PATVIRTINTA

VšĮ Centrinės projektų valdymo agentūros direktoriaus \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ įsakymu Nr. \_\_\_\_\_\_\_\_\_

**2014-2021 M. EUROPOS EKONOMINĖS ERDVĖS IR NORVEGIJOS FINANSINIŲ MECHANIZMŲ ADMINISTRAVIMO IR PROCESŲ AUTOMATIZAVIMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI**

1. **BENDROSIOS NUOSTATOS**
2. 2014-2021 m. Europos Ekonominės erdvės ir Norvegijos finansinių mechanizmų administravimo ir procesų automatizavimo informacinės sistemos (toliau – NORIS) duomenų saugos nuostatai (toliau – saugos nuostatai) reglamentuoja NORIS saugos politiką: NORIS elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui, NORIS valdytojo ir tvarkytojo darbuotojų supažindinimo su saugos politiką įgyvendinančiais dokumentais principus.
3. Naudojamos sąvokos
	1. NORIS naudotojas - NORIS valdytojo ir tvarkytojo darbuotojas, turintis teisę dirbti su NORIS;
	2. Kitos saugos nuostatuose vartojamos sąvokos atitinka 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamente (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas), Lietuvos Respublikos Valstybės informacinių išteklių valdymo įstatyme ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716), Lietuvos standartuose LST ISO / IEC 27002 ir LST ISO / IEC 27001 „Informacinės technologijos. Saugumo metodai.“ grupės standartuose vartojamas sąvokas.
4. NORIS elektroninės informacijos saugumo užtikrinimo tikslai:
	1. saugiai kaupti ir tvarkyti elektroninę informaciją NORIS;
	2. užtikrinti NORIS kaupiamos elektroninės informacijos konfidencialumą, prieinamumą, vientisumą;
5. NORIS elektroninės informacijos saugumo prioritetinės kryptys:
	1. NORIS kaupiamos elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;
	2. NORIS veiklos tęstinumo užtikrinimas;
	3. NORIS elektroninės informacijos asmens duomenų apsauga;
	4. organizacinių, techninių, programinių, teisinių, informacijos sklaidos priemonių, skirtų elektroninės informacijos saugai užtikrinti, įgyvendinimas ir kontrolė.
6. Saugos nuostatų reikalavimų nuostatomis vadovaujasi NORIS valdytojas ir tvarkytojas – VšĮ Centrinė projektų valdymo agentūra, kurios adresas – S. Konarskio g. 13, 03109 Vilnius.
7. NORIS valdytojas rengia ir tvirtina šiuos saugos politiką įgyvendinančius dokumentus:
	1. Centrinės projektų valdymo agentūros informacinės sistemos (toliau – CPVA IS) saugaus elektroninės informacijos tvarkymo taisykles;
	2. CPVA IS naudotojų administravimo taisykles;
	3. CPVA IS veiklos tęstinumo valdymo planą.
8. NORIS valdytojo ir tvarkytojo funkcijos ir atsakomybė:
	1. rengia ir tvirtina NORIS saugos nuostatus ir saugos politiką įgyvendinančius dokumentus;
	2. užtikrina veiksmingą ir spartų NORIS pokyčių valdymo planavimą;
	3. skiria NORIS saugos įgaliotinį, NORIS administratorių;
	4. atsako už NORIS saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;
	5. atlieka Valstybės informacinių išteklių valdymo įstatyme nustatytas funkcijas ir turi šiame įstatyme nurodytas teises ir pareigas.
9. NORIS saugos įgaliotinio funkcijos ir atsakomybė:
	1. teikia NORIS valdytojo vadovui pasiūlymus dėl:
		1. NORIS administratoriaus paskyrimo ir reikalavimų administratoriui nustatymo;
		2. NORIS IT saugos atitikties ir rizikos vertinimo atlikimo organizavimo;
		3. NORIS saugos nuostatų ir saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;
	2. koordinuoja elektroninės informacijos saugos incidentų, įvykusių NORIS, tyrimą ir bendradarbiauja su kompetentingoms institucijoms, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais;
	3. teikia NORIS administratoriams ir naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su NORIS saugos politikos įgyvendinimu;
	4. teisės aktų nustatyta tvarka organizuoja IT saugos atitikties ir rizikos vertinimus;
	5. rengia ir teikia NORIS valdytojui informacinių IT saugos atitikties vertinimo ataskaitą;
	6. periodiškai inicijuoja NORIS administratorių ir naudotojų supažindinimą su NORIS saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais, informuoja apie jų pakeitimus (priminimai elektroniniu paštu, atmintinės priimtiems naujiems darbuotojams ir pan.) ir atsakomybę už šiuose dokumentuose nustatytų reikalavimų nesilaikymą;
	7. organizuoja naudotojų mokymus elektroninės informacijos saugos ir kibernetinio saugumo klausimais;
	8. peržiūri NORIS saugos nuostatus ir saugos politiką įgyvendinančius dokumentus ne rečiau kaip kartą per kalendorinius metus;
	9. atsako už tinkamą NORIS saugos nuostatuose nustatytų funkcijų vykdymą;
	10. atlieka NORIS saugos nuostatuose ir kituose saugos politikos įgyvendinimo dokumentuose nustatytas funkcijas.
10. NORIS administratorius atlieka šias funkcijas:
	1. atsako už NORIS veikimą, administruoja NORIS komponentus (NORIS aplikacijas, duomenų bazių valdymo sistemas ir kt. taikomąją programinę įrangą), rengia ir atnaujina susijusią sąrankos dokumentaciją;
	2. atlieka NORIS naudotojų administravimą (registravimą ir šalinimą) ir prieigos teisių suteikimą pagal darbuotojo įgaliojimus bei roles, vykdomas darbinėje veikloje;
	3. teikia pasiūlymus NORIS saugos įgaliotiniui su duomenų sauga susijusiais klausimais;
	4. dalyvauja atliekant IT saugos atitikties vertinimą;
	5. nedelsdamas vykdo NORIS saugos įgaliotinio nurodymus, susijusius su saugos politikos įgyvendinimu, ir jam atsiskaito už pavestą duomenų saugos organizavimą ir saugos priemonių įgyvendinimą;
	6. informuoja NORIS saugos įgaliotinį apie NORIS saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;
	7. atlieka NORIS saugos nuostatuose ir kituose saugos politikos įgyvendinimo dokumentuose nustatytas funkcijas.
11. NORIS administratorius, naudotojai ir saugos įgaliotinis, pastebėję asmens duomenų saugumo pažeidimą ir (arba) kitą incidentą, nedelsdami apie tai privalo pranešti CPVA Duomenų apsaugos pareigūnui.
12. NORIS saugų elektroninės informacijos tvarkymą užtikrina:
	1. Bendrasis duomenų apsaugos reglamentas;
	2. Valstybės informacinių išteklių valdymo įstatymas;
	3. Lietuvos Respublikos kibernetinio saugumo įstatymas;
	4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas);
	5. Saugos dokumentų turinio gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716;
	6. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716;
	7. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;
	8. Organizaciniai ir techniniai kibernetinio saugumo reikalavimai, taikomi kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;
	9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;
	10. Lietuvos standartai LST ISO/IEC 27002, LST ISO/IEC 27001 bei kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, apibūdinantys saugų informacinių sistemų duomenų tvarkymą;
	11. CPVA IS elektroninės informacijos tvarkymo taisyklės, CPVA IS naudotojų administravimo taisyklės, CPVA IS veiklos tęstinumo valdymo planas, NORIS nuostatai ir saugos nuostatai.
13. **NORIS ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS**
14. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, 9.1. ir 9.3 papunkčių kriterijais, NORIS priskiriama trečios kategorijos informacinėms sistemoms, kurioje tvarkoma vidutinės svarbos informacija.
15. NORIS rizika vertinama vadovaujantis Lietuvos Respublikos vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais ir atliekama ne rečiau kaip kartą per metus.
16. Rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama NORIS valdytojui ir kuri rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos NORIS elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus.
17. NORIS rizikos veiksniai nurodyti Bendrųjų elektroninės informacijos saugos reikalavimų apraše.
18. Rizikos veiksniai vertinami pagal elektroninės informacijos kategorijas, nustatant jų įtaką NORIS elektroninės informacijos saugai laipsnius:
	1. Ž – žemas. Duomenų pažeidimo poveikio laipsnis nėra didelis, padariniai nebus pavojingi – informacija išsiųsta kitam adresatui, įvesti netikslūs duomenys, dingo dalis informacijos, kurią galima greitai atkurti iš turimų atsarginių kopijų, prarasta informacija po paskutinio kopijavimo. Neveikia kompiuterinė programinė įranga ir (ar) operacinė sistema kompiuterizuotose darbo vietose;
	2. V – vidutinis. Duomenų pažeidimo poveikio laipsnis gali būti didelis, padariniai rimti – duomenys netikslūs ar sugadinti, bet juos įmanoma atkurti iš turimų atsarginių kopijų. Duomenų bazių įrašai pakeisti, sunku rasti klaidas ir suklastotą informaciją, neveikia kompiuterinė programinė įranga ir (ar) operacinė sistema tarnybinėse stotyse;
	3. A – aukštas. Duomenų pažeidimo poveikio laipsnis labai didelis, padariniai rimti – duomenys visiškai sugadinti, dėl vagystės, gaisro ar užliejimo prarasti ne tik NORIS duomenų bazėse buvę duomenys, bet ir atsarginės kopijos.
19. Rizikos vertinimo metu atliekamų darbų apimtis:
	1. NORIS sudarančių informacinių išteklių inventorizacija;
	2. NORIS įtakos veiklai vertinimas;
	3. grėsmių ir pažeidimų analizė;
	4. liekamosios rizikos vertinimas.
20. Atsižvelgdamas į rizikos įvertinimo ataskaitą, NORIS valdytojas prireikus tvirtina Rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.
21. NORIS rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas NORIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.
22. Pagrindiniai NORIS elektroninės informacijos saugos priemonių parinkimo principai:
	1. saugos priemonių diegimo kaina turi atitikti saugomos informacijos vertę;
	2. likutinė rizika turi būti sumažinta iki priimtino lygio;
	3. kur galima, turi būti įdiegtos prevencinės elektroninės informacijos saugos priemonės.
23. Siekiant užtikrinti NORIS nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per metus organizuojamas IT saugos atitikties vertinimas, kurio metu:
	1. įvertinama saugos politikos įgyvendinimo dokumentų ir realios informacijos saugos atitiktis;
	2. inventorizuojama NORIS techninė ir programinė įranga;
	3. patikrinama ir įvertinama NORIS administratoriui ir naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;
	4. įvertinamas pasirengimas užtikrinti NORIS veiklos tęstinumą įvykus saugos incidentui.
24. Atlikus IT saugos atitikties įvertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato NORIS valdytojas.
25. IT saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas NORIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.
26. **NORIS ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI**
27. NORIS atitinka saugos nuostatų 11 punkte nurodytuose teisės aktuose numatytus saugos reikalavimus.
28. NORIS programinės įrangos, skirtos apsaugoti informacinę sistemą nuo kenksmingos programinės įrangos, ir kitos programinės įrangos įdiegtos kompiuteriuose ir tarnybinėse stotyse naudojimo nuostatos, tinklo filtravimo įrangos, leistinos kompiuterių naudojimo ribos ir metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą, pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai, konkrečiai nustatomi ir reguliuojami CPVA IS saugaus elektroninės informacijos tvarkymo taisyklėse.
29. Kiekvienas NORIS administratorius ir naudotojas atsako už elektroninės informacijos, kuri jam prieinama naudojant NORIS, tvarkymo teisėtumą ir tvarkomų duomenų saugą.
30. **NORIS REIKALAVIMAI PERSONALUI**
31. NORIS administratorius ir naudotojai privalo turėti pagrindinius darbo su kompiuteriu įgūdžius, turi būti susipažinę su šiais saugos nuostatais, Bendruoju duomenų apsaugos reglamentu ir kitais saugos politiką įgyvendinančiais dokumentais.
32. Tvarkyti NORIS duomenis gali tik NORIS administratorius ir naudotojai, pasirašę pasižadėjimą saugoti asmens duomenų paslaptį ir susipažinę su NORIS nuostatais, NORIS saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais. Ši pareiga galioja ir perėjus dirbti į kitas pareigas arba pasibaigus darbo, sutartiniams ar kitiems santykiams.
33. NORIS administratorius ir naudotojai privalo rūpintis tvarkomos informacijos saugumu.
34. Saugos įgaliotinis privalo išmanyti informacinių sistemų administravimo ir elektroninės informacijos saugos principus, elektroninės informacijos užtikrinimo metodus ir kitus Lietuvos Respublikos ir Europos Sąjungos teisės aktus ir standartus reglamentuojančius saugų duomenų tvarkymą, sugebėti įgyvendinti ir prižiūrėti NORIS saugą.
35. NORIS saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos skyrimo praėję mažiau kaip vieni metai.
36. NORIS administratorius turi išmanyti elektroninės informacijos saugos principus, darbą su operacinėmis sistemomis, duomenų bazių administravimo pagrindus, turi būti susipažinęs su NORIS saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais. Administratorius privalo sugebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, nustatyti ir šalinti sutrikimus.
37. **NORIS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI**
38. NORIS administratoriaus ir naudotojų supažindinimo su saugos dokumentais tvarka principai:
	1. už NORIS administratoriaus ir naudotojų supažindinimą su NORIS saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais ir atsakomybe už šių reikalavimų nesilaikymą yra atsakingas NORIS saugos įgaliotinis;
	2. NORIS administratorius ir naudotojai su saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais bei atsakomybe už šių reikalavimų nesilaikymą pirmą kartą supažindinami pasirašytinai;
	3. pakartotinai su NORIS saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais NORIS administratorius ir naudotojai supažindinami tik iš esmės pasikeitus NORIS arba informacijos saugą reglamentuojantiems teisės aktams;
	4. saugos įgaliotinis periodiškai inicijuoja NORIS administratoriaus ir naudotojų supažindinimą su NORIS saugos politiką įgyvendinančiais dokumentais, informuoja apie jų pakeitimus (priminimai elektroniniu paštu, atmintinės priimtiems naujiems darbuotojams ir pan.) ir atsakomybę už šiuose dokumentuose nustatytų reikalavimų nesilaikymą;
	5. saugos įgaliotinis gali inicijuoti NORIS administratoriaus ir naudotojų mokymą elektroninės informacijos saugos klausimais.
39. NORIS saugos įgaliotinis, administratorius, naudotojai, pažeidę saugos nuostatų ar kitų saugos politiką reguliuojančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.