PATVIRTINTA

Lietuvos Respublikos finansų ministro

2021 m. lapkričio d. įsakymu Nr.

**EUROPOS SĄJUNGOS INVESTICIJŲ ADMINISTRAVIMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI**

1. **SKYRIUS
BENDROSIOS NUOSTATOS**
2. Europos Sąjungos investicijų administravimo informacinės sistemos duomenų saugos nuostatuose (toliau – saugos nuostatai) reglamentuojama Europos Sąjungos investicijų administravimo informacinės sistemos (toliau – INVESTIS) saugos politika: INVESTIS elektroninės informacijos (duomenų, dokumentų ir informacijos tvarkomos INVESTIS ir nurodytos INVESTIS nuostatuose) saugos valdymas, organizaciniai ir techniniai reikalavimai, reikalavimai personalui, INVESTIS administratorių, INVESTIS ir DMS naudotojų supažindinimo su saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais principai.
3. Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos:
	1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme (toliau – Išteklių valdymo įstatymas);
	2. Lietuvos Respublikos kibernetinio saugumo įstatyme;
	3. Bendrųjų elektroninės informacijos saugos reikalavimų apraše (toliau Saugos reikalavimų aprašas), 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“;
	4. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakyme Nr. V-941 ,,Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;
	5. Lietuvos standartuose LST ISO / IEC 27002 ir LST ISO / IEC 27001 bei kituose Lietuvos ir tarptautiniuose „Informacinės technologijos. Saugumo metodai“ grupės standartuose.
4. INVESTIS saugos politika įgyvendinama pagal INVESTIS valdytojo tvirtinamus INVESTIS saugos politiką įgyvendinančius dokumentus (toliau – saugos politiką įgyvendinantys dokumentai):
	1. INVESTIS saugaus elektroninės informacijos tvarkymo taisykles;
	2. INVESTIS naudotojų administravimo taisykles;
	3. INVESTIS veiklos tęstinumo valdymo planą.
5. INVESTIS elektroninės informacijos saugumo užtikrinimo prioritetinės kryptys:
	1. INVESTIS elektroninės informacijos saugos – konfidencialumo, vientisumo ir prieinamumo užtikrinimas;
	2. INVESTIS veiklos tęstinumo užtikrinimas;
	3. INVESTIS elektroninės informacijos ir tvarkomų asmens duomenų apsauga;
	4. organizacinių, techninių, programinių, teisinių, informacijos sklaidos priemonių, skirtų elektroninės informacijos saugai užtikrinti, įgyvendinimas ir kontrolė.
6. INVESTIS elektroninės informacijos saugumo užtikrinimo tikslai:
	1. sudaryti sąlygas saugiai tvarkyti elektroninę informaciją INVESTIS;
	2. užtikrinti, kad INVESTIS tvarkoma elektroninė informacija būtų apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, praradimo, taip pat nuo bet kokio kito neteisėto tvarkymo;
	3. vykdyti INVESTIS elektroninės informacijos saugos ir kibernetinių incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į INVESTIS elektroninės informacijos saugos ir kibernetinius incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai valdyti.
7. Saugos nuostatų reikalavimai taikomi:
	1. INVESTIS valdytojui - Lietuvos Respublikos finansų ministerijai (Lukiškių g. 2, 01512 Vilnius);
	2. INVESTIS tvarkytojams:
		1. Lietuvos Respublikos finansų ministerijai (Lukiškių g. 2, 01512 Vilnius);
		2. Lietuvos Respublikos vidaus reikalų ministerijai (Šventaragio g. 2, 01510 Vilnius);
		3. Lietuvos Respublikos socialinės apsaugos ir darbo ministerijai (A. Vivulskio g. 11, 03610 Vilnius);
		4. Lietuvos Respublikos ekonomikos ir inovacijų ministerijai (Gedimino pr. 38, 01104 Vilnius);
		5. Lietuvos Respublikos švietimo, mokslo ir sporto ministerijai (A. Volano g. 2, 01124 Vilnius);
		6. Lietuvos Respublikos susisiekimo ministerijai (Gedimino pr. 17, 01505 Vilnius);
		7. Lietuvos Respublikos aplinkos ministerijai (A. Jakšto g. 4, 01105 Vilnius);
		8. Lietuvos Respublikos sveikatos apsaugos ministerijai (Vilniaus g. 33, 01506 Vilnius);
		9. Lietuvos Respublikos kultūros ministerijai (J. Basanavičiaus g. 5, 01118 Vilnius);
		10. Lietuvos Respublikos energetikos ministerijai (Gedimino pr. 38, 01104 Vilnius);
		11. Lietuvos Respublikos krašto apsaugos ministerijai (Totorių g. 25, 01121 Vilnius);
		12. Lietuvos Respublikos žemės ūkio ministerijai (Gedimino pr. 19, 01103 Vilnius);
		13. viešajai įstaigai Centrinei projektų valdymo agentūrai (toliau - CPVA) (S. Konarskio g. 13, 03109 Vilnius);
		14. viešajai įstaigai Lietuvos verslo paramos agentūrai (Savanorių pr. 28, 03116 Vilnius);
		15. Alytaus regiono plėtros tarybai (Rotušės a. 4, 62141 Alytus);
		16. Kauno regiono plėtros tarybai (L. Sapiegos g. 10, 44251 Kaunas);
		17. Klaipėdos regiono plėtros tarybai (Liepų g. 11, 92138 Klaipėda);
		18. Marijampolės regiono plėtros tarybai (Vytauto g. 28, 68295 Marijampolė);
		19. Panevėžio regiono plėtros tarybai (Respublikos g. 38, 35173 Panevėžys);
		20. Šiaulių regiono plėtros tarybai (Vilniaus g. 263, 76337 Šiauliai);
		21. Tauragės regiono plėtros tarybai (Vasario 16-osios g. 6, 72258 Tauragė);
		22. Telšių regiono plėtros tarybai (Respublikos g. 32, 87333 Telšiai);
		23. Utenos regiono plėtros tarybai (Utenio a. 8, 28248 Utena);
		24. Vilniaus regiono plėtros tarybai (Konstitucijos pr. 3, 09308 Vilnius);
	3. INVESTIS administratoriams - CPVA darbuotojas, dirbantiems pagal darbo sutartį, prižiūrintiems INVESTIS infrastruktūrą, užtikrinantiems jos veikimą, elektroninės informacijos saugą, INVESTIS žinynų ir naudotojų administravimą (sąvoka naudojama visiems saugos nuostatų 10 punkte nurodytiems administratorių tipams įvardinti);
	4. INVESTIS naudotojams - INVESTIS valdytojo ir (ar) INVESTIS tvarkytojų valstybės tarnautojas ir (arba) darbuotojas, dirbantis pagal darbo sutartį, INVESTIS veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją tvarkantis INVESTIS elektroninę informaciją;
	5. DMS naudotojams - juridinių ir fizinių asmenų, potencialių paraiškų teikėjų, ir fizinių ir juridinių asmenų, kurie vykdo projektų įgyvendinimo sutartyse numatytas projektų įgyvendinimo veiklas, valstybės tarnautojas ir (arba) darbuotojas, dirbantis pagal darbo sutartį, INVESTIS veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją tvarkantis INVESTIS elektroninę informaciją;
	6. INVESTIS saugos įgaliotiniui.
8. INVESTIS valdytojo funkcijos:
	1. tvirtina INVESTIS saugos nuostatus ir saugos politiką įgyvendinančius dokumentus;
	2. atlieka INVESTIS nuostatuose ir Išteklių valdymo įstatyme nustatytas funkcijas.
9. CPVA, kaip INVESTIS tvarkytojo, funkcijos:
	1. rengia saugos nuostatų ir saugos politiką įgyvendinančių dokumentų ir jų pakeitimo projektus;
	2. užtikrina veiksmingą ir spartų INVESTIS pokyčių valdymo planavimą;
	3. skiria INVESTIS saugos įgaliotinį, INVESTIS administratorius;
	4. atsako už INVESTIS saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą;
	5. atlieka INVESTIS nuostatuose ir Išteklių valdymo įstatyme nustatytas funkcijas.
10. INVESTIS saugos įgaliotinio funkcijos ir atsakomybė:
	1. teikia CPVA vadovui pasiūlymus, kaip nustatyta Saugos reikalavimų apraše;
	2. rengia ir teikia INVESTIS valdytojui IT saugos atitikties vertinimo ataskaitą;
	3. periodiškai inicijuoja INVESTIS administratorių ir INVESTIS naudotojų supažindinimą su 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;
	4. organizuoja INVESTIS naudotojų mokymus elektroninės informacijos saugos klausimais;
	5. peržiūri saugos nuostatus ir saugos politiką įgyvendinančius dokumentus ne rečiau kaip kartą per kalendorinius metus;
	6. atsako už tinkamą saugos nuostatuose nustatytų funkcijų vykdymą;
	7. atlieka Saugos reikalavimų apraše, saugos nuostatuose ir INVESTIS saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.
11. INVESTIS administratoriai skirstomi į šiuos tipus:
	1. INVESTIS funkcinis administratorius, kurio funkcijos kurti INVESTIS naudotojus ir jiems suteikti teises INVESTIS;
	2. INVESTIS žinynų administratorius, kurio funkcijos prižiūrėti ir administruoti INVESTIS žinynus;
	3. INVESTIS infrastruktūros administratorius, kuris atlieka šias funkcijas:
		1. užtikrina kompiuterinių tinklų veikimą, saugumą, konfigūruoja ir prižiūri kompiuterinių tinklų įrangą;
		2. užtikrina tarnybinių stočių veikimą, saugumą, diegia ir konfigūruoja operacines sistemas ir jų atnaujinimus;
		3. kuria ir administruoja tarnybinių stočių naudotojus ir prieigas prie jų;
		4. atlieka virtualių tarnybinių stočių atsarginį kopijavimą, atstatymą ir priežiūrą;
		5. dalyvauja atliekant IT saugos atitikties vertinimą;
		6. vykdo INVESTIS saugos įgaliotinio nurodymus, susijusius su saugos politikos įgyvendinimu, ir jam atsiskaito už pavestą duomenų saugos organizavimą ir saugos priemonių įgyvendinimą;
		7. informuoja INVESTIS saugos įgaliotinį apie saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytų reikalavimų nesilaikymą, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;
		8. atlieka saugos nuostatuose ir kituose saugos politikos įgyvendinimo dokumentuose nustatytas funkcijas.
	4. INVESTIS sisteminis administratorius, kuris atlieka šias funkcijas:
		1. užtikrina INVESTIS veikimą, diegia ir administruoja INVESTIS aplikacijas, duomenų bazių valdymo sistemas ir kt. taikomąją programinę įrangą, rengia ir atnaujina susijusią sąrankos dokumentaciją;
		2. atlieka ir prižiūri duomenų bazių valdymo sistemų atsarginį kopijavimą ir atstatymą;
		3. atlieka INVESTIS aplikacijų, duomenų bazių valdymo sistemų kt. taikomosios programinės įrangos, sukurtų integracijų su kitomis informacinėmis sistemomis priežiūrą;
		4. atlieka versijų diegimo kontrolę, INVESTIS ir (ar) DMS naudotojų informavimą apie planuojamus diegimus ar sutrikimus;
		5. teikia pasiūlymus INVESTIS saugos įgaliotiniui su duomenų sauga susijusiais klausimais;
		6. dalyvauja atliekant IT saugos atitikties vertinimą;
		7. vykdo INVESTIS saugos įgaliotinio nurodymus, susijusius su saugos politikos įgyvendinimu, ir jam atsiskaito už pavestą duomenų saugos organizavimą ir saugos priemonių įgyvendinimą;
		8. informuoja INVESTIS saugos įgaliotinį apie saugos nuostatuose ir saugos politiką įgyvendinančiuose dokumentuose nustatytų reikalavimų nesilaikymą, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;
		9. atlieka saugos nuostatuose ir kituose saugos politikos įgyvendinimo dokumentuose nustatytas funkcijas.
12. INVESTIS administratoriai, INVESTIS naudotojai ir INVESTIS saugos įgaliotinis, pastebėję asmens duomenų saugumo pažeidimą ir (arba) kitą incidentą, nedelsdami apie tai privalo pranešti CPVA Duomenų apsaugos pareigūnui.
13. INVESTIS saugų elektroninės informacijos tvarkymą užtikrina laikymasis reikalavimų, kuriuos reglamentuoja:
	1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);
	2. Išteklių valdymo įstatymas;
	3. Kibernetinio saugumo įstatymas;
	4. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas 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“;
	5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;
	6. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;
	7. Lietuvos standartai LST ISO/IEC 27002 ir LST ISO/IEC 27001 bei kiti Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, apibūdinantys saugų informacinių sistemų duomenų tvarkymą;
	8. INVESTIS nuostatai, saugos nuostatai, INVESTIS naudotojų administravimo taisyklės, INVESTIS saugaus elektroninės informacijos tvarkymo taisyklės, INVESTIS veiklos tęstinumo valdymo planas.
14. **SKYRIUS
INVESTIS ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS**
15. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto 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 – IS klasifikavimo gairių aprašas) 9.1 ir 9.3 papunkčių kriterijais ir IS klasifikavimo gairių aprašo 12.3 papunkčiu, INVESTIS priskiriama trečios kategorijos informacinėms sistemoms, kurioje tvarkoma vidutinės svarbos informacija.
16. INVESTIS rizika vertinama atsižvelgiant į Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais ir atliekama ne rečiau kaip kartą per metus.
17. Rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama INVESTIS valdytojui ir kuri rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos INVESTIS elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus.
18. INVESTIS rizikos veiksniai nurodyti Saugos reikalavimų apraše.
19. Rizikos veiksniai vertinami pagal elektroninės informacijos kategorijas, nustatant jų įtaką INVESTIS 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 INVESTIS duomenų bazėse buvę duomenys, bet ir atsarginės kopijos.
20. Rizikos vertinimo metu atliekamų darbų apimtis:
	1. INVESTIS sudarančių informacinių išteklių inventorizacija;
	2. INVESTIS įtakos veiklai vertinimas;
	3. grėsmių ir pažeidimų analizė;
	4. liekamosios rizikos vertinimas.
21. Atsižvelgdamas į rizikos įvertinimo ataskaitą, INVESTIS valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.
22. INVESTIS rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas INVESTIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.
23. Pagrindiniai INVESTIS 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.
24. Siekiant užtikrinti saugos 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 nuostatų ir saugos politiką įgyvendinančių dokumentų reikalavimų ir faktinės saugos atitiktis;
	2. inventorizuojama INVESTIS techninė ir programinė įranga;
	3. patikrinama ir įvertinama INVESTIS administratoriams ir INVESTIS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis;
	4. įvertinamas pasirengimas užtikrinti INVESTIS veiklos tęstinumą įvykus saugos incidentui.
25. Atlikus IT saugos atitikties įvertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato INVESTIS valdytojas.
26. IT saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas INVESTIS valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai.
27. **SKYRIUS
INVESTIS ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI**
28. INVESTIS atitinka saugos nuostatų 12 punkte nurodytuose teisės aktuose nustatytus saugos reikalavimus.
29. INVESTIS 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 INVESTIS saugaus elektroninės informacijos tvarkymo taisyklėse.
30. Kiekvienas INVESTIS administratorius ir INVESTIS ir (ar) DMS naudotojas atsako už elektroninės informacijos, kuri jam prieinama naudojant INVESTIS, tvarkymo teisėtumą ir tvarkomų duomenų saugą.
31. **SKYRIUS
INVESTIS REIKALAVIMAI PERSONALUI**
32. INVESTIS naudotojų, INVESTIS administratorių, INVESTIS saugos įgaliotinio kvalifikacija turi atitikti bendruosius ir specialiuosius reikalavimus, nustatytus jų pareiginiuose nuostatuose.
33. INVESTIS administratoriai ir INVESTIS naudotojai privalo turėti pagrindinius darbo su kompiuteriu įgūdžius, prieš pradėdami tvarkyti INVESTIS elektroninę informaciją, turi būti susipažinę su INVESTIS nuostatais, saugos nuostatais, Reglamentu (ES)2016/679 ir saugos politiką įgyvendinančiais dokumentais.
34. DMS naudotojai privalo turėti pagrindinius darbo su kompiuteriu įgūdžius, prieš pradėdami tvarkyti INVESTIS elektroninę informaciją turi būti susipažinę su INVESTIS nuostatais ir saugos nuostatais.
35. INVESTIS administratoriai, INVESTIS ir DMS naudotojai privalo rūpintis tvarkomos elektroninės informacijos saugumu.
36. INVESTIS 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 INVESTIS saugą.
37. INVESTIS 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.
38. INVESTIS sisteminis administratorius turi išmanyti elektroninės informacijos saugos principus, darbą su operacinėmis sistemomis, duomenų bazių valdymo sistemų ir aplikacijų administravimo pagrindus.
39. INVESTIS infrastruktūros administratorius privalo sugebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą, stebėti techninės ir programinės, tinklo įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, nustatyti ir šalinti sutrikimus.
40. INVESTIS saugos įgaliotinis pagal INVESTIS naudotojų išreikštą poreikį arba įvykus saugos incidentui gali inicijuoti INVESTIS naudotojų mokymus elektroninės informacijos saugos klausimais.
41. INVESTIS naudotojų mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:
	1. INVESTIS saugos įgaliotinis turi organizuoti mokymus elektroninės informacijos saugos (kibernetinio saugumo) klausimais, įvairiais būdais priminti apie elektroninės informacijos saugos (kibernetinio saugumo) problemas (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems INVESTIS naudotojams ir kt.);
	2. INVESTIS saugos įgaliotinis mokymus elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi planuoti ir mokymo būdus parinkti atsižvelgiant į elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), INVESTIS naudotojų ar INVESTIS administratorių poreikius;
	3. INVESTIS saugos įgaliotinis mokymus gali vykdyti fiziškai susirenkant (kontaktiniu būdu) (pvz., paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.);
	4. INVESTIS saugos įgaliotinis mokymus INVESTIS naudotojams turi organizuoti periodiškai, bet ne rečiau kaip kartą per metus;
42. Mokymai DMS naudotojams ir INVESTIS administratoriams gali būti organizuojami pagal poreikį, už šių mokymų organizavimą atsakingas saugos įgaliotinis.
43. **SKYRIUS
INVESTIS IR DMS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI**
44. INVESTIS ir DMS naudotojų supažindinimo su saugos dokumentais tvarka principai:
	1. INVESTIS ir DMS naudotojų supažindinimą su saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais ir atsakomybe už šiuose dokumentuose nustatytų reikalavimų nesilaikymą organizuoja INVESTIS saugos įgaliotinis;
	2. INVESTIS ir DMS naudotojai su saugos nuostatais ir taikomais kitais saugos politiką įgyvendinančiais dokumentais bei atsakomybe už šiuose dokumentuose nurodytų reikalavimų nesilaikymą supažindinami pirmą kartą prisijungus prie INVESTIS ir (arba) DMS, išsaugant susipažinimo datą susipažinimo įrodomumo užtikrinimui;
	3. pakartotinai supažindinami, kai iš esmės pakeičiami saugos nuostatai ar kiti saugos politiką įgyvendinantys dokumentai;
	4. INVESTIS saugos įgaliotinis gali savo iniciatyva papildomai inicijuoti INVESTIS naudotojų supažindinimą su saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais, informuodamas apie jų pakeitimus naudodamas tokias priemones, kaip priminimai elektroniniu paštu, atmintinės priimtiems naujiems darbuotojams ir pan.
45. **SKYRIUS
BAIGIAMOSIOS NUOSTATOS**
46. Už saugos nuostatų pažeidimus INVESTIS valdytojas, INVESTIS tvarkytojai, INVESTIS saugos įgaliotinis, INVESTIS administratoriai, INVESTIS ar DMS naudotojai atsako Lietuvos Respublikos teisės aktų reglamentuojančių duomenų saugą nustatyta tvarka.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_