

**LIETUVOS AUDITORIŲ RŪMŲ PREZIDIUMO
N U T A R I M A S**

**DĖL LIETUVOS AUDITORIŲ RŪMŲ TINKLŲ IR INFORMACINIŲ SISTEMŲ
KIBERNETINIO SAUGUMO POLITIKOS APRAŠO TVIRTINIMO**

2026 m. balandžio 28 d. Nr. 1.4-32.7.1.1

Vilnius

Vadovaudamasis Lietuvos Respublikos kibernetinio saugumo įstatymo 14 straipsniu, Lietuvos auditorių rūmų prezidiumas **n u t a r i a** :

tvirtinti Lietuvos auditorių rūmų tinklų ir informacinių sistemų kibernetinio saugumo politikos aprašą (pridedama).

PREZIDENTĖ

VAIDA KAČERGIENĖ

PATVIRTINTA
Lietuvos auditorių rūmų prezidiumo
2026 m. balandžio 28 d. nutarimu
Nr. 1.4-32.7.1.1

**LIETUVOS AUDITORIŲ RŪMŲ TINKLŲ IR INFORMACINIŲ SISTEMŲ
KIBERNETINIO SAUGUMO POLITIKOS APRAŠAS**

**I SKYRIUS
BENDROSIOS NUOSTATOS**

1. Lietuvos auditorių rūmų tinklų ir informacinių sistemų kibernetinio saugumo politikos aprašas (toliau – Kibernetinio saugumo politikos aprašas) yra pagrindinis Lietuvos auditorių rūmų (toliau – LAR) kibernetinio saugumo valdymo dokumentas, reglamentuojantis LAR valdomų ir (ar) tvarkomų tinklų ir informacinių sistemų, naudojamų LAR funkcijoms atlikti ar paslaugoms teikti, (toliau – TIS) atitiktį kibernetinio saugumo rizikos valdymo priemonėms, apibrėžiantis kibernetinio saugumo tikslus, atsakingų asmenų funkcijas ir atsakomybę bei bendruosius reikalavimus.

2. Kibernetinio saugumo politikos aprašas yra taikomas LAR tinklams ir LAR valdomoms ir tvarkomoms informacinėms sistemoms, kurių sąrašas tvirtinamas LAR direktoriaus įsakymu.

3. Kibernetinio saugumo politikos aprašą ir kitus susijusius dokumentus, kuriais įgyvendinamas kibernetinis saugumas, tvirtina LAR prezidiumas.

4. Kibernetinio saugumo politikos aprašo tikslas – užtikrinti LAR TIS saugumą, nepertraukiamą veikimą, LAR duomenų ir informacijos, nustatytos LAR konfidencialios

informacijos apsaugos tvarkos apraše, slaptumą, konfidencialumą, prieinamumą ir atsparumą, tinkamą LAR ir LAR narių, audito įmonių bei auditoriaus padėjėjų teisių ir teisėtų interesų apsaugą.

5. LAR kibernetinis saugumas grindžiamas kibernetinio saugumo principais, kurie numatyti Lietuvos Respublikos kibernetinio saugumo įstatymo (toliau – Kibernetinio saugumo įstatymas) 3 straipsnyje.

6. Kibernetinio saugumo politikos apraše vartojamos sąvokos:

6.1. **Atitikties vertinimas** – LAR atitikties reikalavimams, nustatytiems Lietuvos Respublikos kibernetinio saugumo įstatyme, kituose kibernetinio saugumo įgyvendinimą reglamentuojančiuose teisės aktuose ir šio Kibernetinio saugumo politikos apraše, vertinimas.

6.2. **Kibernetinio saugumo vadovas** – LAR direktoriaus paskirtas LAR darbuotojas, atsakingas už LAR kibernetinio saugumo organizavimą, koordinavimą ir priežiūrą bei kibernetinio saugumo reikalavimų įgyvendinimo užtikrinimą, arba LAR iš tiekėjo įsigytos paslaugos, kurias teikiant būtų atliekamos kibernetinio saugumo vadovo funkcijos.

6.3. **TIS saugos įgaliotinis** (toliau – Saugos įgaliotinis) – LAR direktoriaus įsakymu paskirtas darbuotojas, atsakingas už priskirtų LAR TIS ar jų dalių kibernetinio saugumo atitikties užtikrinimą bei kibernetinio saugumo vadovo pavestų ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytų funkcijų vykdymą, arba LAR iš teikėjo įsigytos paslaugos, kurias teikiant būtų atliekamos Saugos įgaliotinio funkcijos.

6.4. **Rizikos vertinimas** – rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal LAR prezidiumo patvirtintą Kibernetinio saugumo užtikrinimo LAR tvarkos aprašą.

7. Kitos šiame Kibernetinio saugumo politikos apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo politikos aprašo 8 punkte nurodytuose teisės aktuose.

8. Kibernetinis saugumas LAR užtikrinamas vadovaujantis šiais teisės aktais:

8.1. Kibernetinio saugumo įstatymu;

8.2. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ patvirtintais teisės aktais (toliau – Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818);

8.3. Lietuvos Respublikos finansinių ataskaitų audito ir kitų užtikrinimo paslaugų įstatymu;

8.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu bei kitais susijusiais teisės aktais;

8.5. Kibernetinio saugumo užtikrinimo LAR tvarkos aprašas;

8.6. kitais teisės aktais, reglamentuojančiais kibernetinį saugumą.

II SKYRIUS

FUNKCIJOS IR ATSAKOMYBĖS

9. LAR direktorius įsakymu paskiria:

9.1. Kibernetinio saugumo vadovą. LAR 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 LAR darbuotojus.

9.2. Saugos įgaliotinį.

9.3. TIS administratorių (-ius), atsakingą (-us) už informacinių sistemų, tinklų ir infrastruktūros administravimą.

9.4. Fizinės apsaugos įgaliotinį, atsakingą už fizinio saugumo priemonių įgyvendinimą.

9.5. Saugumo operacijų centrą (toliau – SOC) arba subjektą, atliekantį SOC funkcijas pagal paslaugų sutartį. SOC funkcijas gali atlikti ir kiti LAR direktoriaus įsakymu paskirti asmenys ar grupės pagal TIS paslaugų teikimo sutartį.

9.6. Veiklos testinimo valdymo ir veiklos atkūrimo grupę, kurios atsakingos už veiklos testinimo priemonių planavimą ir įgyvendinimą.

10. Kibernetinio saugumo vadovas, koordinuodamas ir prižiūrėdamas Kibernetinio saugumo politikos apraše ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose teisės aktuose nustatytų reikalavimų įgyvendinimą, turi atlikti šias funkcijas:

10.1. užtikrinti, kad kibernetinio saugumo politikos dokumentai būtų parengti ir periodiškai atnaujinami remiantis Kibernetinio saugumo įstatymo ir jį įgyvendinančių teisės aktų reikalavimais;

10.2. organizuoti LAR atitikties kibernetinio saugumo įgyvendinimą reglamentuojančių teisės aktų reikalavimams vertinimą NKSC patvirtintos Kibernetinio saugumo auditų atlikimo metodikos nustatyta tvarka;

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

10.4. teikti TIS administratoriui (-iams), Saugos įgaliotiniui, jeigu saugos įgaliotinio funkcijas atlieka ne Kibernetinio saugumo vadovas, ir (ar) naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su kibernetinio saugumo politikos apraše nustatytų reikalavimų įgyvendinimu;

10.5. organizuoti rizikos vertinimą ir dalyvauti rizikos vertinimo procese, rengti ir teikti tvirtinti LAR direktoriui rizikos vertinimo ataskaitas ir rizikos valdymo planus;

10.6. organizuoti TIS veiklos testinimo valdymo plano veiksmingumo išbandymą, rengti ir teikti tvirtinti LAR direktoriui TIS veiklos testinimo valdymo plano veiksmingumo išbandymo rezultatų ataskaitą;

10.7. organizuoti darbuotojų mokymus kibernetinio saugumo klausimais;

10.8. atlikti kitas kibernetinio saugumo politikos apraše ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

11. Kibernetinio saugumo vadovas turi pateikti ir (ar) atnaujinti Kibernetinio saugumo politikos prašo 10.1, 10.5 ir 10.6 punktuose nurodytų dokumentų patvirtinimo duomenis, nurodydamas dokumentų pavadinimą, patvirtinimo datą ir registracijos numerį, NKSC į KSIS ne vėliau kaip per 5 darbo dienas nuo šių dokumento (-ų) patvirtinimo ir (ar) pakeitimo dienos.

12. **Saugos įgaliotinio funkcijos:**

12.1. rengti LAR teisės aktų ir kitų susijusių dokumentų, reglamentuojančių kibernetinio saugumo įgyvendinimą projektus, vykdyti jų periodinę peržiūrą ir teikti siūlymus dėl jų atnaujinimo;

12.2. užtikrinti, kad Kibernetinio saugumo politikos apraše ir kituose kibernetinio saugumo įgyvendinimą reglamentuojančiuose teisės aktuose nustatyti reikalavimai būtų įgyvendinami TIS;

12.3. dalyvauti rizikos vertinimo procese: rinkti informaciją, rengti rizikos vertinimo dokumentų projektus, rengti rizikos valdymo planų projektus ir teikti reikalingus duomenis kibernetinio saugumo vadovui;

12.4. vykdyti priskirtų TIS nuolatinę kibernetinio saugumo būklės stebėseną, stebėti identifikuotas spragas, incidentus ir rizikos valdymo priemonių įgyvendinimą;

12.5. dalyvauti kibernetinio saugumo incidentų tyrimuose, rengiant informaciją apie incidentus bei teikiant duomenis kibernetinio saugumo vadovui, jeigu kibernetinio saugumo vadovui nepriskirtos saugumo įgaliotinio funkcijos;

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

- 12.7. koordinuoti darbuotojų mokymus, susijusius su kibernetiniu saugumu, bei užtikrinti darbuotojų informuotumą apie taikomas kibernetinio saugumo priemones ir grėsmes;
- 12.8. teikti nurodymus TIS administratoriui (-iams) ir kitiems atsakingiems asmenims, siekiant laiku identifikuoti ir pašalinti saugumo spragas;
- 12.9. teikti kibernetinio saugumo vadovui reguliariai informaciją apie priskirtų TIS būklę, incidentus ir rizikos valdymo veiksmus;
- 12.10. vykdyti techninių saugumo sprendimų priežiūrą ir užtikrinti, kad TIS atitiktų nustatytus saugumo ir gerosios praktikos reikalavimus;
- 12.11. dalyvauti veiklos tęstinumo valdymo planų rengime, testavime ir įgyvendinime;
- 12.12. atlikti kitas Kibernetinio saugumo politikos apraše ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.
13. Saugos įgaliotinio funkcijų vykdymas gali būti paskirtas kibernetinio saugumo vadovui.
14. 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.
15. TIS administratoriaus funkcijos:
- 15.1. valdyti TIS naudotojų prieigos teises;
- 15.2. prižiūrėti TIS komponentus (kompiuterių, operacinių sistemų, duomenų bazių, taikomųjų programų, saugasienių, įsibrovimo aptikimo sistemų);
- 15.3. valdyti TIS komponentų sąranką;
- 15.4. nustatyti TIS pažeidžiamas vietas;
- 15.5. nustatyti ir stebėti saugumo reikalavimų atitiktį, reagavimą į kibernetinius incidentus.
16. Fizinės apsaugos įgaliotinio, SOC ir Veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės funkcijos nustatytos Kibernetinio saugumo užtikrinimo LAR tvarkos apraše.

III SKYRIUS

ĮSIPAREIGOJIMAI

17. Kibernetinio saugumo politikos apraše ir Kibernetinio saugumo užtikrinimo LAR tvarkos apraše nustatytų reikalavimų privalo laikytis LAR prezidentas, LAR administracijos darbuotojai, o trečiosios šalys – sutartyse nustatyta apimtimi, kiek tai susiję su jų veikla LAR TIS.
18. LAR prezidentas ir LAR administracijos darbuotojai pasirašytinai supažindinami su Kibernetinio saugumo politikos aprašu ir Kibernetinio saugumo užtikrinimo LAR tvarkos aprašu. Kibernetinio saugumo vadovas yra atsakingas už supažindinimą.
19. Vadovaudamiesi Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 ir siekdami mažinti rizikas, susijusias su TIS paslaugų, darbų ar įrangos pirkimais (projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ar kibernetinio saugumo užtikrinimu), LAR trečiosioms šalims (įskaitant subteikėjus) nustato reikalavimus pagal Kibernetinio saugumo užtikrinimo LAR tvarkos aprašą ir šiuos reikalavimus įtraukia į sutartis su paslaugų teikėjais.
20. Kibernetinio saugumo vadovas arba sutarties įgyvendinimą užtikrinantis atsakingas darbuotojas sudaro trečiųjų šalių paslaugų teikėjų (įskaitant subteikėjus) sąrašą, jį tvarko, peržiūri ir atnaujiną periodiškai, bet ne rečiau kaip kartą per metus, taip pat kai įvyksta reikšmingi pokyčiai arba reikšmingi incidentai, susiję su trečiųjų šalių paslaugų teikėjais ar kitos aplinkybės, galinčios turėti reikšmingą poveikį LAR kibernetiniam saugumui.
21. NKSC, atlikdamas LAR patikrinimą, turi teisę pareikalauti, o LAR privalo per 5 darbo dienas nuo NKSC prašymo gavimo dienos, pateikti:

21.1. patvirtintus Kibernetinio saugumo politikos aprašo 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.

IV SKYRIUS

BAIGIAMOSIOS NUOSTATOS

22. Kibernetinio saugumo politikos aprašas peržiūrimas ir, esant poreikiui, atnaujinamas ne rečiau kaip kartą per metus, taip pat pasikeitus teisės aktams, įsigaliojus naujiems kibernetinio saugumo reikalavimams, pasikeitus LAR organizacinei struktūrai ar technologinei aplinkai, arba atsiradus kitiems esminiams pokyčiams, lemiantiems tokios peržiūros būtinybę.

23. Kibernetinio saugumo politikos aprašas įsigalioja nuo jo patvirtinimo dienos.
