



**LIETUVOS RESPUBLIKOS KONKURENCIJOS TARYBOS
PIRMININKAS**

**ĮSAKYMAS
DĖL TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKOS
PATVIRTINIMO**

2026 m. d. Nr. 2V -

Vilnius

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 14 straipsniu ir Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“:

1. T v i r t i n u Tinklų ir informacinių sistemų kibernetinio saugumo politiką (pridedama).
2. Į p a r e i g o j u Konkurencijos tarybos vyresnįjį patarėją Martyną Plikusą – asmenį, atsakingą už Konkurencijos tarybos kibernetinio saugumo organizavimą ir užtikrinimą – iki 2026 m. balandžio 17 d. organizuoti:
 - 2.1. Tinklų ir informacinių sistemų kibernetinio saugumo politikos 1 priede nustatytų kibernetinio saugumo politikos įgyvendinimą reglamentuojančių dokumentų parengimą ir patvirtinimą;
 - 2.2. Duomenų apie patvirtintus kibernetinio saugumo politikos įgyvendinimą reglamentuojančius dokumentus ir šių dokumentų pateikimą į Kibernetinio saugumo informacinę sistemą.
3. P a v e d u Konkurencijos tarybos administracijos direktoriui Arūnui Keraminui kontroliuoti šio įsakymo vykdymą.

Pirmininkė

Jolanta Ivanauskienė

PATVIRTINTA

Lietuvos Respublikos konkurencijos
tarybos pirmininko

2026 m.

d. įsakymu Nr. 2V-

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKA

I SKYRIUS BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų kibernetinio saugumo politika (toliau – Kibernetinio saugumo politikos dokumentas) yra pagrindinis Lietuvos Respublikos konkurencijos tarybos (toliau – KT) kibernetinio saugumo valdymo dokumentas, kuris apibrėžia kibernetinio saugumo tikslus, teisės aktus, atsakingų asmenų funkcijas ir atsakomybes, įsipareigojimus KT valstybės pareigūnams, valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau kartu – darbuotojai) ir trečiosioms šalims.

2. Kibernetinio saugumo politikos dokumento 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 KT veiklą.

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

4. Kibernetinio saugumo politikos dokumente vartojamos sąvokos:

4.1. **Atitikties vertinimas** – KT atitikties reikalavimams, nustatytiems Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nutarimas Nr. 818), šiame Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose vertinimas;

4.2. **Kibernetinio saugumo vadovas** – KT 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;

4.3. **Rizikos vertinimas** – rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal KT patvirtintą Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarką;

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 šiame Kibernetinio saugumo politikos dokumente vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

II SKYRIUS TEISĖS AKTAI

6. Kibernetinį saugumą reglamentuojančių teisės aktų, kuriais vadovaujasi KT, sąrašas:
 - 6.1. Kibernetinio saugumo įstatymas;
 - 6.2. Lietuvos Respublikos komercinių paslapčių teisinės apsaugos įstatymas;
 - 6.3. Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;
 - 6.4. Lietuvos Respublikos konkurencijos įstatymas;
 - 6.5. Lietuvos Respublikos viešųjų pirkimų įstatymas;
 - 6.6. Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;
 - 6.7. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;
 - 6.8. Nutarimas Nr. 818;
 - 6.9. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;
 - 6.10. kiti teisės aktai, reglamentuojantys kibernetinį saugumą.
7. KT sudaromas institucijos Kibernetinio saugumo politikos įgyvendinimą reglamentuojančių dokumentų sąrašas (1 priedas).

III SKYRIUS FUNKCIJOS IR ATSAKOMYBĖS

8. KT pirmininkas privalo užtikrinti žmogiškųjų ir finansinių išteklių skyrimą kibernetinio saugumo valdymui.
9. KT pirmininkas ar jo įgaliotas asmuo įsakymu paskiria:
 - 9.1. Kibernetinio saugumo vadovą – asmenį, atsakingą už KT kibernetinio saugumo organizavimą ir užtikrinimą. KT privalo Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – NKSC) pateikti kibernetinio saugumo vadovo kontaktinę informaciją Kibernetinio saugumo informacinėje sistemoje (toliau – KSIS), ir informuoti KT darbuotojus. Organizacijai 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 apsaugos įgaliotinį;
 - 9.5. Saugumo operacijų centrą (toliau – SOC). SOC funkcijas gali vykdyti ir kiti organizacijos paskirti asmenys ar grupės pagal TIS paslaugų teikimo sutartis;
 - 9.6. Veiklos tęstinumo valdymo grupę;
 - 9.7. Veiklos atkūrimo grupę.
10. Kibernetinio saugumo vadovas, koordinuodamas ir prižiūrėdamas Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų įgyvendinimą, turi atlikti šias funkcijas:
 - 10.1. užtikrinti, kad Kibernetinio saugumo politikos dokumentas ir kibernetinio saugumo įgyvendinimą reglamentuojantys dokumentai būtų parengti ir periodiškai atnaujinami;

10.2. organizuoti KT atitikties vertinimą, rengti ir teikti tvirtinti organizacijos vadovui ar jo įgaliotam asmeniui Atitikties vertinimo ataskaitą ir Neatitiktį šalinimo planą bei jų patvirtinimo datas ir registracijos numerius 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 organizacijos vadovui ar jo įgaliotam asmeniui Rizikos vertinimo ataskaitas ir rizikos valdymo planus bei jų patvirtinimo datas ir registracijos numerius Kibernetinio saugumo įstatymo nustatyta tvarka, ne vėliau kaip per 5 darbo dienas, pateikti į NKSC administruojamą KSIS;

10.4. organizuoti TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymą, rengti ir teikti tvirtinti organizacijos vadovui ar jo įgaliotam asmeniui TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo rezultatų ataskaitas ir jų patvirtinimo datas ir registracijos numerius 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, saugos įgaliotiniui ir (ar) naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų įgyvendinimu;

10.8. atlikti TIS saugos įgaliotinio funkcijas, išskyrus atvejus kai šias funkcijas ar jų dalį atlieka tiekėjas pagal viešųjų pirkimų būdu sudarytą paslaugų sutartį.

10.9. atlikti kitas Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose 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 TIS administravimu ar kitomis pareigybėmis, susijusiomis su techninės kompiuterinės įrangos ar programinės įrangos priežiūra ir valdymu.

12. Saugos įgaliotinio funkcijos:

12.1. užtikrinti, kad Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatyti reikalavimai būtų įgyvendinami priskirtuose TIS;

12.2. dalyvauti kibernetinio saugumo incidentų tyrimuose, rengiant 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 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 Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose bei kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

13. TIS administratoriaus funkcijos:
 - 13.1. valdyti TIS naudotojų prieigos teises;
 - 13.2. prižiūrėti TIS komponentus (kompiuterių, operacinių sistemų, duomenų bazių, taikomųjų programų, saugasienui, įsibrovimo aptikimo sistemų);
 - 13.3. valdyti TIS komponentų sąranką;
 - 13.4. nustatyti TIS pažeidžiamas vietas;
 - 13.5. nustatyti ir stebėti saugumo reikalavimų atitikti, reagavimą į kibernetinius incidentus.
14. Fizinės apsaugos įgaliotinio funkcijos nustatytos Fizinės apsaugos tvarkoje.
15. SOC funkcijos nustatytos Kibernetinių incidentų valdymo plane.
16. Veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės funkcijos nustatytos Veiklos tęstinumo valdymo tvarkoje.

IV SKYRIUS ĮSIPAREIGOJIMAI

17. Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų privalo laikytis visi darbuotojai, taip pat studentų praktiką, savanorišką praktiką ar stažuotę KT atliekantys asmenys. Šis dokumentas taip pat taikomas fiziniams ir juridiniams asmenims, kurie sutartiniais ar kitais pagrindais gali turėti ar turėjo prieigą prie TIS.

18. Darbuotojai pasirašytinai supažindinami su Kibernetinio saugumo politikos dokumentu ir kibernetinio saugumo įgyvendinimą reglamentuojančiais dokumentais. Už supažindinimą su Kibernetinio saugumo politikos dokumentu ir kibernetinio saugumo įgyvendinimą reglamentuojančiais dokumentais bei jų pakeitimais yra atsakingas kibernetinio saugumo vadovas arba kitas organizacijos vadovo įgaliotas asmuo.

19. Organizacija vadovaudamasi 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 subtiekejus) nustato reikalavimus pagal Tiekimo grandinės saugumo valdymo tvarką ir juos numato sutartyse su trečiųjų šalių paslaugų tiekėjais (įskaitant subtiekejus).

20. KT kibernetinio saugumo vadovas sudaro trečiųjų šalių paslaugų tiekėjų sąrašą (įskaitant subtiekejus), jį tvarko ir pasikeitus sutartims peržiūri ir atnaujina periodiškai, bet ne rečiau kaip kartą per metus, ir kai įvyksta reikšmingi pokyčiai arba reikšmingi incidentai, susiję su trečiųjų šalių paslaugų tiekėjais (įskaitant subtiekejus).

21. NKSC, atlikdamas KT patikrinimą, turi teisę pareikalauti, o organizacija privalo per 5 darbo dienas nuo NKSC prašymo gavimo dienos, pateikti:

- 21.1. Patvirtintus Kibernetinio saugumo politikos dokumento ir kibernetinio saugumo įgyvendinimą reglamentuojančių dokumentų kopijas;
- 21.2. Atliktų kibernetinio saugumo auditų, atitikties vertinimo ataskaitos ir nustatytų neatitikčių šalinimo plano, rizikų vertinimo ataskaitos ir rizikos valdymo planų kopijas;
- 21.3. Veiklos tęstinumo valdymo plano išbandymo ataskaitos kopiją.

V SKYRIUS

BAIGIAMOSIOS NUOSTATOS

22. Kibernetinio saugumo politikos dokumentas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba kai atsiranda esminiai pokyčiai.

**KIBERNETINIO SAUGUMO POLITIKOS ĮGYVENDINIMĄ REGLAMENTUOJANČIŲ
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 valdymą ir atskleidimą, 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. Turto valdymo tvarka;
13. Prieigų valdymo tvarka.

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Lietuvos Respublikos konkurencijos taryba 188668192, Jogailos g. 14, Vilnius 01116
Dokumento pavadinimas (antraštė)	DĖL TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKOS PATVIRTINIMO
Dokumento registracijos data ir numeris	2026-03-06 Nr. 2V-10
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Jolanta Ivanauskienė, Pirmininkė, Konkurencijos tarybos nariai
Sertifikatas išduotas	JOLANTA IVANAUSKIENĖ LT
Parašo sukūrimo data ir laikas	2026-03-06 08:41:23 (GMT+02:00)
Parašo formatas	XAdES-EPES
Laiko žymoje nurodytas laikas	–
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2023-06-09 17:30:35 – 2028-06-07 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA-2, VI Registru Centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Lietuvos Respublikos konkurencijos taryba, į.k. 188668192 LT", sertifikatas galioja nuo 2024-12-18 13:28:57 iki 2027-12-18 13:28:57
Pagrindinio dokumento priedų skaičius	–
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Priedamo dokumento sudarytojas (-ai)	–
Priedamo dokumento pavadinimas (antraštė)	–
Priedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.88
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2026-06-18 13:58:56)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2026-06-18 13:58:57 Dokumentų valdymo sistema Avilys