ŽUVININKYSTĖS TARNYBOS
PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS
DIREKTORIUS

ĮSAKYMAS
DĖL TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO RIZIKOS VERTINIMO IR VALDYMO TVARKOS PATVIRTINIMO

2026 m. birželio 15 d. Nr. V1-85
Klaipėda

Vadovaudamasis Lietuvos Respublikos kibernetinio saugumo įstatymo 14 straipsnio 1 dalies 1 punktu ir įgyvendindamas Kibernetinio saugumo reikalavimų aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“:

1. Tvirtinu Tinklų ir informacinių sistemų kibernetinio saugumo rizikos vertinimo ir valdymo tvarką (pridedama).

2. Nustatau, kad šis įsakymas įsigalioja nuo jo pasirašymo dienos.

Žuvivaisos departamento direktorius,
laikinai atliekantis direktoriaus funkcijas Justas Poviliūnas

PATVIRTINTA
Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos direktoriaus 2026 m. birželio 15 d. įsakymu Nr. V1-85

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO RIZIKOS VERTINIMO IR VALDYMO TVARKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų (toliau – TIS) kibernetinio saugumo rizikos vertinimo ir valdymo tvarka (toliau – Tvarka) reglamentuoja Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Tarnybos) TIS kibernetinio saugumo rizikos vertinimo, valdymo ir stebėsenos procesą, už šį procesą atsakingų padalinių ir darbuotojų funkcijas ir atsakomybes.

2. Tvarka taikoma atliekant Tarnybos TIS kibernetinio saugumo rizikos vertinimą, valdant rizikas ir vykdant jų stebėseną.

3. Šioje Tvarkoje naudojamos sąvokos:

3.1. **Kibernetinio saugumo rizika** (toliau – rizika) – galimybė, kad dėl kibernetinio incidento bus sutrikdytas TIS konfidencialumas, vientisumas ar prieinamumas ir dėl to bus padarytas neigiamas poveikis Tarnybos veiklai. Kibernetinio saugumo rizika išreiškiama kaip poveikio Tarnybos veiklai masto ir kibernetinio incidento tikimybės derinys;

3.2. **Likutinė rizika** – rizika, liekanti po rizikos valdymo priemonių įgyvendinimo;

3.3. **Rizikų registras** – šios Tvarkos 1 priede esančios Rizikos registro formos pagrindu parengtas Tarnybos identifikuotų kibernetinio saugumo rizikų ir jų savininkų sąrašas, taip pat rizikos vertinimo rezultatai;

3.4. **Rizikos savininkas –** Tarnybos darbuotojas, Rizikų registre paskirtas vykdyti rizikos savininko funkcijas, t. y. vertinti ir stebėti riziką bei užtikrinti jos efektyvų valdymą;

3.5. **Rizikos valdymo priemonės vykdytojas** – Tarnybos darbuotojas, Rizikų valdymo plane paskirtas vykdyti rizikos valdymo priemonės vykdytojo funkcijas, t. y. įgyvendinti rizikų valdymo plane numatytą rizikos valdymo priemonę;

3.6. **Rizikos vertinimas** – procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą;

3.7. **Rizikų vertinimo ataskaita** (toliau – RVA) – Tarnybos direktoriaus patvirtintas dokumentas, kuriame aprašomi rizikos vertinimo rezultatai, nurodomos vertintos TIS ar TIS grupės ir su jomis susijusios Tarnybos funkcijos ar paslaugos, identifikuotos grėsmės, pažeidžiamumai ir rizikos, jų tikimybė, poveikis, bendras rizikos balas (RP), rizikos grupė pagal tolerancijos lygį bei rizikos valdymo sprendimai. RVA sudėtinė dalis yra rizikų valdymo planas.

3.8. **Rizikų valdymo planas** (toliau – RVP) – RVA sudėtinė dalis, rengiama pagal šios Tvarkos 2 priede esančią formą, kurioje pateikiamos Tarnybos nepriimtinoms rizikoms numatytos valdymo priemonės, jų įgyvendinimo prioritetai, terminai, reikalingi ištekliai, atsakingi vykdytojai, taip pat dabartinės ir numatomos likutinės rizikos vertinimai.

3.9. **Saugos įgaliotinis** – Tarnybos vadovo paskirtas darbuotojas arba paslaugų teikėjas, vykdantis informacijos ir kibernetinio saugumo priežiūros, konsultavimo ir kontrolės funkcijas.

4. Kitos šioje Tvarkoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Lietuvos Respublikos kibernetinio saugumo įstatyme (toliau – Kibernetinio saugumo įstatymas) ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose.

5. Kibernetinio saugumo vadovas ne rečiau kaip kartą per metus organizuoja Tarnybos TIS kibernetinio saugumo rizikos vertinimą. Prireikus gali būti organizuojamas neeilinis Tarnybos TIS kibernetinio saugumo rizikos vertinimas.

6. Neeilinį rizikos vertinimą inicijuoja kibernetinio saugumo vadovas arba saugos įgaliotinis.

7. Neeilinis Tarnybos rizikos vertinimas gali būti atliekamas, kai įvyksta esminiai pokyčiai, darantys įtaką Tarnybos veiklai ir kibernetiniam saugumui:

7.1. inicijuojama nauja arba iš esmės keičiama organizacijos veikla ir (ar) pagrindiniai veiklos procesai (teikiamos paslaugos);

7.2. sukuriama nauja TIS arba iš esmės modernizuojama jau veikianti TIS, prieš ją diegiant į gamybinę aplinką;

7.3. migruojama į debesijos paslaugas ar migruojama iš debesijos paslaugų;

7.4. atliekami esminiai TIS programinės ir (ar) aparatinės įrangos pakeitimai;

7.5. pakeičiamos administracinės ir (ar) serverinių, duomenų centrų bei IT tinklo įrangos patalpos ir (ar) persikeliama į kitus pastatus;

7.6. įvyksta didelis kibernetinis incidentas;

7.7. TIS skenavimo (pvz., pažeidžiamumų skenavimo, įsilaužimų testavimo ir pan.) ar programinio kodo saugumo vertinimo metu nustatomi kritinės ir didelės rizikos pažeidžiamumai;

7.8. pasikeičia darbuotojai, administruojantys ar prižiūrintys TIS ir dėl to gali būti reikšmingai paveiktas TIS veikimo ar kibernetinio saugumo užtikrinimo tęstinumas;

7.9. pasikeičia TIS priežiūros ir vystymo paslaugų tiekėjai, kurie Tarnybai teikia TIS saugumui, veiklos tęstinumui reikšmingas paslaugas;

7.10. kiti esminiai pokyčiai, darantys įtaką Tarnybos veiklai ir kibernetiniam saugumui.

8. Tvarka yra skirta visiems Tarnybos darbuotojams, dalyvaujantiems rizikos vertinimo procese.

9. Šios Tvarkos nuostatos taip pat gali būti taikomos Tarnybos tiekėjams (įskaitant subtiekėjus), kiek tai susiję su teikiamomis paslaugomis ir numatytais kibernetinio saugumo reikalavimais pagal Kibernetinio saugumo reikalavimų aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (aktualią redakciją).

10. Jeigu saugos įgaliotinio funkcijas vykdo išorinis paslaugų tiekėjas, jis privalo užtikrinti rizikos vertinimo metu gautos informacijos konfidencialumą ir laikytis saugos įgaliotinio funkcijas reglamentuojančių Lietuvos Respublikos teisės aktų, Tarnybos vidaus teisės aktų bei sutartinių įsipareigojimų.

II SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

11. Tarnybos direktoriaus funkcijos ir atsakomybės:

11.1. tvirtina RVA, kurios sudėtinė dalis yra RVP;

11.2. RVP numatytoms priemonėms įgyvendinti skiria reikiamus išteklius;

11.3. priima sprendimus dėl nepriimtinos rizikos toleravimo.

12. Kibernetinio saugumo vadovo funkcijos ir atsakomybės:

12.1. koordinuoja ir kontroliuoja rizikos vertinimo ir valdymo procesą;

12.2. teikia tvirtinti Tarnybos direktoriui RVA, kurios sudėtinė dalis yra RVP;

12.3. kartu su TIS savininkais identifikuoja ir klasifikuoja TIS;

12.4. kartu su TIS, rizikos savininkais ir saugos įgaliotiniu identifikuoja esamas ir galimas TIS grėsmes ir pažeidžiamumus;

12.5. identifikuotas rizikas registruoja Rizikų registre;

12.6. paskiria darbuotoją konkrečios rizikos savininku kiekvienai rizikai stebėti ir valdyti, jį įrašo į Rizikų registrą;

12.7. kartu su rizikos savininkais nustato bendrą rizikos balą (RP);

12.8. padeda rizikos savininkams parinkti rizikos valdymo priemones;

12.9. parengia RVA;

12.10. konsultuoja darbuotojus rizikos vertinimo ir valdymo klausimais;

12.11. pateikia informaciją apie Tarnybos atliktą rizikos vertinimą Kibernetinio saugumo įstatymo ir jo įgyvendinimą reglamentuojančių teisės aktų nustatyta tvarka ir terminais Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) administruojamą Kibernetinio saugumo informacinę sistemą (toliau – KSIS).

13. Saugos įgaliotinio funkcijos ir atsakomybės:

13.1. dalyvauja organizuojant ir vykdant rizikos vertinimą;

13.2. kartu su kibernetinio saugumo vadovu ir TIS savininkais identifikuoja grėsmes ir pažeidžiamumus;

13.3. dalyvauja vertinant rizikos tikimybę ir poveikį;

13.4. teikia siūlymus dėl rizikos valdymo priemonių;

13.5. stebi rizikos valdymo priemonių įgyvendinimą;

13.6. konsultuoja Tarnybos darbuotojus informacijos ir kibernetinio saugumo klausimais;

13.7. informuoja kibernetinio saugumo vadovą apie nustatytus reikšmingus pažeidžiamumus ar rizikas.

14. Rizikos savininko funkcijos ir atsakomybės:

14.1. kartu su TIS savininkais vertina esamas ir galimas TIS grėsmes bei egzistuojančius pažeidžiamumus, kurių sąsaja sukelia riziką;

14.2. nustato bendrą rizikos balą (RP), įvertina rizikos poveikio ir tikimybės lygį bei priskiria riziką atitinkamai rizikos grupei pagal tolerancijos lygį;

14.3. nustato rizikos valdymo būdą;

14.4. nepriimtinoms rizikoms valdyti parenka ir RVP suplanuoja rizikos valdymo priemones, paskiria už jų įgyvendinimą atsakingus rizikos valdymo priemonių vykdytojus, nustato įgyvendinimo terminus bei įvertina dabartinę ir numatomą likutinę riziką;

14.5. įvertina likutinės rizikos tikimybę, poveikį, bendrą rizikos balą (RP) ir likutinės rizikos grupę;

14.6. stebi rizikos valdymo priemonių įgyvendinimą ir efektyvumą;

14.7. vykdo nustatytos rizikos stebėseną;

14.8. ne rečiau kaip kartą per ketvirtį peržiūri RVP įgyvendinimo būklę.

15. TIS savininko funkcijos ir atsakomybės:

15.1. rizikos savininkams padeda identifikuoti ir įvertinti kibernetinio saugumo rizikas, kurios gali pasireikšti TIS, už kurių valdymą jis yra atsakingas;

15.2. rizikos savininkams padeda nepriimtinoms rizikoms parinkti ir suplanuoti RVP;

15.3. teikia informaciją apie TIS pokyčius, galinčius turėti įtakos rizikos lygiui.

16. Rizikos valdymo priemonės vykdytojas, derindamas savo veiksmus su TIS savininku,

įgyvendina RVP numatytas priemones nepriimtinoms rizikoms valdyti.

17. Jeigu tas pats asmuo Tarnyboje vykdo ir kibernetinio saugumo vadovo, ir saugos įgaliotinio funkcijas, šioje Tvarkoje abiem funkcijoms nustatytos atsakomybės vykdomos vieno asmens.

III SKYRIUS
RIZIKOS VERTINIMAS

18. Rizikos vertinimo tarpiniai ir detalūs duomenys bei skaičiavimai fiksuojami Rizikos registre, kuris rengiamas pagal šios Tvarkos 1 priede esančią formą ir kurį tvarko kibernetinio saugumo vadovas.

19. Rizikos vertinimo apibendrinti rezultatai ir RVP pateikiami RVA.

20. Rizikos vertinimas gali būti atliekamas vadovaujantis tarptautiniu standartu IEC/ISO 27005 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo rizikos valdymas“ (aktualia redakcija) ar NKSC išleista „Kibernetinio saugumo rizikos vertinimo metodika“ (toliau – Rizikos vertinimo metodika).

21. Tarnyba taip pat gali taikyti kitą rizikos vertinimo metodiką, jeigu ji užtikrina teisės aktuose nustatytų kibernetinio saugumo rizikos vertinimo reikalavimų įgyvendinimą.

22. Rizikos vertinimo procesą sudaro 3 (trys) pagrindiniai etapai:

22.1. rizikos identifikavimas;

22.2. rizikos analizė;

22.3. rizikos įvertinimas.

23. Rizikos identifikavimo metu kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis kartu su organizacijos TIS savininkais identifikuoja ir klasifikuoja TIS, kurių atžvilgiu atliekamas rizikos vertinimas, bei nustato jų palaikomas Tarnybos funkcijas ir (ar) paslaugas.

24. Pagal kiekvieną TIS ar jų grupę kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis kartu su TIS savininkais identifikuoja ir klasifikuoja rizikas, atsižvelgdamas į TIS palaikomas Tarnybos funkcijas ir (ar) paslaugas, aktualias grėsmes bei pažeidžiamumus.

25. Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis visas identifikuotas rizikas registruoja Rizikų registre ir kiekvienai rizikai priskiria rizikos savininką.

26. Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis kartu su TIS savininkais kiekvienam vertinamam TIS nustato esamas ir galimas TIS grėsmes ir pažeidžiamumus, susieja juos su paveikiamomis Tarnybos funkcijomis ar paslaugomis ir juos įrašo Rizikų registre.

27. Grėsmės gali būti identifikuojamos šiais būdais:

27.1. renkant informaciją iš vidinių šaltinių;

27.2. gaunant informaciją iš išorinių šaltinių, įskaitant atviruųjų šaltinių žvalgybą (OSINT);

27.3. atliekant kibernetinio saugumo valdymo atitikties vertinimą;

27.4. analizuojant kibernetinio saugumo incidentų ataskaitas.

28. Pažeidžiamumai gali būti nustatomi šiais būdais:

28.1. atliekant automatizuotus TIS skenavimus;

28.2. atliekant TIS saugumo testavimus ir įvertinimus;

28.3. atliekant TIS įsilaužimų testavimus;

28.4. apklausiant darbuotojus;

28.5. atliekant fizinę apžiūrą;

28.6. atliekant kibernetinio saugumo valdymo atitikties Kibernetinio saugumo įstatymo ir jo įgyvendinimą reglamentuojančių teisės aktų bei Kibernetinio saugumo politikos ir jos

įgyvendinimą reglamentuojančių vidaus tvarkų reikalavimams ;

28.7. atliekant kibernetinio saugumo auditus;

28.8. analizuojant dokumentus.

29. Pažeidžiamumai gali būti nustatomi šiose srityse:

29.1. veiklos procesuose ir procedūrose;

29.2. darbuotojų veikloje;

29.3. fizinėje aplinkoje;

29.4. TIS sąrankoje (konfigūracijoje);

29.5. techninėje ir programinėje įrangoje;

29.6. trečiųjų šalių teikiamose paslaugose.

30. Identifikuojant grėsmes ir pažeidžiamumus gali būti naudojamasi Rizikos vertinimo metodikoje pateiktu tipinių grėsmių ir pažeidžiamumų sąrašu.

31. Rizikos identifikavimo metu taip pat turi būti surenkama informacija apie Tarnybos turimas rizikos valdymo priemones, įskaitant kibernetinio saugumo priemones.

32. Rizikos analizės metu kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis kartu su rizikos ir TIS savininkais įvertina kiekvienos rizikos tikimybę ir poveikį balais nuo 1 iki 5 bei apskaičiuoja bendrą rizikos balą (RP) pagal formulę:

$$RP = (1{,}5 \times P) + (0{,}5 \times T)$$, kur P – poveikio balas, o T – tikimybės balas.

Tikimybės ir poveikio vertinimui galima naudotis šios tvarkos 3 priede pateiktais kriterijais ir jų aprašymu.

33. Rizikos analizės metu, siekiant nustatyti rizikos tikimybę ir poveikį, gali būti atliekamas Tarnybos turimų rizikos valdymo priemonių, įskaitant kibernetinio saugumo priemonių, vertinimas (atliekant rizikos analizę galima remtis Kibernetinio saugumo rizikos vertinimo metodikoje numatyta rizikos analizės įgyvendinimo tvarka).

34. Bendras rizikos balas (RP) nustatomas taikant poveikio koeficientą KP = 1,5 ir tikimybės koeficientą KT = 0,5, t. y. $RP = (KP \times P) + (KT \times T)$. Poveikiui suteikiamas didesnis svoris siekiant didesnę reikšmę suteikti rizikoms, galinčioms turėti didžiausią poveikį Tarnybos veiklos tęstinumui ir kritinių funkcijų vykdymui.

35. Rizikos įvertinimo metu kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis kartu su rizikos savininkais priskiria riziką atitinkamai rizikos grupei pagal nustatytą tolerancijos lygį.

36. Rizikos grupės:

36.1. žema rizika – RP nuo 2 iki 4,5 balo. Tai toleruojamas rizikos lygis, laikomas priimtu; rizika periodiškai peržiūrima ir stebima, tačiau papildomų priemonių imtis paprastai nebūtina;

36.2. vidutinė rizika – RP nuo 4,6 iki 7,9 balo . Tokia rizika laikoma nepriimtina ir turi būti stebima, vertinama bei valdoma nustatytomis kontrolės priemonėmis

36.3. didelė rizika – RP nuo 8 iki 10 balų. Tai nepriimtina rizika, kuriai reikalingas aktyvus valdymas ir Tarnybos vadovybės lygmens sprendimai. Šios Tvarkos 4 priede pateikiama rizikos vertinimo matrica ir rizikos grupių paaiškinimai .

37. Rizikos savininkai nepriimtinoms rizikoms valdyti parenka vieną iš šių rizikos valdymo būdų:

37.1. pašalinti – rizika pašalinama reorganizuojant tam tikrą veiklos procesą, atsisakant atskirų veiklų ar kitaip iki minimumo sumažinant esamus rizikos veiksnius;

37.2. sumažinti – taikomos tinkamos rizikos valdymo priemonės, siekiant sumažinti rizikos tikimybę ir (ar) poveikį;

37.3. perkelti – rizika ar jos dalis sutartiniais pagrindais perduodama trečiajai šaliai, siekiant sumažinti jos poveikį Tarnybai;

37.4. prisiimti (toleruoti) – rizika toleruojama, kai ji neviršija nustatyto tolerancijos lygio arba papildomos priemonės nebūtų proporcingos galimam poveikiui.

38. Nepriimtina rizika gali būti prisiimta tik Tarnybos direktoriaus motyvuotu sprendimu, įvertinus galimą poveikį Tarnybos veiklai ir planuojamųjų priemonių proporcingumą. Toks sprendimas priimamas nustatytam laikotarpiui, kuris negali būti ilgesnis kaip 1 metai, po kurio rizika turi būti peržiūrėta pakartotinai.

39. Jeigu nepriimtinai rizikai parenkamas valdymo būdas „sumažinti“ arba „perkelti“, RVP turi būti numatytos konkrečios rizikos valdymo priemonės.

40. Rizikos savininkai nepriimtinoms rizikoms valdyti pagal šios Tvarkos 2 priede pateiktą RVP formą parengia RVP, kuriame nurodo rizikos valdymo priemones, jų įgyvendinimo prioritetus, terminus, reikalingus išteklius, rizikos valdymo priemonių vykdytojus, dabartinę riziką (tikimybę, poveikį ir bendrą RP) bei numatomą likutinę riziką (tikimybę, poveikį, bendrą RP ir rizikos grupę).

41. Atlikus rizikos vertinimą kibernetinio saugumo vadovas parengia RVA, kurios sudėtinė dalis yra RVP. RVA pateikiamas TIS ar TIS grupių ir su jomis susijusių Tarnybos funkcijų ar paslaugų, kurių atžvilgiu atliktas rizikos vertinimas, sąrašas, vertinime dalyvavusių asmenų sąrašas, taikytų kibernetinio saugumo priemonių sąrašas, identifikuotos grėsmės ir pažeidžiamumai, detalūs rizikos vertinimo rezultatai, nepriimtinų rizikų santrauka ir RVP. RVA pateikiama ją tvirtinti Tarnybos direktoriui.

42. Tarnybos direktoriui patvirtinus RVA, ji registruojama Tarnybos dokumentų valdymo sistemoje.

43. Kibernetinio saugumo vadovas , Tarnybos direktoriui patvirtinus ir užregistravus RVA, ne vėliau kaip per 5 darbo dienas nuo jos patvirtinimo dienos turi į NKSC administruojamą KSIS pateikti RVA patvirtinimo duomenis ir teisės aktų nustatyta apimtimi rizikos vertinimo metu nustatytus apibendrintus rezultatus: identifikuotas rizikas, jų tikimybę ir poveikį veiklai, bendrus rizikos balus (RP), rizikos grupes ir valdymo priemones.

44. Tarnybos direktoriaus patvirtinta RVA vidaus teisės aktų nustatyta tvarka saugoma ne mažiau kaip 3 metus.

IV SKYRIUS
RIZIKOS VALDYMAS IR STEBĖSENA

45. Rizikos savininkai turi nuolat stebėti rizikas ir RVP įgyvendinimą, rizikos valdymo pokyčius ir vertinti, ar numatytos RVP vis dar yra veiksmingos; jeigu ne, rizikos savininkai turi suplanuoti naujas ir (ar) papildomas RVP, siekiant sumažinti rizikas iki Tarnybai priimtino lygio.

46. Rizikos savininkai ne rečiau kaip kartą per pusmetį peržiūri:

46.1. RVP įgyvendinimo būklę;

46.2. jų veiksmingumą;

46.3. likutinės rizikos pokyčius.

47. Nustačius, kad taikomos priemonės nėra pakankamai veiksmingos, rizikos savininkai planuoja papildomas priemones.

48. Apie reikšmingus rizikos pokyčius ir RVP vykdymo problemas rizikos savininkai nedelsdami informuoja kibernetinio saugumo vadovą ir saugos įgaliotinį.

49. Jeigu įmanoma, rizikos savininko ir rizikos valdymo priemonės vykdytojo funkcijos

turėtų būti atskiriamos.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

50. Tvarka turi būti peržiūrima ir atnaujinama ne rečiau kaip kartą per metus arba atsiradus esminiams pokyčiams, galintiems turi įtakos Tvarkos nuostatų taikymui.

51. Už Tvarkos peržiūrėjimą, atnaujinimą ir įgyvendinimo kontrolę atsakingas kibernetinio saugumo vadovas.

_____

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO RIZIKOS VERTINIMO IR VALDYMO TVARKOS PERŽIŪRA

Dokumento versija	Veiklos data	Statusas	Dokumento savininkas	Pagrindinės korekcijos	Patvirtinimo data ir Nr.
v1.0	2026-XX-XX	Patvirtinta	Kibernetinės saugos vadovas	-	2026-XX-XX Nr. XXX-XXX

Tinklų ir informacinių sistemų kibernetinio saugumo rizikos vertinimo ir valdymo tvarkos
1 priedas

RIZIKŲ REGISTRAS

(Rizikų registro forma)

Rizikos Nr.	TIS ar TIS grupė / susijusi funkcija ar paslauga	Grėsmė	Pažeidžiamumas	Dabartinė rizikos tikimybė	Dabartinis rizikos poveikis	Bendras RP	Rizikos grupė	Rizikos savininkas	Rizikos valdymo būdas	Rizikos valdymo priemonės pavadinimas ir aprašymas	Likutinės rizikos tikimybė	Likutinės rizikos poveikis	Likutinis RP	Likutinės rizikos grupė
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)

Pildymo instrukcija:

(1) Nurodomas rizikos numeris (pvz. R01).

(2) Nurodomas TIS ar TIS grupės pavadinimas ir su ja susijusi Tarnybos funkcija ar paslauga (pvz. Personalo valdymo informacinė sistema / personalo administravimas).

(3) Nurodoma su TIS susijusi grėsmė (pvz. potvynis, socialinė inžinerija, paslaugų teikimo sutrikdymas, gaisras ir pan.).

(4) Nurodomas su TIS susijęs pažeidžiamumas.

(5) Nurodomas dabartinės rizikos tikimybės vertinimo balas pagal šios Tvarkos 3 priedą.

(6) Nurodomas dabartinės rizikos poveikio vertinimo balas pagal šios Tvarkos 3 priedą.

(7) Nurodomas bendras dabartinės rizikos balas (RP), apskaičiuotas pagal formulę $RP = (1,5 \times P) + (0,5 \times T)$.

(8) Nurodoma dabartinės rizikos grupė pagal tolerancijos lygį: žema, vidutinė arba didelė.

(9) Nurodomos rizikos savininko pareigos, vardas ir pavardė.

(10) Nurodomas rizikos valdymo būdas (pašalinti, sumažinti, perkelti arba prisiimti (toleruoti)).

(11) Nurodomas rizikos valdymo priemonės, skirtos nepriimtinai rizikai valdyti, pavadinimas ir trumpas aprašymas.

(12) Nurodoma numatomos likutinės rizikos tikimybė, pilnai įgyvendinus plane numatytas priemones.

(13) Nurodomas numatomos likutinės rizikos poveikis, pilnai įgyvendinus plane numatytas priemones.

(14) Nurodomas numatomos likutinės rizikos bendras balas (RP), apskaičiuotas pagal formulę $RP = (1,5 \times P) + (0,5 \times T)$.

(15) Nurodoma numatomos likutinės rizikos grupė pagal tolerancijos lygį: žema, vidutinė arba didelė.

Tinklų ir informacinių sistemų kibernetinio saugumo rizikos vertinimo ir valdymo tvarkos
2 priedas

RIZIKŲ VALDYMO PLANAS

(Rizikų valdymo plano forma)

Rizikos Nr.	Rizika (trumpas aprašymas)	Rizikos valdymo būdas	Priemonės pavadinimas ir aprašymas	Prioritetas	Rizikos savininkas	Priemonės vykdytojas	Reikalingi ištekliai	Įgyvendinimo terminas	Dabartinė tikimybė	Dabartinis poveikis	Dabartinis RP	Likutinė tikimybė	Likutinis poveikis	Likutinis RP	Likutinės rizikos grupė

PASTABA. RVP yra RVA sudėtinė dalis. Plane nurodoma dabartinė nepriimtinos rizikos būklė ir numatoma likutinė rizika po priemonių įgyvendinimo.

Tinklų ir informacinių sistemų kibernetinio saugumo rizikos vertinimo ir valdymo tvarkos
3 priedas

TIKIMYBĖS IR POVEIKIO VERTINIMO KRITERIJAI

Finansinio poveikio kriterijai nustatomi absoliučiomis eurų reikšmėmis, atsižvelgiant į Tarnybos rizikų vertinimo sistemoje taikomus rėžius.

Tikimybės vertinimo lentelė

Tikimybė	Balas	Aprašas
Labai tikėtina (50–100 %)	5	Rizikos pasireiškimo tikimybė labai didelė. Vertinama remiantis ankstesne patirtimi, panašių įvykių dažnumu ir numatomomis aplinkybėmis.
Gana tikėtina (20–50 %)	4	Rizika gali pasireikšti gana dažnai arba yra realių prielaidų manyti, kad ji gali materializuotis artimiausiu laikotarpiu.
Tikėtina (10–20 %)	3	Rizika gali pasireikšti, tačiau jos materializavimasis priklauso nuo papildomų veiksnių ar aplinkybių.
Nelabai tikėtina (1–10 %)	2	Rizikos pasireiškimas mažai tikėtinas, tačiau jo visiškai atmesti negalima.
Mažai tikėtina (<1 %)	1	Rizikos pasireiškimas labai mažai tikėtinas, remiantis turima patirtimi ir esamomis aplinkybėmis.

Poveikio vertinimo lentelė

Poveikis	Balas	Finansiniai nuostoliai dėl neefektyvaus lėšų panaudojimo	Kiti poveikio vertinimo pavyzdžiai
Kritinis poveikis	5	>300 tūkst. Eur	Kritinių sistemų sutrikimas, reikšmingas išorinių reikalavimų pažeidimas, plataus masto neigiamas poveikis Tarnybos strateginiams tikslams ir reputacijai, vadovaujančios grandies darbuotojų kaita >5 per 1 metus.
Reikšmingas poveikis	4	>150 tūkst. Eur – 300 tūkst. Eur	Reikšmingas išorinių reikalavimų pažeidimas ar svarbios informacinės sistemos darbo sutrikimas, reikšmingas poveikis Tarnybos strategijai ir reputacijai, vadovaujančios grandies darbuotojų kaita 3–4 per 1 metus.
Vidutinis poveikis	3	>30 tūkst. Eur – 150 tūkst. Eur	Reikšmingas išorinių reikalavimų pažeidimas, kuris gali būti greitai ir nesudėtingai pašalintas, ribotas poveikis Tarnybos strategijai ir reputacijai, vadovaujančios grandies darbuotojų kaita 2–3 per 1 metus.
Nežymus poveikis	2	>3 tūkst. Eur – 30 tūkst. Eur	Nereikšmingas išorinių reikalavimų pažeidimas, kuris negali būti greitai ir nesudėtingai pašalintas, nežymus poveikis Tarnybos strategijai ir reputacijai, vadovaujančios grandies darbuotojų kaita 1–2 per 1 metus.
Nereikšmingas poveikis	1	<3 tūkst. Eur	Nereikšmingas išorinių reikalavimų pažeidimas, kuris gali būti greitai ir nesudėtingai pašalintas, minimalus poveikis Tarnybos strategijai ir reputacijai, vadovaujančios grandies darbuotojų kaita 1 per 1 metus.

Tinklų ir informacinių sistemų kibernetinio saugumo rizikos vertinimo ir valdymo tvarkos
4 priedas

RIZIKOS VERTINIMO MATRICA

Poveikis / Tikimybė	Mažai tikėtina (1)	Nelabai tikėtina (2)	Tikėtina (3)	Gana tikėtina (4)	Labai tikėtina (5)
Kritinis (5)	**8**	**8,5**	**9**	**9,5**	**10**
Reikšmingas (4)	**6,5**	**7**	**7,5**	**8**	**8,5**
Vidutinis (3)	**5**	**5,5**	**6**	**6,5**	**7**
Nežymus (2)	**3,5**	**4**	**4,5**	**5**	**5,5**
Nereikšmingas (1)	**2**	**2,5**	**3**	**3,5**	**4**

Paaiškinimai

Spalva	Rizikos grupė	Paaiškinimas
	Didelė rizika – 8–10 balų	Nepriimtina rizika – aktyviai valdoma; sprendimai priimami Tarnybos vadovybės lygmeniu.
	Vidutinė rizika – 4,6–7,9 balo	Nepriimtina rizika – stebima, vertinama ir valdoma nustatytomis kontrolės priemonėmis.
	Žema rizika – 2–4,5 balo	Priimtina rizika – toleruojama, periodiškai peržiūrima ir stebima; papildomų priemonių imtis paprastai nebūtina.

Rizikos grupių rėžiai ir priimtinumas: didelė rizika – 8–10 balų (nepriimtina); vidutinė rizika – 4,6–7,9 balo (nepriimtina); žema rizika – 2–4,5 balo (priimtina).