



**AKCINĖS BENDROVĖS „REGITRA“  
GENERALINIS DIREKTORIUS**

**ĮSAKYMAS  
DĖL ŽURNALINIŲ ĮRAŠŲ VALDYMO TVARKOS  
APRAŠO PATVIRTINIMO**

2025 m. d. Nr.  
Vilnius

Vadovaudamasis Akcinės bendrovės „Regitra“ įstatų, patvirtintų Lietuvos Respublikos vidaus reikalų ministro 2024 m. birželio 7 d. įsakymu Nr. 1V-385 „Dėl valstybės įmonės „Regitra“ pertvarkymo į akcinę bendrovę „Regitra“, 63.1 papunkčiu bei Informacijos saugumo politikos, patvirtintos akcinės bendrovės „Regitra“ valdybos 2025 m. rugsėjo 16 d. posėdžio protokolu Nr. 2V-5754, 2.7 papunkčiu:

1. T v i r t i n u Žurnalinių įrašų valdymo tvarkos aprašą (pridedama).
2. P a v e d u AB „Regitra“ Skaitmeninimo ir informacinių technologijų departamento skyrių vadovams su šiuo įsakymu supažindinti visus skyriaus pavaldžius darbuotojus.

Laikinais einantis generalinio direktoriaus pareigas

Rytis Polikauskas

## ŽURNALINIŲ ĮRAŠŲ VALDYMO TVARKOS APRAŠAS

### I SKYRIUS BENDROSIOS NUOSTATOS

1. Žurnalinių įrašų valdymo tvarkos aprašas (toliau – Tvarkos aprašas) reglamentuoja akcinės bendrovės „Regitra“ (toliau – AB „Regitra“) žurnalinių įrašų rinkimo, saugojimo, analizavimo ir ištrynimo bei šių procesų auditavimo tvarką.

2. Tvarkos apraše vartojamos sąvokos:

2.1. **Informaciniai ištekliai** – AB „Regitra“ valdomas IT turtas, numatytas AB „Regitra“ generalinio direktoriaus patvirtintoje AB „Regitra“ informacinių technologijų turto valdymo tvarkoje;

2.2. **Kibernetinio saugumo vadovas (angl. CISO)** – AB „Regitra“ darbuotojas, atsakingas už tinkamą žurnalinių įrašų valdymo procesą ir techninių priemonių įgyvendinimą;

2.3. **Saugumo operacijų centras (toliau – SOC)** – AB „Regitra“ generalinio direktoriaus ar jo įgalioto asmens paskirtas asmuo ar grupė, taip pat – paslaugas teikianti trečioji šalis, atsakinga už žurnalinių įrašų ir kibernetinių incidentų stebėjimą ir valdymą;

2.4. **Žurnaliniai įrašai (angl. log files)** – tai įrašai, kuriuose sistemingai fiksuojama informacija apie įvairius įvykius, veiksmus ar būsenas AB „Regitra“ informaciniuose ištekluose. Šie įrašai leidžia atsekti sistemų veiklą, analizuoti incidentus, identifikuoti grėsmes ir užtikrinti atitiktį reguliaciniams reikalavimams.

3. Tvarkos aprašo nuostatos privalomos visiems AB „Regitra“ darbuotojams ir išorinių informacinių technologijų (IT) paslaugų teikėjams, kurie pagal savo funkcijas yra susiję su Tvarkos apraše apibrėžtais vaidmenimis.

4. Jei tinklų ir (ar) informacinių sistemų priežiūros paslaugas, susijusias su kibernetinių incidentų valdymu, teikia išorės paslaugų teikėjai, jie su Tvarkos aprašo reikalavimais supažindinami per sutartinius įsipareigojimus, užtikrinant, kad jiems būtų prieinama aktuali Tvarkos aprašo redakcija, o prievolė jos laikytis įtvirtinama sutartyse ar kituose susitarimuose.

### II SKYRIUS FUNKCIJOS IR ATSAKOMYBĖS

5. Tvarkos apraše numatytos SOC funkcijos ir atsakomybės:

5.1. techninės ir programinės įrangos žurnalinių įrašų saugojimas, fiksavimas ir analizė;

5.2. įeinančio ir išėinančio tinklo duomenų srauto, antivirusinės programinės įrangos, įsibrovimų aptikimo ir prevencijos sistemos ar saugasienės žurnalinių įrašų saugojimas ir analizė;

5.3. informacinių sistemų konfigūracinių ir atsarginių kopijų failų prieigos ar pakeitimo veiksmų rinkimas.

6. SOC funkcijos negali būti pavedamos darbuotojui, atsakingam už tinkamą tinklų ir (ar) informacinių sistemų veiklą (t. y., IT administratoriui).

7. Tvarkos apraše numatytos kibernetinio saugumo vadovo funkcijos ir atsakomybės:
  - 7.1. Tvarkos aprašo koordinavimas ir įgyvendinimo kontrolė;
  - 7.2. žurnalinių įrašų valdymo atitikties teisės aktų reikalavimams užtikrinimas;
  - 7.3. Tvarkos aprašo periodinė peržiūra ir atnaujinimas;
  - 7.4. galimų rizikų, susijusių su žurnalinių įrašų valdymu identifikavimas.
  - 7.5. techninių priemonių, skirtų žurnalinių įrašų rinkimui ir analizei, tinkamumo vertinimo ir tobulinimo iniciavimas;
  - 7.6. SOC pateiktų žurnalinių įrašų analizės ataskaitų peržiūra ir vertinimas bei identifikavimas problemų ir iniciavimas taisomųjų veiksmų;
  - 7.7. žurnalinių įrašų valdymo auditų organizavimas.
8. Kibernetinio saugumo vadovas yra atsakingas už Tvarkos aprašo 1 priede nustatytos formos žurnalinių įrašų valdymo matricos parengimą ir nuolatinį atnaujinimą, vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatyme ir Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 3 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, nustatytais techninių žurnalinių įrašų valdymo reikalavimais..

### **III SKYRIUS**

#### **ŽURNALINIŲ ĮRAŠŲ NAUDOJIMAS IR VALDYMAS**

9. AB „Regitra“ žurnalinius įrašus renka ir naudoja informacinių išteklių veiksnio, jų naudotojų ir administratorių veiksmų (toliau – įvykių) auditui ir kontrolei bei incidentų tyrimui, siekiant:
  - 9.1. nustatyti (atsekti) neteisėtus ir (ar) neleistinus veiksmus, atliekamus informaciniuose ištekliuose (pvz., įvykus kibernetiniam incidentui, kai būtina ištirti jo atsiradimo priežastis);
  - 9.2. fiksuoti informaciniams ištekliams kylančias grėsmes;
  - 9.3. fiksuoti informacinių išteklių infrastruktūros gedimus;
  - 9.4. išsaugoti techninės ir programinės įrangos klaidų pranešimus;
  - 9.5. atitikti Lietuvos Respublikos teisės aktus, reglamentuojančius kibernetinį saugumą;
  - 9.6. analizuoti žurnalinių įrašų duomenis, siekiant optimizuoti IT veiklą, sumažinti kibernetinių incidentų ir informacijos saugumo rizikų įvykio tikimybę;
  - 9.7. tirti kibernetinius incidentus.
10. Žurnaliniai įrašai yra saugomi ne trumpiau kaip 90 kalendorinių dienų. Jei žurnaliniuose įrašuose yra asmens duomenų, jų saugojimo ir sunaikinimo terminai turi būti nustatomi atsižvelgiant į Bendrojo duomenų apsaugos reglamento (BDAR) reikalavimus.
11. Naudojant technines ir organizacines priemones turi būti užtikrinamas žurnalinių įrašų konfidencialumas, vientisumas ir prieinamumas. Būtina užtikrinti kontrolės mechanizmus, įgalinančius identifikuoti šių principų pažeidimus.
12. Žurnalinių įrašų apie informacinius išteklius valdymo procesas turi užtikrinti savalaikį žurnalinių įrašų fiksavimą, rinkimą, analizavimą ir saugojimą. Žurnalinių įrašų valdymo procesas vyksta pagal Tvarkos aprašo Žurnalinių įrašų valdymo matricą, kurios forma nustatyta Tvarkos aprašo 2 priede ir pildoma įdiegus SOC.
13. SOC žurnalinius įrašus turi analizuoti nepertraukiamai (8 val. 5 darbo dienas per savaitę arba 24 val. 7 dienas per savaitę – priklausomai nuo SOC modelio pasirinkimo).
14. SOC žurnalinių įrašų analizės metu nustatę informaciją apie galimą kibernetinio saugumo įvykį privalo nedelsiant, bet ne vėliau kaip per 1 val., informuoti kibernetinio saugumo vadovą.

15. Kibernetinio saugumo vadovas, gavęs informaciją apie galimą kibernetinio saugumo įvykį, atlieka jo vertinimą ir inicijuoja kibernetinio incidento valdymą pagal AB „Regitra“ generalinio direktoriaus patvirtintą AB „Regitra“ kibernetinių incidentų valdymo tvarką.

16. SOC kas mėnesį kibernetinio saugumo vadovui turi pateikti žurnalinių įrašų analizės apibendrintą ataskaitą. Kibernetinio saugumo vadovas, įvertinęs žurnalinių įrašų analizės apibendrintą ataskaitą ir nustatęs identifikuotas galimas grėsmes, inicijuoja informacijos saugumo rizikų vertinimą pagal AB „Regitra“ generalinio direktoriaus patvirtintos Informacijos saugumo rizikos valdymo tvarkos nuostatas.

17. Kibernetinio saugumo vadovas kartą per pusmetį atlieka techninių žurnalinių įrašų valdymo reikalavimų (pateikti 1 priede) patikrą, siekdamas nustatyti, ar šie techniniai reikalavimai yra įgyvendami.

#### **IV SKYRIUS**

#### **BAIGIAMOSIOS NUOSTATOS**

18. Visi AB „Regitra“ žurnalinių įrašų valdymo procese dalyvaujantys darbuotojai privalo laikytis Tvarkos aprašo nuostatų.

19. Kibernetinio saugumo vadovas turi užtikrinti ir kontroliuoti, kad SOC, atsakingi už žurnalinių įrašų valdymą, atliktų veiksmus Tvarkos apraš nustatyta tvarka ir terminais.

20. Už Tvarkos aprašo vykdymo kontrolę atsakingas AB „Regitra“ kibernetinio saugumo vadovas.

21. Tvarkos aprašas turi būti peržiūrinamas ir, esant poreikiui, atnaujinamas bent kartą per metus arba kai atsiranda esminiai informacinių išteklių ir (ar) kibernetinio saugumo valdymo procesų pasikeitimai, kurie turi įtakos Tvarkos aprašu reglamentuojamai tvarkai.

---

## TECHNINIAI ŽURNALINIŲ ĮRAŠŲ VALDymo REIKALAVIMAI

Nr.	Techniniai reikalavimai
1.	Turi būti fiksuojami bent jau šie žurnaliniai įrašai (jei tinklų ir informacinės sistemos dalys palaiko tokį funkcionalumą):
1.1.	tinklų ir informacinės sistemos komponentų (serverių, virtualių serverių, ugniasienių, maršrutizatorių, komutatorių ir kitų subjekto identifikuotų svarbių komponentų) įjungimas, išjungimas ar perkrovimas;
1.2.	naudotojų ir administratorių autentifikavimo įvykiai;
1.3.	naudotojų, administratorių paskyrų sukūrimas, prieigų prie tinklų ir informacinių sistemų pakeitimai;
1.4.	administratorių atliekami veiksmai;
1.5.	operacinėse sistemose sukurti ir atlikti sisteminiai uždavinių įvykiai (angl. <i>Scheduled task</i> );
1.6.	grupinių politikų pakeitimai;
1.7.	ugniasienių taisyklių pakeitimai;
1.8.	žurnalinių įrašų rinkimo funkcijos įjungimas, išjungimas;
1.9.	operacinių sistemų laiko ir datos pakeitimai;
1.10.	saugumo sistemų (antivirusinių, įsibrovimo aptikimo sistemų) įjungimas ir išjungimas;
1.11.	operacinėse sistemose vykstančių procesų ar servisų įvykiai;
1.12.	tinklų ir informacinių sistemų galinių įrenginių autentifikavimo įvykiai;
1.13.	žurnalinių įrašų peržiūrėjimas, trynimas, kūrimas ar keitimas.
2.	Tinklai ir informacinės sistemos turi turėti ne mažiau kaip 2 laiko šaltinius.
3.	Žurnaliniuose įrašuose turi būti fiksuojami bent jau šie duomenys (jei tinklų ir informacinės sistemos dalys palaiko tokį funkcionalumą):
3.1.	įvykio data ir tikslus laikas;
3.2.	įvykio rūšis (informacija, klaida, saugumo pranešimas, sisteminis pranešimas, perspėjimas (angl. <i>warning</i> ));
3.3.	naudotojo/ administratoriaus ir (arba) tinklų ir informacinės sistemos įrenginio,

Nr.	Techniniai reikalavimai
	susijusio su įvykiu, identifikavimo duomenys;
3.4.	įvykio aprašymas.
4.	Priemonės, naudojamos vidinės tinklų ir informacinės sistemos sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad žurnaliniuose įrašuose fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais.
5.	Žurnaliniai įrašai turi būti saugomi ne trumpiau kaip 90 kalendorinių dienų.
6.	Draudžiama žurnalinį įrašą trinti, keisti, kol nesibaigęs žurnalinio įrašo saugojimo terminas.
7.	Žurnalinio įrašo kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.
8.	Naudojimas žurnaliniuose įrašais turi būti kontroliuojamas ir fiksuojamas, žurnaliniai įrašai turi būti pasiekiami tik AB „Regitra“ įgaliotiems asmenims ir kibernetinio saugumo vadovui (peržiūros teisėmis).
9.	Žurnalinio įrašo duomenys turi būti analizuojami įgalioto asmens ne rečiau kaip kartą per mėnesį ir apie analizės rezultatų nuokrypius informuojamas kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.
10.	Turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų į tinklų ir informacinę sistemą įeinantį ir iš jos išeinantį duomenų srautą.
11.	Neįprasta veikla turi būti užfiksuojama žurnaliniuose įrašuose ir, jei įmanoma, automatizuotomis priemonėmis sukuriama automatinis pranešimas, kurį matytų kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis.
12.	AB „Regitra“ vidinės tinklų ir informacinės sistemos turi būti atskirtos nuo viešųjų ryšių tinklų naudojant ugniasienę.
13.	Ugniasienės saugumo taisyklės turi būti nuolat peržiūrimos ir prireikus atnaujinamos. Būtina atlikti detalią taisyklių analizę ne rečiau kaip kartą per 6 mėn.

Akcinės bendrovės „Regitra“  
Žurnalinių įrašų valdymo tvarkos  
aprašo  
2 priedas

(Žurnalinių įrašų valdymo matricos forma)

## ŽURNALINIŲ ĮRAŠŲ VALDymo MATRICA

[illegible]

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	AB "REGITRA", Liepkalnio g. 97A, 02121 Vilnius, Lietuva (2026-02-14 00:46:23)
Dokumento pavadinimas (antraštė)	DĖL ŽURNALINIŲ ĮRAŠŲ VALDYMO TVARKOS APRAŠO PATVIRTINIMO
Dokumento rūšys	-
Dokumento registracijos data ir numeris	2025-10-20 Nr. 1V-193
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	Rytis Polikauskas, Generalinis direktorius
Parašo sukūrimo data ir laikas	2025-10-20 09:05:53 (GMT+03:00)
Parašo formatas	XAdES-A
Laiko žymoje nurodytas laikas	2025-10-20 09:06:06 (GMT+03:00)
Informacija apie sertifikavimo paslaugos teikėją	EID-SK 2016,2.5.4.97=#160e4e545245452d3130373437303133,AS Sertifitseerimiskeskus,EE
Sertifikato galiojimo laikas	2024-08-15 15:37:05–2029-08-14 23:59:59
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Regitra DVS, Sistema
Parašo sukūrimo data ir laikas	2025-10-20 09:06:11 (GMT+03:00)
Parašo formatas	XAdES-EPES
Laiko žymoje nurodytas laikas	-
Informacija apie sertifikavimo paslaugos teikėją	RCSC IssuingCA-2,RCSC,VI Registru Centras - i.k. 124110246,LT
Sertifikato galiojimo laikas	2024-06-28 14:53:25–2027-06-28 14:53:25
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	-
Pagrindinio dokumento pridedamų dokumentų skaičius	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	DocLogix v12.8.7.0
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Tikrinant dokumentą nenustatyta jokių klaidų ( 2026-02-14 00:46:23)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2026-02-14 00:46:23 atspausdino Jonas Piliponis
Paieškos nuoroda	-
Papildomi metaduomenys	-