



**VIEŠOJI ĮSTAIGA „INDĖLIŲ IR INVESTICIJŲ DRAUDIMAS“
DIREKTORIUS**

ĮSAKYMAS

**DĖL VIEŠOSIOS ĮSTAIGOS „INDĖLIŲ IR INVESTICIJŲ DRAUDIMAS“ TINKLŲ IR
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ,
VIEŠOSIOS ĮSTAIGOS „INDĖLIŲ IR INVESTICIJŲ DRAUDIMAS“ TINKLŲ IR
INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ IR VIEŠOSIOS
ĮSTAIGOS „INDĖLIŲ IR INVESTICIJŲ DRAUDIMAS“ KIBERNETINIŲ INCIDENTŲ
VALDYMO PLANO PATVIRTINIMO**

2026 m. kovo d. Nr. V-
Vilnius

Vadovaudamasi Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 (2024 m. lapkričio 6 d. nutarimo Nr. 945 redakcija) „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ ir siekdama įgyvendinti viešojoje įstaigoje „Indėlių ir investicijų draudimas“ (toliau – IID) kibernetinio saugumo priemonės, kibernetinių incidentų valdymo procedūras bei tinklų ir informacinių sistemų naudotojų administravimo reikalavimus, ir atsižvelgdama į LR Finansų ministerijos vidaus audito rekomendacijas (2025 m. lapkričio 4 d. Informacijos saugumo valdymo sistemų, tinklų ir informacinių sistemų saugumo vertinimo vidaus audito ataskaita Nr. 16.2E-A-6):

1. T v i r t i n u naujos redakcijos viešosios įstaigos „Indėlių ir investicijų draudimas“ Tinklų ir informacinių sistemų naudotojų administravimo taisykles (toliau – Taisyklės) (pridedama);
2. P r i p a ž i s t u netekusiu galios IID direktoriaus 2023 m. gruodžio 22 d. patvirtintas įsakymu Nr. V-110 Taisyklių redakciją;
3. Į p a r e i g o j u IID Fondų administravimo skyriaus (toliau – FAS) vadovą/direktoriaus pavaduotoją:
 - 3.1. Iki 2026-04-01 užtikrinti IID darbuotojų konfidencialumo pasižadėjimo pasirašymą;
 - 3.2. Iki 2026-04-10 užtikrinti Taisyklėse nurodytų paslaugų teikėjų supažindinimą su Aprašu ir konfidencialumo pasižadėjimo pasirašymą;
 - 3.3. Iki 2026-04-11 informuoti IID direktorių dėl šio įsakymo 3.1-3.2 punktų įgyvendinimą;
4. T v i r t i n u naujos redakcijos viešosios įstaigos „Indėlių ir investicijų draudimas“ kibernetinių incidentų valdymo planą (pridedama);
5. P r i p a ž i s t u netekusiu galios IID direktoriaus 2025 m. gruodžio 31 d. patvirtintą viešosios įstaigos „Indėlių ir investicijų draudimas“ kibernetinių incidentų valdymo planą Nr. V-115;
6. T v i r t i n u naujos redakcijos viešosios įstaigos „Indėlių ir investicijų draudimas“ Informacinių sistemų saugos nuostatus (pridedama);
7. P r i p a ž i s t u netekusiu galios IID direktoriaus 2023 m. gruodžio 22 d. patvirtintus įsakymu Nr. V-110 viešosios įstaigos „Indėlių ir investicijų draudimas“ Informacinių sistemų saugos nuostatų redakciją;
8. Iki 2026-06-31 atlikti FAS žinioje esančių IID vidaus dokumentų ir procesų peržiūrą, atsižvelgiant į naujos redakcijos Taisykles, ir, pagal poreikį, inicijuoti jų pakeitimus.
9. N u r o d a u IID administratoriui su šiuo įsakymu supažindinti visus IID darbuotojus.

Direktorė

Aurelija Mažintienė

PATVIRTINTA

Viešosios įstaigos „Indėlių ir investicijų draudimas“
direktorius 2026 m. kovo d. įsakymu Nr.

**VIEŠOSIOS ĮSTAIGOS „INDĖLIŲ IR INVESTICIJŲ DRAUDIMAS“ TINKLŲ IR
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS**

Dokumento data ir Nr.	2026-03- Nr.
Dokumento versija	2.0
Dokumento statusas	Patvirtinta
Dokumento įsigaliojimo data	2026-03-
Artimiausios dokumento peržiūros data	2027-03-31
Dokumento savininkas	VšĮ „Indėlių ir investicijų draudimas“ (toliau – IID) Fondų administravimo skyrius (toliau – FAS)
Dokumento autorius	FAS
Dokumentą tvirtina	IID direktorius
Dokumento klasifikacija	Vidinio naudojimo

Dokumento peržiūros ir kontrolės istorija

Versija	Data	Atlikto pakeitimo esmė	Pakeitimo autorius
2.0	2026-03-31	Atnaujinta siekiant įgyvendinti Finansų Ministerijos vidaus audito rekomendacijas (2025 m. lapkričio 4 d. Informacijos saugumo valdymo sistemų, tinklų ir informacinių sistemų saugumo vertinimo vidaus audito ataskaita Nr. 16.2E-A-6)	Fondų administravimo skyriaus vyr. specialistas/IS saugos įgaliotinis Tomas Jurkovlianeč; Fondų administravimo skyriaus vadovė/direktorius pavaduotoja Alena Blažienė IID direktorė Aurelija Mažintienė

**I SKYRIUS
BENDROSIOS NUOSTATOS**

- Šios taisyklės (toliau – Taisyklės) nustato Viešosios įstaigos „Indėlių ir investicijų draudimas“ (toliau – IID) tinklų ir informacinių sistemų (toliau – IS) naudotojų, IS administratorių, IID išorės paslaugų teikėjų ir fondų dalyvių darbuotojų prieigos prie IID valdomų IS suteikimo, naudojimo, saugos, stebėsenos ir kontrolės principus bei kibernetinio saugumo reikalavimus. Taisyklės reglamentuoja techninius ir organizacinius reikalavimus, susijusius su IS naudotojų tapatybės nustatymu, autentifikavimu, privilegijų valdymu, nuotoline prieiga, tinklų sauga ir IS saugumu.
- Taisyklėse naudojamos sąvokos:
 - kritinė sistema** – IID naudojama IS ar kitas IT išteklius, būtinas pagrindinėms IID veiklos funkcijoms vykdyti, kurio saugumo pažeidimas ar veikimo sutrikimas turėtų reikšmingą neigiamą poveikį IID veiklos tęstinumui, finansinei būklei ar teisinių įsipareigojimų vykdymui.

3. Kitos Taisyklėse naudojamos sąvokos suprantamos taip, kaip jos apibrėžtos Taisyklių 4 punkte nurodytuose teisės aktuose ir kituose IS saugą reglamentuojančiuose teisės aktuose.
4. Taisyklės parengtos vadovaujantis [Lietuvos Respublikos kibernetinio saugumo įstatymu, Kibernetinio saugumo reikalavimų aprašu](#), patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 (2024 m. lapkričio 6 d. nutarimo Nr. 945 redakcija) „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ ir kitais teisės aktais.
5. Taisyklės nereglamentuoja Prieigų matricos sudarymo, tvirtinimo ir keitimo procedūrų. Prieigų matricos administracinė prieigos suteikimo / keitimo / panaikinimo tvarka vykdoma vadovaujantis IID „Dokumentų tvarkymo ir apskaitos taisyklėmis“, patvirtintomis 2025-12-23 įsakymu Nr. V-105.
6. Taisyklėse nustatyti reikalavimai yra privalomi visiems IID darbuotojams ir asmenims, kurie naudoja IID valdomas IS bei tinklus.
7. Taisyklės laikomos vienu iš IID informacijos saugą įgyvendinančių dokumentų ir taikytinos su kitais IID vidaus teisės aktais, reglamentuojančiais dokumentų valdymą, informacijos saugą ir asmens duomenų apsaugą (toliau – Saugos dokumentai).

II SKYRIUS

IID IS NAUDOTOJŲ GRUPĖS IR JŲ TEISĖS

IS naudotojai neskirstomi į atskiras grupes, tačiau jiems gali būti priskiriami šie vaidmenys, kurie lemia prieigos teises

8. IS naudotojai – visi asmenys, kuriems suteikta teisė naudotis IID valdomomis informacinėmis sistemomis, nepriklausomai nuo jų atliekamų funkcijų, teisinio statuso ar santykių su IID,
9. IID IS naudotojų teises ir prieigų apimtis nustato Prieigų matrica, sudaroma ir tvarkoma vadovaujantis IID Dokumentų tvarkymo ir apskaitos taisyklėmis, reglamentuojančios prisijungimų procedūras prie IID ir išorės IS (toliau – Prieigų matrica (-os)).
10. IS naudotojams suteikiamos prieigos turi atitikti šiuos principus: mažiausios privilegijos, būtina žinoti, pareigų atskyrimo, unikalios tapatybės, teisėtų funkcijų vykdymo.
11. IS naudotojams priskiriami šie vaidmenys:
 - 11.1. Paprastas IS naudotojas – IID darbuotojai ar kitas subjektas, atliekantys kasdienes funkcijas ir naudojančys IID IS pagal jiems priskirtas pareigas bei suteiktas prieigos teises pagal Prieigų matricą;
 - 11.2. IS administratorius – IID direktoriaus paskirtas darbuotojas arba paslaugų teikėjų atstovai, turintys specialiąsias administravimo teises ir vykdančys IS techninės priežiūros, administravimo, stebėsenos ir saugumo užtikrinimo funkcijas;
 - 11.3. Indėlių ir įsipareigojimų investuotojams draudimo sistemos (IIIDS) dalyvių darbuotojai – finansų įstaigų atstovas, kuriam suteikiamos ribotos prieigos prie IID IS tik ir išskirtinai duomenų suvedimo tikslais;
 - 11.4. Paslaugų teikėjo atstovas – IID išoriniai tiekėjai ir jų darbuotojai, kuriems būtina ribota prieiga prie IID IS siekiant vykdyti sutartines funkcijas, vadovaujantis minimalios privilegijos principu.
12. IS naudotojams suteikiama teisė:
 - 12.1. naudotis jiems suteiktais IS funkcijomis pagal patvirtintas prieigos teises ir darbo funkcijas;
 - 12.2. vykdyti duomenų paiešką ir peržiūrą, jei tai įtraukta į jų pareigines funkcijas;
 - 12.3. pranešti apie incidentus IID Kibernetinių incidentų valdymo plane nustatyta tvarka
 - 12.4. įvesti, keisti, atnaujinti, naikinti duomenis, jei tai būtina jų pareigoms atlikti, vadovaujantis mažiausios privilegijos ir būtina žinoti principais;
 - 12.5. gauti techninę pagalbą iš IS administratorių;
 - 12.6. IS naudotojams draudžiama savarankiškai plėsti savo prieigos teises, naudoti kitų naudotojų paskyras, keisti saugumo nustatymus, ignoruoti saugos reikalavimus.
13. IS administratoriams suteikiama teisė:
 - 13.1. administruoti IID IS ir techninę infrastruktūrą (tarnybines stotis (serverius), tinklus, paskyras) ;

- 13.2. nustatyti ir keisti IS naudotojų prieigų teises;
- 13.3. taikyti kibernetinio saugumo priemones ir reaguoti į incidentus;
- 13.4. tvarkyti atsarginių kopijų kūrimą ir atstatymą.
14. IS administratoriams draudžiama suteikti administratoriaus teises sau, naudoti administratoriaus paskyrą kaip įprastą naudotojo paskyrą, keisti Prieigų matricą be nustatytos tvarkos.
15. IS naudotojams prieigos teisės dirbti su IS gali būti suteiktos tik pasirašius IID konfidencialumo pasižadėjimą, išskyrus IIDS dalyvių darbuotojus (1 priedas);
16. Paslaugų teikėjų atstovams, kuriems suteikiama prieiga prie IID IS, suteikiamos šios teisės:
 - 16.1. vykdyti darbus, numatytus paslaugų teikimo sutartyse, pagal jiems suteiktas ribotas technines prieigos teises;
 - 16.2. leidžiama naudoti tik tas IS funkcijas, kiek būtina sutartinėms paslaugoms vykdyti, vadovaujantis minimalios privilegijos principu;
 - 16.3. Prieiga suteikiama tik IID direktoriaus ar įgalioto asmens sprendimu, arba tais atvejais, kai tai numatyta sutartiniuose santykiuose su Paslaugų teikėjais.
17. Paslaugų teikėjams draudžiama naudoti IID IS už paslaugų sutarties ribų ir keisti saugumo nustatymus.
18. IIDS dalyvių darbuotojams, kuriems suteikiama prieiga prie IID IS, suteikiamos šios teisės:
 - 18.1. Leidžiama naudotis tik tomis funkcijomis, kurios numatytos LR finansų ministro patvirtintuose teisės aktuose;
 - 18.2. Visi veiksmai turi atitikti minimalios privilegijos principą ir Prieigų matricą
19. IIDS dalyvių darbuotojams draudžiama atlikti veiksmus, nesusijusius su įmokų apskaičiavimo procesu ir naudoti IID IS kitiems tikslams nei teisės aktuose nurodyta.
20. Visi IS naudotojai privalo:
 - 20.1. užtikrinti tvarkomų duomenų konfidencialumą, vientisumą ir pasiekiamumą;
 - 20.2. laikytis Saugos dokumentuose nustatytų reikalavimų;
 - 20.3. naudoti tik savo paskyrą ir saugoti tapatybės nustatymo priemones;
 - 20.4. nedelsdami pranešti apie incidentus IID Kibernetinių incidentų valdymo plane nustatyta tvarka;
 - 20.5. laikytis kibernetinio saugumo įstatymo ir kitų teisės aktų.

III SKYRIUS PRIEIGŲ VALDYMO PRINCIPAI

21. Bendrieji prieigų valdymo principai;
 - 21.1. būtina žinoti (angl. *need to know*). Prieiga prie IID IS suteikiama tik tiek, kiek darbuotojui, administratoriams, IIDS dalyvių ar paslaugų teikėjų atstovams būtina jų tiesioginėms funkcijoms atlikti. Prieigos teisės negali būti platesnės nei būtina darbo funkcijoms vykdyti;
 - 21.2. būtina naudoti (angl. *need to use*). IS naudotojui suteikiamos tik tos techninės ir funkcinės priemonės, kurios būtinos jo veiklai atlikti. Prieiga prie nenaudojamų ar perteklinių funkcijų draudžiama ir turi būti panaikinta;
 - 21.3. mažiausios privilegijos principas. IID IS naudotojai ir administratoriai turi gauti tik minimalias, jų veiklai vykdyti būtinas prieigos teises. Prieigų plėtimas be būtinybės draudžiamas;
 - 21.4. pareigų atskyrimo principas. IS naudotojui negali būti suteiktos tokios teisės, kurios sudaro sąlygas savarankiškai atlikti visas proceso dalis nuo pradžios iki pabaigos, kai to galima išvengti. IS administratoriaus paskyra negali būti naudojama IS naudotojo funkcijoms atlikti ir atvirkščiai;
 - 21.5. Unikaliios tapatybės principas. Kiekvienas IS naudotojas, administratorius, IIDS dalyvio darbuotojas ar paslaugų teikėjo atstovas privalo būti identifikuojami unikaliu prisijungimo vardu. Naudoti kito asmens paskyrą griežtai draudžiama.
22. Prieigos teisės suteikiamos pagal naudotojų grupes, patvirtintas šių Taisyklių II skyriuje.
23. Prieigos suteikimo tikslas - užtikrinti saugų, kontroliuojamą ir proporcingą IS naudotojų funkcijoms pritaikytą darbą su IID IS.
24. Prieigos teisės suteikiamos remiantis:

- 24.1. naudotojo pareiginėmis funkcijomis;
- 24.2. skyriui priskirtomis atsakomybėmis;
- 24.3. paslaugų teikimo sutartimi (paslaugų teikėjams);
- 24.4. teisės aktų nustatytais reikalavimais (IIIDS dalyviams).
25. Naujų naudotojų registravimas ir jų prieigos teisių nustatymas vykdomi vadovaujantis nuostatomis, išdėstytomis šiose Taisyklėse, o administracinė prieigų suteikimo procedūra atliekama vadovaujantis IID Dokumentų tvarkymo ir apskaitos taisyklių V skyriaus nuostatomis.
26. Prieigos teisės turi būti keičiamos:
 - 26.1. pasikeitus IS naudotojo pareigoms ar funkcijoms;
 - 26.2. pasikeitus IID veiklos procesams ar atsakomybėms;
 - 26.3. pakeitus paslaugų teikimo apimtį;
 - 26.4. pasikeitus rizikos lygiui ar saugumo reikalavimams.
27. Keičiant prieigą, privaloma užtikrinti:
 - 27.1. kad ankstesnės prieigos, kurios nebereikalingos, būtų panaikintos nedelsiant;
 - 27.2. kad naujos prieigos atitiktų mažiausios privilegijos principą;
 - 27.3. kad būtų atnaujinta informacija Prieigų matricoje.
28. Prieigų keitimo administracinė tvarka vykdoma vadovaujantis Dokumentų tvarkymo ir apskaitos taisyklių V skyriaus nuostatomis.
29. Prieigos teisės turi būti panaikinamos:
 - 29.1. nutraukus darbo ar sutartinius santykius;
 - 29.2. pasibaigus funkcijoms, kurioms reikalinga prieiga;
 - 29.3. pakeitus IS naudotojo pareigas, kurioms prieiga nebereikalinga;
 - 29.4. nustačius saugumo pažeidimus ar rizikas;
 - 29.5. nesinaudojant IS nustatytą laikotarpį (naudotojams >3 mėn., administratoriams >2 mėn.) pagal šių Taisyklių reikalavimus. Prieš stabdant IS naudotojo teises dirbti su IS įvertinamas realios nesinaudojimo sistema priežastys. Tuo atveju, jei nebuvo poreikio naudotis IS (pvz. nevyko draudiminiai įvykiai, nebuvo užklausių iš trečiųjų šalių) arba IS dėl savo specifikos naudojama tik periodiškai (pvz. kartą metuose uždeklaruoti duomenis), IS naudotojo teisė dirbti su konkrečia IID informacine sistema gali būti nestabdoma;
 - 29.6. Prieigos turi būti panaikintos nedelsiant, bet ne vėliau kaip paskutinę darbo ar sutartinių santykių dieną.
30. Prieigos panaikinimas fiksuojamas Prieigų matricoje.
31. Laikinos prieigos suteikiamos išimtiniais atvejais, siekiant užtikrinti veiklos tęstinumą (pavadojant darbuotoją, atliekant incidento valdymo ar techninius darbus). Laikinos prieigos galiojimo laikotarpis turi būti aiškiai nustatytas ir negali būti tęsiamas automatiškai. Laikinių prieigų suteikimas ir panaikinimas fiksuojamas Prieigų matricoje.
32. Prieiga prie kritinių sistemų ir funkcijų, kuriose tvarkomi asmens duomenys ar kita jautri informacija, suteikiama tik:
 - 32.1. Įdiegus dvigubą autentifikavimą (arba alternatyvias kibernetinės saugos priemones, jei dvigubo autentifikavimo sprendimas konkrečiai IS dėl IS specifikos netaikomas);
 - 32.2. įvertinus IS naudotojo funkcijas ir rizikos lygį;
 - 32.3. tik esant būtinybei pareiginių funkcijų vykdymui.
33. IS administratoriams prieiga prie kritinių IS suteikiama per atskiras administravimo paskyras.
34. IS administratoriai ne rečiau kaip kartą per metus atlieka visų IID IS naudotojų paskyrų atitikties patikrą ir pateikia rezultatus IS saugos įgaliotiniui.
35. IS saugos įgaliotinis ne rečiau kaip kartą per metus tikrina IS administratorių paskyrų atitiktį.
 36. Nenaudojamos paskyros, vadovaujantis IID Dokumentų tvarkymo ir apskaitos taisyklių V skyriaus nuostatomis, blokuojamos.

IV SKYRIUS

IS NAUDOTOJŲ REGISTRAVIMO IR IŠREGISTRAVIMO PRINCIPAI

37. Šio skyriaus tikslas - nustatyti saugumo reikalavimus naudotojų registravimui, išregistravimui ir prieigos teisių peržiūrai, siekiant užtikrinti, kad prieiga prie IID IS būtų suteikiama tik tiems asmenims ir tik tiek, kiek būtina jų funkcijoms vykdyti, laikantis mažiausios privilegijos, būtina žinoti ir pareigų atskyrimo principų.
38. Administracinė prieigų suteikimo, keitimo ir panaikinimo procedūra, įskaitant Prieigų matricos sudarymą, tvirtinimą ir atnaujinimą, vykdoma vadovaujantis ID Dokumentų tvarkymo ir apskaitos taisyklių V skyriaus nuostatomis.
39. Prieiga prie IS suteikiama tik tuo atveju, kai:
 - 39.1. yra aiškiai apibrėžtos IS naudotojo funkcijos;
 - 39.2. funkcijoms atlikti būtina prieiga prie konkrečios IID IS ar jos funkcijų;
40. Prieiga negali būti suteikiama:
 - 40.1. jei nėra poreikio;
 - 40.2. jei numatytas vaidmuo kelia nepagrįstą saugumo riziką;
 - 40.3. jei IS naudotojui nenustatytos prieigos Prieigų matricoje;
41. IS naudotojų grupių registravimas:
 - 41.1. IID darbuotojai registruojami kaip IS naudotojai pagal jų pareigines funkcijas ir joms reikalingą prieigos apimtį nustatytą Prieigų matricoje.
 - 41.2. IS administratoriai registruojami tik IID direktoriui patvirtinus administratoriaus teisių suteikimą per Prieigų matricą. IS administratorius pats sau administratoriaus teisių suteikti negali.
 - 41.3. IIIDS dalyvių darbuotojai registruojami vadovaujantis Lietuvos Respublikos finansų ministro 2023 m. gruodžio 12 d. įsakymu Nr. 1K-400 patvirtintu indėlių ir įsipareigojimų investuotojams draudimo įmokų apskaičiavimo ir mokėjimo tvarkos aprašo 7 punktu.
 - 41.4. Paslaugų teikėjų darbuotojai registruojami tik tiek, kiek būtina jų sutartinėms funkcijoms atlikti ir tik ribotam laikotarpiui.
42. Paskyrų naudojimo ir saugos reikalavimai:
 - 42.1. Visi IS naudotojai turi būti identifikuojami unikaliu prisijungimo vardu, kuris negali būti dalijamas, perduodamas ar naudojamas bendrai.
 - 42.2. IS administratoriaus paskyros turi būti atskiros nuo naudotojo paskyrų ir naudojamos tik administravimo funkcijoms atlikti.
 - 42.3. Draudžiama naudoti gamintojo numatytuosius slaptažodžius ir dalytis prisijungimo duomenimis.
 - 42.4. Visi IS naudotojai privalo naudoti dvigubą autentifikavimą, kai jungiasi prie kritinių IS ar sistemų, kuriose tvarkomi asmens duomenys (arba naudoti alternatyvias kibernetinės saugos priemones, jei dvigubo autentifikavimo sprendimas konkrečiai IS dėl IS specifikos netaikomas).
43. Ne rečiau kaip kartą per metus:
 - 43.1. IS administratoriai peržiūri visų naudotojų paskyrų atitiktį;
 - 43.2. IS saugos įgaliotinis peržiūri administratorių paskyras;
 - 43.3. Neatitinkančios paskyros nedelsiant blokuojamos ir inicijuojamas jų panaikinimas pagal nustatytą tvarką.

V SKYRIUS

TAPATYBĖS NUSTATYMO IR SAUGIŲ RYŠIŲ NAUDOJIMO REIKALAVIMAI

44. IS naudotojai ir administratoriai, jungdamiesi prie IID IS ar tinklų, privalo užtikrinti savo tapatybės saugą ir patikimą patvirtinimą, vadovaujantis šiame skyriuje nustatytais kibernetinio saugumo reikalavimais;
45. Tapatybės nustatymas turi būti atliekamas naudojant tik IID patvirtintas technines ir organizacines priemones;

46. IS administratoriams ir IS naudotojams, dirbantiems su kritinėmis IS ar duomenimis, taikomi sustiprinti autentifikavimo ir ryšio apsaugos reikalavimai.
47. Kelių veiksmų autentifikavimo (tapatumo nustatymo) priemonių naudojimas yra privalomas, kai prie IID IS jungiasi:
 - 47.1. IS administratoriai; prisijungimui prie IID IS kuriuose tvarkomi asmens duomenys turi būti taikomas kelių veiksmų autentifikavimas.
 - 47.2. IS naudotojai, kuriems suteikta prieiga prie sistemų, kuriose tvarkomi asmens duomenys,
 - 47.3. IS naudotojai, jungiantys iš išorinių tinklų ar ne IID priklausančių įrenginių,
 - 47.4. paslaugų teikėjų atstovai.
48. Autentifikavimas gali būti atliekamas naudojant:
 - 48.1. slaptažodį;
 - 48.2. slaptažodį kartu su mobilios autentifikavimo programėlės kodu;
 - 48.3. USB saugos raktą;
 - 48.4. el. pašto/ SMS žinutės vienkartinį kodą;
 - 48.5. biometrinius duomenis;
 - 48.6. kitas patvirtintas priemones.
49. Nuolatinio autentifikavimo sprendimų naudojimas:
 - 49.1. IID gali naudoti nuolatinio autentifikavimo sprendimus, užtikrinančius, kad IS naudotojo tapatybė būtų nuolat arba periodiškai tikrinama visos IS sesijos metu;
 - 49.2. tapatumo patikrinimas gali būti atliekamas remiantis:
 - 49.2.1. įrenginio būklės ir patikimumo vertinimu;
 - 49.2.2. naudotojo elgsenos analize (pvz., prisijungimo vieta, įrenginys, veiklos modeliai);
 - 49.2.3. įvykiais grįstu pakartotiniu autentifikavimu.
 - 49.3. IS privalo automatiškai blokuoti sesijas, jei nustatoma netipinė ar rizikinga veikla, arba jei naudotojo tapatybės neįmanoma patvirtinti.
50. Saugių balso, vaizdo ir teksto ryšių naudojimas:
 - 50.1. visi IID tarnybiniai ryšiai (balso, vaizdo, tekstiniai) turi būti vykdomi naudojant tik IID patvirtintas komunikacijos priemones, kurios užtikrina:
 - 50.1.1. ryšių šifravimą;
 - 50.1.2. naudotojų identifikavimą;
 - 50.1.3. prieigos kontrolę;
 - 50.1.4. duomenų konfidencialumą ir prieinamumą.
51. Draudžiama naudoti nepatvirtintas platformas ar ryšio priemones tvarkant su darbu ar IS susijusią informaciją.
52. IS naudotojai privalo užtikrinti, kad konfidencialūs duomenys nebūtų perduodami per viešus, nešifruotus ar neautorizuotus kanalus.
53. Saugių avarinių ryšių sistemų IID naudojimas:
 - 53.1. saugios avarinio ryšio priemonės, skirtos užtikrinti nepertraukiamą, patikimą ir saugų ryšį IID, kai įprasti ryšio kanalai ar IS tampa nepasiekiami, nepatikimi arba kompromituoti (kibernetinių incidentų metu, pagrindinių IS ar ryšių kanalų sutrikimo atvejais, ekstremalių situacijų metu);
 - 53.2. IID privalo turėti saugias avarinio ryšio priemones, užtikrinančias nepertraukiamą, patikimą ir saugų IID darbuotojų komunikavimą kibernetinių incidentų, pagrindinių IS sutrikimų ar ekstremalių situacijų metu.
54. Draudžiama naudoti asmeninius ar neautorizuotus įrenginius prisijungiant prie IID IS ar tvarkant su darbu susijusią informaciją.
55. Įrenginiai turi būti apsaugoti slaptažodžiais ir/arba PIN kodais, ir/arba biometrinėmis priemonėmis ir/arba ekrano užrakto ir/arba kitomis saugos priemonėmis.
56. Naudotojui pasitraukiant nuo darbo vietos, privaloma užrakinti įrenginį ir atsijungti nuo IS. Ekrano užsklendimas turi įsijungti automatiškai ne vėliau kaip po 15 minučių neveikimo.
57. IS naudotojui draudžiama atskleisti savo autentifikavimo priemones (įskaitant slaptažodžius, antrinius kodus, dvigubo autentifikavimo įrenginius).

58. Kilus įtarimui, kad paskyros duomenys galėjo būti atskleisti, IS naudotojas privalo nedelsdamas pakeisti slaptažodį ir informuoti IS administratorių.
59. Neleistini ar įtartini prisijungimo bandymai turi būti blokuojami IS administratoriaus iniciatyva.

VI SKYRIUS

IS NAUDOTOJŲ IR IS ADMINISTRATORIŲ SLAPTAŽODŽIŲ SUDARYMO, GALIOJIMO IR KEITIMO REIKALAVIMAI

60. Visi IS naudotojai ir IS administratorius privalo naudoti tik asmeninius, unikalius slaptažodžius ir užtikrinti jų konfidencialumą.
61. Slaptažodžių sudarymo, keitimo ir apsaugos reikalavimai yra privalomi visoms prieigoms prie IID IS.
62. Slaptažodžiai negali būti perduodami ar atskleidžiami tretiesiems asmenims ir negali būti saugomi atviru tekstu.
63. IS naudotojų slaptažodžių sudarymo reikalavimai:
 - 63.1. IS naudotojo slaptažodį turi sudaryti ne mažiau kaip 10 (dešimt) simbolių, IS administratoriaus – 15 (penkiolika) simbolių;
 - 63.2. slaptažodis turi būti sudarytas iš didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų simbolių;
 - 63.3. slaptažodžiui sudaryti draudžiama naudoti asmeninį turinį (vardai, gimimo datos, telefonai, vietovės), pasikartojančius simbolius, nuoseklias simbolių sekas („1234“, „abcde“ ir pan.), klaviatūros sekas;
 - 63.4. IID IS techninėje ir programinėje įrangoje draudžiama naudoti gamintojo nustatytus slaptažodžius, jie turi būti nedelsiant pakeisti vadovaujantis šiame skyriuje nustatytais reikalavimais.
64. Slaptažodžių galiojimo trukmė ir keitimas:
 - 64.1. IS naudotojų ir IS administratoriaus slaptažodžiai turi būti keičiami ne rečiau kaip kas 6 (šešis) mėnesius;
 - 64.2. IS naudotojas turi turėti galimybę bet kuriuo metu pasikeisti slaptažodį;
 - 64.3. negalima sudaryti slaptažodžių, kurie buvo naudoti per paskutinius 6 (šešis) kartus (IS naudotojams) ir 8 kartus (IS administratoriui).
65. Didžiausias nustatytas maksimalus leistinas IS naudotojų mėginimų prisijungti prie IS skaičius – ne daugiau negu 5 (penki) kartai iš eilės. Po numatyto bandymų skaičiaus prisijungti prie IS, IS naudotojo paskyra turi užsiblokuoti. Užblokuotą IS naudotojo paskyrą atblokuoti gali tik IS administratorius arba kiti IID direktoriaus įgalioti asmenys.
66. IID IS prisijungimo prie IS procedūros metu neturi teikti pagalbos pranešimų, kurie padėtų leidimo neturinčiam naudotojui (pvz., nepavykus prisijungti, IS neturi nurodyti, kuri prisijungimo duomenų dalis yra teisinga ar neteisinga).
67. Laikinas slaptažodis, suteiktas registracijos metu, turi būti pakeistas pirmojo prisijungimo metu.
68. Slaptažodis turi būti nedelsiant pakeistas, jei kyla įtarimas, kad jis galėjo būti atskleistas.
69. Slaptažodžių saugojimas:
 - 69.1. slaptažodžių automatinis išsaugojimas naršyklėse ar IS yra draudžiamas, išskyrus atvejus, kai naudojama specializuota slaptažodžių tvarkyklė.
 - 69.2. draudžiama perduoti slaptažodžius nešifruotais kanalais. Vienintelė išimtis – laikinas slaptažodis, kuris gali būti perduodamas atviru tekstu, tačiau tik:
 - 69.2.1. atskirai nuo prisijungimo vardo;
 - 69.2.2. alternatyviu kanalu (pvz., el. paštu + SMS);
 - 69.2.3. jei nėra techninių galimybių perduoti šifruotu kanalu.
70. IS naudotojas privalo naudoti tik jam suteiktą prisijungimo vardą. Svetimo prisijungimo vardo naudojimas yra griežtai draudžiamas.
71. Draudžiama laikyti slaptažodžius neapsaugotus, popieriuje, užrašuose ar matomose vietose.
72. Išvykstant iš darbo vietos ar paliekant įrenginį be priežiūros, IS naudotojas privalo užrakinti ekraną ir atsijungti nuo IS.

- 73. Slaptažodžiai gali būti atstatomi tik:
 - 73.1. identifikavus naudotoją;
 - 73.2. gavus tinkamai pagrįstą prašymą;
 - 73.3. naudojant saugias komunikacijos priemones.
- 74. Atstatytas slaptažodis laikomas laikinu ir turi būti pakeistas pirmo prisijungimo metu.

VII SKYRIUS NUOTOLINIO PRISIJUNGIMO REIKALAVIMAI

- 75. Nuotolinis prisijungimas prie IID IS gali būti vykdomas tik tada, kai tai būtina darbo funkcijoms atlikti ir atitinka nustatytus kibernetinio saugumo reikalavimus.
- 76. Visi nuotoliniai prisijungimai privalo būti atliekami naudojant šifruotus ryšio kanalus, siekiant užtikrinti perduodamos informacijos konfidencialumą ir vientisumą.
- 77. Nuotolinė prieiga draudžiama naudoti, jei nėra galimybės užtikrinti reikiamo saugumo lygio ar IS naudotojas/IS administratorius neatitinka autentifikavimo reikalavimų.
- 78. IS naudotojų nuotoliniam prisijungimo prie IS būdai ir jiems taikomi reikalavimai:
 - 78.1. turi būti naudojamas VPN;
 - 78.2. įrenginius, kuriuose įdiegta antivirusinė ir saugumo programinė įranga;
 - 78.3. IP adresų kontrolė (*whitelisting*);
 - 78.4. kelių veiksnių autentifikavimas;
 - 78.5. atskira administravimo paskyra (taikoma IS administratoriui);
 - 78.6. IS naudotojai gali jungtis prie IS tik iš įrenginių, kurie yra autorizuoti ir atitinka IID nustatytus techninius saugumo reikalavimus;
 - 78.7. Nuotolinė prieiga suteikiama ribotai pagal darbo funkcijas, laikantis mažiausios privilegijos principo;
- 79. Bet koks nuotolinis prisijungimas prie IS be aukščiau nurodytų saugumo priemonių draudžiamas.
- 80. Visi nuotolinio prisijungimo ryšiai privalo būti šifruojami naudojant saugias kriptografines priemones.
- 81. IS naudotojams nuotolinio darbo metu draudžiama naudoti:
 - 81.1. viešuosius Wi-Fi tinklus be VPN,
 - 81.2. tarpinius serverius ar anonimizavimo priemones,
 - 81.3. nežinomų tiekėjų ryšio sprendimus.
- 82. Prie kritinių IS leidžiama jungtis tik naudojant:
 - 82.1. VPN;
 - 82.2. įrenginius, kuriuose įdiegta antivirusinė ir saugumo programinė įranga;
- 83. tinklo ugniasienės/užkardos įrenginius,
- 84. IS turi neleisti automatiškai išsaugoti slaptažodžių nuotolinio prisijungimo priemonėse.
- 85. IS naudotojai privalo užtikrinti, kad nuotolinio prisijungimo metu jų įrenginiai nebūtų prieinami tretiesiems asmenims.
- 86. Nuotolinio prisijungimo sesija turi būti nedelsiant nutraukta, jei IS naudotojas baigia darbą ar pasitraukia nuo įrenginio.
- 87. Draudžiama naudoti nuotolinę prieigą:
 - 87.1. ne darbo funkcijoms atlikti,
 - 87.2. apeinant saugumo priemones,
 - 87.3. dalijantis prisijungimo duomenimis.
- 88. IS naudotojai privalo nedelsdami pranešti IS saugos įgaliotiniui apie įtartinę veiklą, galimus kenkėjiškus prisijungimus ar incidentus.
- 89. Incidentų valdymas:
- 90. Nustačius neleistinus ar rizikingus nuotolinio prisijungimo bandymus prie IS, IS administratorius savo iniciatyva turi blokuoti prisijungimą;
 - 90.1. IS administratoriai nedelsdami analizuoja incidentą, įvertina riziką ir prireikus inicijuoja:
 - 90.1.1. paskyros blokavimą;

- 90.1.2. slaptažodžio keitimą;
- 90.1.3. papildomas saugumo priemonės;
- 90.1.4. ryšio kanalų apribojimus.
- 90.2. apie incidentą nedelsiant informuojamas IS saugos įgaliotinis.

VIII SKYRIUS BAIGIAMOSIOS NUOSTATOS

- 91. Šios Taisyklės įsigalioja nuo jų patvirtinimo dienos ir yra privalomos visiems IID darbuotojams, IIDS dalyvių darbuotojams, paslaugų teikėjų atstovams ir kitiems asmenims, naudojantiems IID informacines sistemas ar tinklo išteklius.
- 92. Taisyklės peržiūrimos ne rečiau kaip vieną kartą per metus ar dažniau, jeigu įvyksta reikšmingi IS aplinkos pokyčiai, įskaitant, bet neapsiribojant:
 - 92.1. teisės aktų, reglamentuojančių kibernetinį saugumą, duomenų apsaugą ar IS valdymą pasikeitimai ar naujų susijusių teisės aktų priėmimas;
 - 92.2. naujų IID paslaugų, produktų ar informacinių sistemų diegimas;
 - 92.3. esminių organizacinių ar veiklos pokyčių atsiradimas;
 - 92.4. IID administruojamų fondų dalyvių veiklos pokyčiai;
 - 92.5. kibernetinio saugumo incidentai arba identifikuotos naujos rizikos.
- 93. Už šių Taisyklių peržiūrą, atnaujinimą, pakeitimų rengimą ir jų teikimą tvirtinimui IID direktoriui atsakingas IS saugos įgaliotinis.
- 94. IID darbuotojai su aktualia šių Taisyklių redakcija supažindinami per IID elektroninę dokumentą valdymo sistemą, o IS įgaliotinis ne vėliau kaip 1 mėn. atlieka šių Taisyklių aktualios redakcijos pristatymą/mokymus IID darbuotojams ir parengia ir išplatina atmintinę kiekvieną kartą, kai patvirtinama nauja Taisyklių redakcija.
- 95. IID darbuotojų ir paslaugos tiekėjų susipažinimas su Saugos dokumentais saugomis IID elektroninių dokumentų valdymo sistemoje;
- 96. IID darbuotojų pasirašyti konfidencialumo pasižadėjimai (1 priedas) saugomi IID darbuotojų asmens bylose.

KONFIDENCIALUMO PASIŽADĖJIMAS

20 m. d.

Vilnius

Aš,

(vardas, pavardė, pareigos)

patvirtinu, kad:

1. Esu supažindintas (-a) su VŠĮ „Indėlių ir investicijų draudimas“ (toliau – IID) informacijos saugą įgyvendinančiais dokumentais, vidaus tvarkomis bei teisės aktais, reglamentuojančiais duomenų saugą ir informacinių sistemų naudojimą.
2. Įsipareigoju saugoti visą man patikėtą darbo ar sutarties vykdymo metu sužinotą konfidencialią informaciją, įskaitant, bet neapsiribojant:
 - 2.1. asmens duomenimis,
 - 2.2. IID paslaptį sudarančią informaciją,
 - 2.3. informacinių sistemų duomenimis ir prisijungimo informacija.
3. Įsipareigoju:
 - 3.1. naudoti IID informacines sistemas tik darbo funkcijoms vykdyti;
 - 3.2. neatskleisti prisijungimo duomenų tretiesiems asmenims;
 - 3.3. užtikrinti, kad mano naudojami slaptažodžiai būtų saugūs ir nepasiekiami kitiems;
 - 3.4. pranešti apie neteisėtus kitų asmenų veiksmus, dėl kurių duomenys gali būti pakeisti ar prarasti, ir apie visas kitas įtartinas aplinkybes, galinčias kelti grėsmę duomenų konfidencialumui, vientisumui ar prieinamumui;
 - 3.5. nedelsiant pranešti apie galimus saugumo incidentus ar pažeidimus;
 - 3.6. neatskleisti konfidencialios informacijos tretiesiems asmenims tiek darbo metu ir/ar sutarties vykdymo metu, tiek pasibaigus darbo santykiams ir/ar sutartiniams įsipareigojimams.
4. Suprantu, kad netinkamas informacijos naudojimas ar atskleidimas gali užtraukti drausminę, administracinę ar baudžiamąją atsakomybę pagal galiojančius teisės aktus.
5. Įsipareigoju laikytis visų taikomų teisės aktų ir IID informacijos saugą įgyvendinančiuose dokumentuose ir vidaus tvarkose nustatytų reikalavimų, susijusių su informacijos sauga.
6. Esu įspėtas (-a), kad, pažeidęs (-usi) šį pasižadėjimą, turėsiu atsakyti pagal teisės aktus, reglamentuojančius atsakomybę už šių reikalavimų pažeidimą bei įsipareigoju atlyginti nuostolius IID teisės aktų nustatyta tvarka.
7. Šis pasižadėjimas galioja visą darbo ir/ar sutarties laikotarpį ir po darbo santykių ir/ar sutarties pasibaigimo.

(Pareigos)

(parašas)

(vardas pavardė)