigos darbuotojas atsakingas už kibernetinio saugumo subjekto atitikties Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

4.4. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais

5. Kitos šioje Politikoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

II. TEISĖS AKTAI

6. Kibernetinį saugumą reglamentuojančių teisės aktų ir standartų, kurių reikalavimus privalo įgyvendinti Įstaiga, sąrašas:

6.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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);

6.2. Kibernetinio saugumo įstatymas;

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

6.4. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

6.5. Lietuvos standartas LST ISO/IEC ISO 27001 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ (aktuali redakcija);

6.6. Lietuvos standartas LST ISO/IEC 27002 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“ (aktuali redakcija);

6.7. kitais teisės aktais, reglamentuojančiais kibernetinį saugumą.

7. Sudarytas Įstaigos Politikos įgyvendinimą reglamentuojančių kibernetinio saugumo dokumentų sąrašas (žr. 1 priedas).

IV. FUNKCIJOS IR ATSAKOMYBĖS

8. Direktorius privalo užtikrinti žmogiškuosius ir finansinius išteklius kibernetinio saugumo valdymui.

9. Įstaigos direktorius ar jo įgaliotas asmuo įsakymu paskiria šias pareigybės:

9.1. **Kibernetinio saugumo vadovą.** Apie jo paskyrimą Įstaiga privalo informuoti Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos (toliau – NKSC), pateikiant jo kontaktinę informaciją į Kibernetinio saugumo informacinę sistemą (toliau – KSIS) ir Įstaigos darbuotojus. Įstaigai leidžiama iš tiekėjo įsigyti paslaugas, kurias teikiant būtų atliekamos kibernetinio saugumo vadovo ir (ar) saugos įgaliotinio funkcijos;

9.2. **Saugos įgaliotinį;**

9.3. **TIS administratorių (-ius)];**

9.4. **Fizinės saugos įgaliotinį (-ius)];**

9.5. **Saugumo operacijų centrą (toliau – SOC).** SOC funkcijas gali vykdyti ir kiti Įstaigos paskirti asmenys ar grupės pagal TIS paslaugų teikimo sutartis. Apie jos paskyrimą Įstaiga privalo informuoti NKSC, pateikiant jos vadovo kontaktinę informaciją į KSIS;

9.6. **Veiklos tęstinumo valdymo grupę;**

9.7. **Veiklos atkūrimo grupę.**

10. **Kibernetinio saugumo vadovas** koordinuodamas ir prižiūrėdamas Politikos ir ją sudarančių kibernetinio saugumo dokumentuose nustatytų reikalavimų įgyvendinimą, turi atlikti šias funkcijas:

10.1. užtikrinti, kad Politika ir ją sudarantys kibernetinio saugumo dokumentai būtų parengti ir periodiškai atnaujinami;

10.2. organizuoti Įstaigos Atitikties vertinimą, rengti ir teikti tvirtinti Įstaigos direktoriui ar jo įgaliotam asmeniui Atitikties vertinimo ataskaitą (-as) ir Neatitiktį šalinimo planą (-us) bei jų patvirtinimo datą (-as) ir registracijos numerį (-ius) Kibernetinio saugumo įstatymo nustatyta tvarka, ne vėliau kaip per 5 darbo dienas, pateikti į NKSC administruojamą KSIS;

10.3. organizuoti Rizikos vertinimą ir dalyvauti Rizikos vertinimo procese, rengti ir teikti tvirtinti Įstaigos direktoriui ar jo įgaliotam asmeniui Rizikos vertinimo ataskaitas ir rizikos valdymo planus bei jų patvirtinimo datą (-as) ir registracijos numerį (-ius) Kibernetinio saugumo įstatymo nustatyta tvarka, ne vėliau kaip per 5 darbo dienas, pateikti į NKSC administruojamą KSIS;

10.4. organizuoti Įstaigos TIS veiklos tęstinumo valdymo plano (-ų) veiksmingumo išbandymą, rengti ir teikti tvirtinti Įstaigos direktoriui ar jo įgaliotam asmeniui TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo rezultatų ataskaitos (-ų) ir jų patvirtinimo datą (-as) ir registracijos numerį (-ius) Kibernetinio saugumo įstatymo nustatyta tvarka, ne vėliau kaip per 5 darbo dienas, pateikti į NKSC administruojamą KSIS;

10.5. organizuoti darbuotojų mokymus kibernetinio saugumo klausimais;

10.6. koordinuoti TIS kibernetinių incidentų tyrimus ir bendradarbiauti su kompetentingomis institucijoms, tiriančiomis kibernetinius incidentus bei neteisėtas veikas, susijusias su kibernetiniais incidentais;

10.7. teikti TIS administratoriui (-iams) ir (ar) naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Politikos ir ją sudarančiuose kibernetinio saugumo dokumentuose nustatytų reikalavimų įgyvendinimu;

10.8. atlikti kitas Politikoje ir ją sudarančiuose kibernetinio saugumo dokumentuose bei kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

11. Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis negali vykdyti funkcijų, susijusių su tinklų ar TIS administravimu ar kitomis pareigybėmis, susijusiomis su techninės kompiuterinės įrangos ar programinės įrangos priežiūra ir valdymu.

12. **Saugos įgaliotinio** (jei Įstaiga neturi Saugos įgaliotinio 12.1-12.9 punktuose aprašytas funkcijas vykdo Kibernetinio saugumo vadovas) funkcijos:

12.1. užtikrinti, kad Politikos ir ją sudarančių dokumentų reikalavimai būtų įgyvendinami priskirtuose TIS;

12.2. dalyvauti kibernetinio saugumo incidentų tyrimuose, rengiant pirminę informaciją apie incidentus bei teikiant duomenis kibernetinio saugumo vadovui;

12.3. organizuoti ir vykdyti kibernetinio saugumo priemonių diegimą ir stebėseną;

12.4. koordinuoti darbuotojų mokymus, susijusius su priskirtų kibernetiniu saugumu, bei užtikrinti darbuotojų informuotumą apie grėsmes ir prevencines priemones;

12.5. teikti nurodymus TIS administratoriams ir kitiems atsakingiems asmenims, siekiant laiku identifikuoti ir pašalinti saugumo spragas;

12.6. teikti kibernetinio saugumo vadovui reguliarias ataskaitas apie priskirtų TIS būklę, incidentus ir rizikos valdymo veiksmus;

12.7. vykdyti techninių saugumo sprendimų priežiūrą ir užtikrinti, kad TIS atitiktų nustatytus saugumo ir gerosios praktikos reikalavimus;

12.8. dalyvauti veiklos tęstinumo valdymo planų rengime, testavime ir įgyvendinime;

12.9. atlikti kitas Politikoje ir ją sudarančiuose kibernetinio saugumo dokumentuose bei kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

13. **TIS administratoriaus** funkcijos:

13.1. TIS naudotojų prieigos teisių valdymas;

13.2. TIS komponentų (kompiuterių, operacinių sistemų, duomenų bazių, taikomųjų programų, saugasienu, įsibrovimo aptikimo sistemų) priežiūra ir sąranka;

13.3. TIS pažeidžiamų vietų nustatymas;

13.4. saugumo reikalavimų atitikties nustatymas ir stebėseną;

13.5. reagavimą į kibernetinius incidentus.

14. **Fizinės saugos įgaliotinio** funkcijos nustatytos Įstaigos Fizinės apsaugos tvarkoje.

15. **SOC** funkcijos nustatytos Įstaigos Kibernetinių incidentų valdymo plane ir Žurnalinių

įrašų valdymo tvarkoje.

16. **Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupių** funkcijos nustatytos Įstaigos Veiklos tęstinumo valdymo tvarkoje.

V. ĮSIPAREIGOJIMAI

17. Įstaigos Politikos ir ją sudarančių kibernetinio saugumo dokumentuose nurodytų reikalavimų privalo laikytis visi Įstaigos darbuotojai ir trečiosios šalys.

18. Įstaigos darbuotojai pasirašytinai supažindinami su Įstaigos Politika ir ją sudarančiais kibernetinio saugumo dokumentais. Su Politikos ir ją sudarančių kibernetinio saugumo dokumentų bei jų pakeitimais supažindinimą yra atsakingas Kibernetinio saugumo vadovas arba kitas organizacijos vadovo įgaliotas asmuo.

19. Įstaiga Politiką viešina svetainėje, adresu www.skuodopspc.lt.

20. Įstaiga vadovaudamasi Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818, siekdama mažinti galimas kilti rizikas TIS paslaugų, darbų ar įrangos pirkimams, susijusiems su TIS projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, trečiosioms šalims (įskaitant subtiekęjus) nustato reikalavimus pagal Įstaigos Tiekimo grandinės saugumo valdymo tvarką ir juos numato sutartyse su trečiųjų šalių paslaugų tiekėjais (įskaitant subtiekęjus).

21. Įstaigos Kibernetinio saugumo vadovas arba kitas organizacijos vadovo įgaliotas asmuo sudaro trečiųjų šalių paslaugų tiekėjų sąrašą (įskaitant subtiekęjus), jį tvarko ir pasikeitus sutartims peržiūri ir atnaujiną periodiškai, bet ne rečiau kaip kartą per metus, ir kai įvyksta reikšmingi pokyčiai arba reikšmingi incidentai, susiję su trečiųjų šalių paslaugų tiekėjais (įskaitant subtiekęjus).

22. NKSC, atlikdamas Įstaigos patikrinimą, turi teisę pareikalauti, o Įstaiga privalo per 5 darbo dienas nuo NKSC prašymo gavimo dienos, pateikti:

22.1. Patvirtintos ar atnaujintos Politikos ir jos įgyvendinimą reglamentuojančių kibernetinio saugumo dokumentų kopijas;

22.2. Atliktų kibernetinio saugumo auditų, atitikties vertinimo ataskaitos ir nustatytų neatitikčių šalinimo plano, rizikų vertinimo ataskaitos ir rizikos valdymo planų kopijas;

22.3. Veiklos tęstinumo valdymo plano išbandymo ataskaitos kopiją.

VI. BAIGIAMOSIOS NUOSTATOS

23. Įstaigos kibernetinio saugumo vadovas reguliariai, ne rečiau kaip kartą per metus arba pasikeitus aplinkybėms, turi peržiūrėti ir, esant poreikiui, atnaujinti Politiką.

POLITIKOS ĮGYVENDINIMĄ REGLAMENTUOJANČIŲ KIBERNETINIO SAUGUMO DOKUMENTŲ SĄRAŠAS

1. Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarka;
2. Kibernetinių incidentų valdymo planas
3. Žurnalinių įrašų valdymo tvarka;
4. Tinklų ir informacinių sistemų veiklos tęstinumo valdymo tvarka;
5. Atsarginių duomenų kopijų valdymo tvarka;
6. Tiekimo grandinės saugumo valdymo tvarka;
7. Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo įskaitant spragų atskleidimo, pataisų ir pokyčių valdymo tvarka;
8. Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarka;
9. Kibernetinės higienos praktikos organizavimo ir kibernetinio saugumo mokymų organizavimo ir vykdymo tvarka;
10. Kriptografijos ir šifravimo naudojimo tvarka;
11. Fizinės apsaugos tvarka;
12. Tinklų ir informacinių sistemų turto valdymo tvarka;
13. Prieigų valdymo tvarka.