PATVIRTINTA
Lietuvos Respublikos finansų ministro
2026 m. balandžio 28 d. įsakymu Nr. 1K-130

FINANSŲ MINISTERIJOS INFORMACINIŲ SISTEMŲ PRIEIGŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Finansų ministerijos informacinių sistemų prieigų valdymo tvarkos apraše (toliau – Aprašas) reglamentuojama Lietuvos Respublikos finansų ministerijos (toliau – ministerija) valdomų ir tvarkomų valstybės informacinių sistemų, vidaus administravimo informacinės sistemos, intraneto svetainės (toliau kartu – IS), vidinių IS naudotojų ir išorinių IS naudotojų (kuriems suteikta teisė naudotis ministerijos tvarkomų IS duomenimis (toliau – IS duomenys) (toliau kartu – IS naudotojai) ir juos tvarkyti) ir IS administratorių, IS infrastruktūros administratorių, IS veiklos administratorių ir vietinių naudotojų administratorių (toliau kartu – administratoriai) teisės ir pareigos, prieigų prie IS valdymo tvarka, taip pat slaptažodžių valdymo bei saugaus duomenų teikimo IS naudotojams kontrolės tvarka.

2. Aprašas taikomas:

2.1. IS naudotojams;

2.2. administratoriams.

3. Aprašas netaikomas ministerijos tvarkomiems socialiniams tinklams.

4. Prieiga prie IS duomenų suteikiama vadovaujantis šiais principais:

4.1. IS naudotojams ir administratoriams prieiga prie IS ir (arba) infrastruktūros tinklų turi būti suteikiama tik prie tų IS tvarkomų duomenų ir tik tokia apimtimi, kuri nustatyta IS nuostatuose ir reikalinga konkretaus ministerijos valstybės tarnautojo ar pagal darbo sutartį dirbančio darbuotojo (toliau kartu – darbuotojas) pareigybės aprašyme nurodytoms funkcijoms atlikti ar vykdant sutartinius įsipareigojimus.

4.2. Prieiga prie tvarkomų IS duomenų ir teisė juos tvarkyti suteikiama tik atlikus kiekvieno IS naudotojo ir kiekvieno administratoriaus identifikavimą ir patvirtinus jo tapatybę.

4.3. IS duomenis gali tvarkyti tik tokius įgaliojimus ir priskirtas prieigos teises turintys IS naudotojai.

4.4. IS priežiūros funkcijos turi būti atliekamos per tokios IS tam skirtą administratoriaus paskyrą, kuria naudojantis negalima atlikti IS naudotojo funkcijų.

4.5. Papildomos prieigos teisės IS naudotojams gali būti suteikiamos tik testuojant IS ir tik IS administratoriui kontroliuojant IS naudotojo darbą. Papildomos prieigos teisės turi būti panaikinamos per vieną darbo dieną nuo IS testavimo pabaigos.

4.6. Taikomi šie IS naudotojų ir administratorių paskyrų ir prieigos prie IS teisių valdymo principai:

4.6.1. Būtina žinoti (angl. *need to know*) – IS naudotojams turėtų būti suteikta prieiga tik prie tų ministerijos IS tvarkomų duomenų, kurie jiems reikalingi darbo funkcijoms atlikti ar sutartiniams įsipareigojimams vykdyti.

4.6.2. Mažiausios privilegijos (angl. *least privilege*) – IS naudotojams suteikiamos mažiausios prieigos prie ministerijos tinklų ir IS (toliau kartu – TIS), kurie jiems reikalingi darbo funkcijoms atlikti ar sutartiniams įsipareigojimams vykdyti, teisės, bet ne daugiau.

4.6.3. Pareigų atskyrimo (angl. *segregation of duties*) – ministerijoje turi būti sukurtos procedūros ir organizacinė struktūra, neleidžiančios vienam naudotojui kontroliuoti visų pagrindinių TIS veiklos aspektų ir atlikti neleistinų veiksmų ar neteisėtai pasiekti ministerijos TIS ir juose esančių duomenų.

5. IS duomenis tvarkyti gali tik tie IS naudotojai, kurie yra susipažinę su TIS saugos dokumentais – šiuo finansų ministro įsakymu patvirtintu Finansų ministerijos tinklų ir informacinių sistemų kibernetinio saugumo politikos aprašu (toliau – TIS kibernetinio saugumo politikos aprašas), Finansų ministerijos tinklų ir informacinių sistemų veiklos tęstinumo valdymo planu (su šiuo planu susipažįsta ministerijos darbuotojai ir IS vidiniai naudotojai, kuriems yra pareiga susipažinti su šio plano nuostatomis ir jomis vadovautis) ir Aprašu (toliau kartu – TIS saugos dokumentai) – ir sutikę laikytis juose nustatytų reikalavimų.

6. IS naudotojai ir administratoriai prisijungti prie IS gali tik susipažinę su TIS saugos dokumentais ir sutikę laikytis juose nustatytų reikalavimų.

7. IS naudotojai su TIS saugos dokumentais pirmą kartą prisijungdami prie IS susipažįsta tam tikslui toje IS skirta susipažinimo patvirtinimo priemone, pažymėdami savo sutikimą laikytis TIS saugos dokumentuose esančių nuostatų ir nustatytų reikalavimų ir patvirtindami susipažinimą su atsakomybe už visus veiksmus jiems naudojantis IS. Jei tokia susipažinimo patvirtinimo priemonė nėra realizuota IS, IS naudotojai su TIS saugos dokumentais susipažįsta užpildydami ir pasirašydami TIS kibernetinio saugumo politikos aprašo priedo „Finansų ministerijos tinklų ir informacinių sistemų ir juose esančių duomenų kibernetinio saugumo užtikrinimo taisyklės“ 2 priede nustatytos formos asmens, prižiūrinčio IS arba besinaudojančio jomis, įsipareigojimą. Šį įsipareigojimą prieš pradėdami administruoti atitinkamą IS pasirašo IS administratoriai ir IS infrastruktūros administratoriai. Pasirašyti įsipareigojimai pateikiami IS saugos įgaliotiniui, kuris juos saugo teisės aktų nustatyta tvarka.

8. Pakartotinai IS naudotojai ir administratoriai susipažįsta su pakeistais TIS saugos dokumentais elektroniniu būdu, jei IS yra tokia funkcinė galimybė. Jei tokios funkcinės galimybės nėra, IS naudotojų susipažinimą su TIS saugos dokumentais vykdo atitinkamos IS administratorius, o ministerijos darbuotojus su pasikeitusiais TIS saugos dokumentais supažindina IS saugos įgaliotinis, naudodamas ministerijos dokumentų valdymo sistemą.

9. IS duomenų teikėjai ar gavėjai, IS priežiūros paslaugų teikėjai su pasikeitusiais TIS saugos dokumentais susipažįsta pakartotinai viešai juos paskelbus ministerijos interneto svetainėje. Už paslaugų teikėjų supažindinimą su atnaujintais TIS saugos dokumentais atsakingi už paslaugų sutarties vykdymą paskirti atsakingi ministerijos darbuotojai.

10. IS naudotojai, administratoriai, pažeidę Taisyklių ar kitų TIS saugos politiką reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos administracinių nusižengimų kodekso ir kitų teisės aktų, reglamentuojančių atsakomybę už IS saugos reikalavimų nesilaikymą, nustatyta tvarka.

11. Administratorių ir IS saugos įgaliotinio funkcijos nustatytos TIS kibernetinio saugumo politikos apraše.

12. Apraše vartojamos sąvokos suprantamos taip, kaip apibrėžiamos 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 (Bendrasis duomenų apsaugos reglamentas), Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, kituose teisės aktuose, reglamentuojančiuose kibernetinę saugą, ir Lietuvos standarte LST EN ISO/IEC 27000:2020.

II SKYRIUS
IS NAUDOTOJŲ IR ADMINISTRATORIŲ PASKYRŲ IR PRIEIGŲ VALDYMAS

PIRMASIS SKIRSNIS
IS NAUDOTOJO, ADMINISTRATORIAUS PRIEIGŲ PRIE IS SUTEIKIMO BENDROSIOS NUOSTATOS

13. Paskyras, kurios yra unikalus IS naudotojo identifikatorius, suteikiantis IS naudotojui ar techninei sistemai prieigą prie IS, gali sukurti tik finansų ministro tam tikrai IS paskirtas IS administratorius.

14. IS valdytojo ar jo įgalioto IS tvarkytojo paskirti konkrečios IS administratoriai ar IS infrastruktūros administratoriai valdo (suteikia, stabdo, keičia, panaikina) naudotojų prieigą prie tam tikros IS paskyros. Tam tikrais atvejais išoriniams IS naudotojams prieigos prie IS paskyros valdymas gali būti perduotas kitoms įstaigoms, įpareigojant jas paskirti vietinį IS naudotojų administratorių, atsakingą už įstaigos ir įstaigos vadovo valdymo srityje veikiančių įstaigų išorinių IS naudotojų prieigos valdymą, priskiriant jiems atitinkamas prieigos prie IS teises, atitinkančias jų atliekamas funkcijas.

ANTRASIS SKIRSNIS
IS NAUDOTOJO REGISTRAVIMAS IR JO TAPATYBĖS NUSTATYMAS

15. IS administratorius, IS infrastruktūros administratorius registruoja asmenį IS naudotoju, jeigu jis atitinka visas šias sąlygas:

15.1. gautas jo rašytinis prašymas ir užpildyta nustatytos formos IS naudotojo registracijos kortelė (jei tokios kortelės forma nustatyta atitinkamos IS nuostatuose ar kitame IS veiklą reglamentuojančiame dokumente), kurios privalomų duomenų sąrašas pateiktas Aprašo priede;

15.2. IS naudotojui negali būti suteiktos IS administratoriaus teisės, o IS administratorius negali iš savo paskyros atlikti IS naudotojo veiksmų.

16. Tokiose IS, kurias naudoja ir kitos valstybės ar savivaldybės įstaigos, turi būti galimybė registruoti konkrečios įstaigos paskirtą vietinį IS naudotojų administratorių, atsakingą už savo įstaigos ir įstaigos vadovo valdymo srityje veikiančių įstaigų išorinių IS naudotojų registravimą ir prieigos prie IS teisių jiems priskyrimą.

17. IS administratoriams prieigos teises suteikia ir panaikina IS valdytojo paskirtas kitas atitinkamos IS administratorius.

18. IS naudotojai registruojami tokia tvarka:

18.1. IS naudotojai registruojami ir prieigos prie IS teises jiems suteikia IS administratorius, o jei yra paskirtas ir įgaliotas, prieigas gali suteikti ir vietinis IS naudotojų administratorius.

18.2. Pasikeitus IS naudotojo funkcijoms, jo prieigos teisės koreguojamos. Apie pasikeitimus, kuriuos reikia atlikti, ministerijos Informacinių technologijų departamentą (toliau – ITD) raštu informuoja ministerijos struktūrinis padalinys, kuriame dirba IS naudotojas, arba įstaiga, kurios darbuotojas naudoja ministerijos IS, pateikdami informaciją elektroniniu paštu – atsiųsdami užpildytą nustatytos formos IS naudotojo registracijos kortelę, jei tokios kortelės forma nustatyta atitinkamos IS veiklą reglamentuojančiuose dokumentuose. Apie Valstybės biudžeto, apskaitos ir mokėjimų sistemos (toliau – VBAMS) naudotojo funkcijų pasikeitimus, kuriuos reikia atlikti, ministerijos Apskaitos informacinių sistemų strategijos valdymo grupę (toliau – AISSVG) raštu informuoja ministerijos struktūrinis padalinys, kuriame dirba VBAMS naudotojas, arba įstaiga, kurios darbuotojas naudoja VBAMS, pateikdami IS naudotojų registracijos korteles, kaip tai numatyta

Valstybės biudžeto, apskaitos ir mokėjimų sistemos naudotojų skaičiaus nustatymo, identifikavimo kortelių formų pildymo ir kortelių pateikimo taisyklėse, patvirtintose Lietuvos Respublikos finansų ministro 2006 m. balandžio 6 d. įsakymu Nr. 1K-152 „Dėl Valstybės biudžeto, apskaitos ir mokėjimų sistemos nuostatų patvirtinimo“. Jeigu įstaigoje yra paskirtas vietinis IS naudotojų administratorius, pasikeitus šios įstaigos IS naudotojo funkcijoms, jo prieigos teises koreguoja vietinis IS naudotojų administratorius.

18.3. IS naudotojams prieigos teisės suteikiamos per laikotarpį, nustatytą pagal atitinkamos IS administravimo tvarką. Jeigu tokios tvarkos nėra nustatytos, prieigos teisės suteikiamos ne vėliau kaip per vieną darbo dieną nuo rašytinio prašymo gavimo dienos, jei prašyme nurodyti teisingi ir tikslūs duomenys, arba ne vėliau kaip iki prašyme nurodyto termino pabaigos, jei terminas buvo nurodytas.

18.4. IS naudotojai registruojami vadovaujantis atitinkamos IS naudotojų registravimo tvarka, kuri nustatyta kiekvienos IS veiklą reglamentuojančiuose teisės aktuose. Už šios tvarkos nustatymą atsakingi konkrečios IS administravimą atliekantys ministerijos struktūriniai padaliniai.

19. Priemonės IS naudotojų tapatybei nustatyti:

19.1. IS naudotojo prisijungimo vardas, slaptažodis ir prieigos teisių rinkiniai yra svarbiausia saugos priemonė, leidžianti apsaugoti IS ir jose tvarkomus duomenis. Jeigu prisijungiant prie IS naudojamas prisijungimas per Valstybės informacinių išteklių sąveikumo platformą ar Elektroninius valdžios vartus, IS naudotojams identifikuoti naudojami atitinkami prisijungimo būdai.

19.2. IS naudotojų autentiškumo užtikrinimo priemonės yra šios:

19.2.1. Kiekvienam IS naudotojui priskiriamas unikalus naudotojo prisijungimo vardas. Draudžiama priskirti vienodą IS naudotojo prisijungimo vardą keliems IS naudotojams.

19.2.2. Visi IS naudotojo prisijungimo vardai turi būti susieti su slaptažodžiu, siekiant užtikrinti, kad IS naudotojo vardu naudojasi tik tas asmuo, kuriam jis priskirtas.

19.2.3. IS naudotojai atsako už IS naudotojo vardo ir slaptažodžių naudojimo saugumo reikalavimų laikymąsi.

19.2.4. Pagal IS naudotojų atliekamas funkcijas jiems priskiriami atitinkami prieigos teisių rinkiniai.

19.2.5. IS naudotojų prisijungimo prie IS ekrano vaizdo forma turi būti sukurta taip, kad bandančiam prisijungti IS naudotojui nebūtų suteikiama informacija, palengvinanti IS naudotojo vardo ir slaptažodžio spėjimą.

20. IS naudotojai ir administratoriai turi patvirtinti savo tapatybę slaptažodžiu ir papildoma kelių veiksnių tapatumo nustatymo priemone, tokia kaip PIN kodas, SMS žinutė ar biometriniai duomenys.

TREČIASIS SKIRSNIS
IS NAUDOTOJŲ IR ADMINISTRATORIŲ PRIEIGOS PRIE IS TEISIŲ SUSTABDYMAS

21. IS naudotojo ar administratoriaus prieigos prie IS teisė stabdoma nedelsiant, ne vėliau nei per vieną darbo dieną, nustačius, kad jis naudoja IS pažeisdamas ministerijos TIS saugos dokumentuose ar kituose su duomenų tvarkymu susijusiuose teisės aktuose nustatytus reikalavimus.

22. Pasikeitus IS naudotojo funkcijoms, jo prieigos prie IS teises koreguoja paskirtas atitinkamos IS administratorius. Apie pasikeitimus, kuriuos reikia atlikti, ministerijos Personalo valdymo skyrius vidiniu raštu per dokumentų valdymo bendrąją IS ar elektroniniu paštu informuoja ministerijos ITD arba ministeriją informuoja įstaiga, kurioje dirba IS naudotojas.

23. IS naudotojo ar administratoriaus prisijungimo paskyra užblokuojama, kad nebūtų galima

prisijungti prie IS, tačiau nėra ištrinama iš IS duomenų bazių ir įvykių žurnalų, kol juose yra IS naudotojo ar administratoriaus darytų įrašų, kad išliktų galimybė atsekti jo veiksmus IS. Ši informacija saugoma ne ilgiau kaip 6 mėnesius po IS naudotojo ar administratoriaus teisės dirbti su konkrečia IS sustabdymo dienos. Po šio laikotarpio, jei IS techninės galimybės leidžia ir tai neprieštarauja duomenų vientisumo išlaikymo principams, prisijungimo paskyra gali būti visiškai pašalinta.

24. IS naudotojų paskyros, kurios nenaudojamos ilgiau kaip 3 mėnesius, o administratoriaus paskyros, kurios nenaudojamos ilgiau kaip 2 mėnesius, turi būti sustabdomos.

25. Jeigu IS naudotojui iškyla poreikis naudotis IS po ilgiau nei 90 kalendorinių dienų, o administratoriui po ilgiau nei 60 kalendorinių dienų:

25.1. ministerijos struktūrinio padalinio vadovas vidiniu raštu per dokumentų valdymo bendrąją IS turi informuoti ministerijos ITD, kad būtų atkurtos IS naudotojo prieigos teisės;

25.2. kitos įstaigos, naudojančios ministerijos IS, turi IS sistemos bendruoju elektroniniu paštu, kurio adresas nurodytas ministerijos interneto svetainėje, informuoti atitinkamos IS administratorių, kad būtų atkurtos išorinio IS naudotojo prieigos teisės. Jei įstaigoje yra paskirtas vietinis IS naudotojų administratorius ir jam suteiktos tokios teisės, jis atkuria įstaigos IS naudotojo prieigos teises.

26. Jeigu ministerijos valdomos ir tvarkomos Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinės sistemos (toliau – VSAKIS) naudotojai konsoliduotąsias finansines ataskaitas rengia vieną kartą per metus, jų naudotojų paskyros po 90 kalendorinių dienų nestabdomos. Visiems VSAKIS naudotojams jungiantis po nurodyto termino reikalaujama pasikeisti slaptažodį.

KETVIRTASIS SKIRSNIS
IS NAUDOTOJŲ IR ADMINISTRATORIŲ PRIEIGOS PRIE IS PANAIKINIMAS

27. IS naudotojo ar administratoriaus prieigos prie IS panaikinamos tokia tvarka:

27.1. Kai IS vidinis naudotojas ar administratorius nušalinamas ar atleidžiamas iš pareigų arba nebeatlieka funkcijų, kurioms atlikti jam buvo suteikta prieiga prie ministerijos IS, praranda patikimumą, ministerijos Personalo valdymo skyrius privalo prieš 5 darbo dienas elektroniniu paštu adminai@finmin.lt informuoti ministerijos ITD, kad laiku būtų panaikinta vidinio IS naudotojo ar administratoriaus prieiga prie IS.

27.2. Panaikinus IS naudotojo ar administratoriaus teisę dirbti su IS, visos jam suteiktos prieigos prie IS panaikinamos ne vėliau kaip atleidimo ar perkėlimo į kitas pareigas dieną. Prieigos teises panaikina atitinkamos IS paskirtas administratorius.

27.3. Dėl Atvirųjų finansų informacinės sistemos (toliau – AFIS) funkcinių galimybių veikimo užtikrinimo paskyros negali būti blokuojamos, todėl AFIS administratorius nenaudojamų paskyrų blokavimą užtikrina kartą per ketvirtį patikrindamas AFIS naudotojų prisijungimą rankiniu būdu, ar buvo nesijungusių ilgiau negu 6 mėnesius, ir blokuoja ilgiau negu 6 mėnesius nenaudojamas paskyras.

27.4. IS naudotojui neatliekant jokių veiksmų, kompiuterizuota darbo vieta turi užsirakinti, kad toliau naudotis IS būtų galima tik pakartotinai patvirtinus savo tapatybę. Ilgiausias neaktyvumo laikas, kuriam pasibaigus IS naudotojų ryšio sesijos automatiškai nutraukiamos, turi būti ne ilgesnis kaip 15 minučių. Šis reikalavimas netaikomas, jeigu, atlikus TIS rizikos vertinimą, nustatomos kitos nustatytą riziką atitinkančios techninės kibernetinio saugumo priemonės. Europos Sąjungos struktūrinės paramos kompiuterinės informacinės valdymo ir priežiūros sistemos (SFMIS) ilgiausias neaktyvumo laikas yra 1 valanda. VSAKIS ilgiausias neaktyvumo laikas yra 4 valandos.

PENKTASIS SKIRSNIS
IS NAUDOTOJŲ TEISĖS IR PAREIGOS

28. IS naudotojų teisės:

28.1. Naudoti IS ir tvarkyti jose kaupiamus duomenis turi teisę tik registruoti IS naudotojai.

28.2. IS naudotojas gali turėti tik tokias prieigos prie IS teises, kurios jam yra reikalingos jo darbo funkcijoms atlikti.

28.3. IS naudotojų IS duomenų tvarkymo teisės ribojamos įgaliojimais (teisėmis), nustatančiais prieigos prie ministerijos IS duomenų lygį.

28.4. IS naudotojai, kuriems suteikta teisė tvarkyti IS duomenis, juos tvarko (keičia, atnaujina, įveda ir naikina) vadovaudamiesi IS naudojimo instrukcijomis (naudotojų vadovais), kuriuos tvirtina finansų ministro įsakymu paskirtas atitinkamos IS duomenų valdymo įgaliotinis. Už IS tvarkomų duomenų teisingumą atsakingas juos tvarkantis IS naudotojas.

28.5. Kai tam pačiam asmeniui reikia suteikti IS administratoriaus prieigą ir IS naudotojo prieigą, jam sukuriamos atskiros paskyros (IS administratoriaus paskyra ir IS naudotojo paskyra) atitinkamoms funkcijoms atlikti.

28.6. IS naudotojai turi teisę kreiptis į IS saugos įgaliotinį, IS administratorių, IS infrastruktūros administratorių IS naudojimo ir saugos klausimais. Asmens duomenų apsaugos klausimais IS naudotojai konsultuojasi su ministerijos duomenų apsaugos pareigūnu.

29. IS naudotojų pareigos tvarkant IS duomenis:

29.1. užtikrinti jų naudojamų ir tvarkomų IS duomenų konfidencialumą, vientisumą, savo veiksmais netrikdyti IS duomenų prieinamumo;

29.2. tinkamai tvarkyti IS duomenis ir saugoti tvarkomų IS duomenų paslaptį vadovaujantis IS duomenų tvarkymą ir apsaugą reglamentuojančiais teisės aktais ir (ar) duomenų teikimo sutartimis;

29.3. susipažinti su ministerijos IS naudojimo instrukcijomis (naudotojų vadovais) ir jomis vadovautis;

29.4. atsijungti nuo visų IS prieš baigiant darbą su kompiuteriu;

29.5. apie pastebėtus IS naudojimo sutrikimus, pavojus kompiuterių tinklui ar IS duomenų saugumui, TIS saugos dokumentuose nustatytų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias IS kibernetinio saugumo užtikrinimo priemones nedelsiant, ne vėliau nei per vieną darbo dieną, informuoti naudojamos IS administratorių ir (arba) IS infrastruktūros administratorių ar IS saugos įgaliotinį;

29.6. vykdyti IS valdytojo, IS tvarkytojo, IS saugos įgaliotinio, IS administratorių ir (arba) IS infrastruktūros administratorių nurodymus dėl IS naudojimo ir IS duomenų saugos.

30. IS naudotojams draudžiama:

30.1. palikti kompiuterizuotą darbo vietą neįjungus slaptažodžiu apsaugotos ekrano užsklandos, kad nebūtų sudaryta galimybė kitam asmeniui dirbti su IS pasinaudojus svetimu prisijungimo vardu ir slaptažodžiu;

30.2. atskleisti kitiems asmenims jiems suteiktą prisijungimo prie IS vardą ir slaptažodį, IS naudotojo tapatybės kodą ar kitą informaciją, leidžiančią naudojantis programinėmis ir techninėmis priemonėmis sužinoti tvarkomus IS duomenis;

30.3. atskleisti tvarkomus IS duomenis ar suteikti kitokią galimybę bet kokia forma su ja susipažinti tokios teisės neturintiems asmenims;

30.4. prisijungti prie IS naudojantis kitam IS naudotojui suteiktais prisijungimo vardais ir slaptažodžiais, IS naudotojo tapatybės kodais ar kita informacija, leidžiančia naudojantis programinėmis ir techninėmis priemonėmis sužinoti tvarkomus IS duomenis;

30.5. naudoti IS duomenis kitokiais nei IS nuostatuose, kituose teisės aktuose ar sutartyse nurodytais tikslais;

30.6. atlikti veiksmus, dėl kurių gali būti neteisėtai pakeisti ar sunaikinti IS duomenys, arba atlikti bet kokius kitus neteisėtus IS duomenų tvarkymo veiksmus.

ŠEŠTASIS SKIRSNIS
PRIEIGOS PRIE IS DUOMENŲ LYGIAI

31. Administratoriai registruoja, išregistruoja IS naudotojus, administruoja IS naudotojų prieigos prie IS teises.

32. IS administratoriai ir IS infrastruktūros administratoriai tvarko IS nustatymų duomenis, diegia IS pakeitimus. Jiems suteikiamos teisės skaityti ir redaguoti IS naudotojų duomenis, matyti IS naudotojų atliktus veiksmus su tvarkomais IS duomenimis, skaityti ir redaguoti IS nustatymų duomenis, taip pat teisė naudoti IS priemones, reikalingas IS pakeitimams įdiegti, IS klaidoms nustatyti ir pašalinti.

33. Siekiant išskirti IS administratorių funkcijas, gali būti skiriami vietiniai IS naudotojų administratoriai, turintys teisę administruoti tik savo įstaigos IS naudotojų prieigą arba tam tikru atveju ir viešojo sektoriaus subjektų, jei jų veikla yra centralizuota, IS naudotojų prieigą. Vietiniams IS naudotojų administratoriams taikomi tie patys informacijos saugos reikalavimai, kaip ir administratoriams.

34. IS infrastruktūros administratorius administruoja vidinės Administravimo informacinės sistemos (AIS) naudotojų prieigos teises, vykdo techninę IS infrastruktūros priežiūrą. IS infrastruktūros administratoriui gali būti suteikta teisė jungtis prie IS ir skaityti IS duomenis, kiek to reikia IS infrastruktūros administratoriaus funkcijoms atlikti.

35. IS administratoriams suteikiama tiesioginė prieiga prie IS duomenų bazių naudojantis IS naudojamos duomenų bazių valdymo sistemos palaikomomis priemonėmis.

36. IS administratorius, atsakingas už IS duomenų bazės priežiūrą, neturi teisės tvarkyti IS duomenų kitaip, kaip tik vykdydamas su IS administravimu susijusias užduotis.

37. IS administratoriams ir vietiniams IS naudotojų administratoriams draudžiama suteikti IS naudotojams:

37.1. teises skaityti IS duomenis tiesiai iš ministerijos IS duomenų bazės lentelių ar taisyti IS duomenis jose;

37.2. prieigą prie IS kodų, duomenų bazių objektų, IS kūrimo ir programavimo įrankių.

38. Laikina prieiga prie IS gali būti suteikiama atsakingoms institucijoms ir įstaigoms, kurios yra įgaliotos gauti iš IS reikiamus IS duomenis ar atlikti patikras. Tokiu atveju institucijos ar įstaigos raštu kreipiasi į ministerijos IS valdytojo paskirtus konkrečios IS duomenų valdymo įgaliotinius, prašydamos suteikti laikiną prieigą prie IS duomenų, nurodydamos prisijungimo tikslą, reikiamą prisijungimo prie IS laikotarpį bei prie kokių IS duomenų norima gauti prieigą. Ministerijos ITD ar AISSVG, gavę iš IS duomenų valdymo įgaliotinio raštą, suteikia prieigą prie IS duomenų per naršyklės prieigą su peržiūros teisėmis.

39. IS naudotojai ir administratoriai, kurie tvarko IS duomenis (įskaitant asmens duomenis), privalo juos saugoti, jei jie neskirti skelbti viešai. Ši pareiga galioja ir pasibaigus valstybės tarnybos ar darbo santykiams.

40. Kitų įstaigų darbuotojai, kurie naudoja ministerijos IS, privalo vykdyti IS valdytojo, IS tvarkytojo, IS kibernetinio saugumo vadovo, IS saugos įgaliotino, IS administratorių ir (arba) IS infrastruktūros administratorių nurodymus dėl IS naudojimo.

SEPTINTASIS SKIRSNIS
SLAPTAŽODŽIŲ SUDARYMAS IR KEITIMAS

41. IS naudojami slaptažodžiai turi atitikti šiuos IS naudotojams ir administratoriams taikomus slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimus:

41.1. IS naudotojo slaptažodis turi būti ne trumpesnis kaip 10 simbolių ir keičiamas ne rečiau kaip kartą per 3 mėnesius.

41.2. Administratoriaus slaptažodis turi būti ne trumpesnis kaip 15 simbolių ir keičiamas ne rečiau kaip kartą per 2 mėnesius.

41.3. Slaptažodis turi būti sudarytas iš didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų simbolių.

41.4. Keičiant slaptažodį, taikomoji programinė įranga turi neleisti administratoriams sudaryti slaptažodžio iš buvusių 8 paskutinių slaptažodžių, o IS naudotojams – 6 paskutinių slaptažodžių, kad slaptažodžiai nebūtų naudojami pakartotinai.

41.5. Slaptažodžiui sudaryti draudžiama naudoti asmeninio pobūdžio arba kitą lengvai atspėjamą informaciją: gimimo datą, asmens kodą, šeimos narių vardus ir panašiai.

41.6. Slaptažodis negali būti sudarytas iš pasikartojančių arba nuoseklių simbolių, tokių kaip „aaaaaaaaaaaa“ arba „0123456789“, ar įprastos klaviatūros sekos (pvz., „Qwerty“).

41.7. Draudžiama techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti vadovaujantis šiame punkte nustatytais reikalavimais.

41.8. Pirmo prisijungimo prie IS metu programinė įranga automatiškai turi inicijuoti, kad IS naudotojas pakeistų konkrečios IS paskirto administratoriaus suteiktą laikiną IS prisijungimo slaptažodį į jam vienam žinomą slaptažodį.

41.9. Po 5 nesėkmingų bandymų prisijungti prie IS bandant atspėti IS naudotojo prisijungimo vardą ir (arba) slaptažodį IS turi blokuoti naudotoją ir neleisti toliau spėlioti slaptažodžio. Atblokuoti IS naudotoją gali tik administratoriai.

42. Ministerijos darbuotojui draudžiama:

42.1. slaptažodžius siųsti elektroniniais laiškais (išskyrus pirminį slaptažodį, kurį reikia iš karto pasikeisti);

42.2. slaptažodžius atskleisti kitiems asmenims ir įvardyti telefoninio pokalbio metu;

42.3. nešifruotus slaptažodžius laikyti bet kur ministerijos patalpose (išskyrus seifą);

42.4. slaptažodžius saugoti elektronine forma bendruose S disko kataloguose ar kompiuterizuotoje darbo vietoje, jei jie yra nešifruoti.

43. IS naudotojas, pamiršęs, praradęs arba kitaip netekęs savo prisijungimo prie IS vardo ir (ar) slaptažodžio, kai tik apie tai sužino, elektroniniu paštu arba telefonu informuoja konkrečios IS paskirtą administratorių. Administratorius turi įsitikinti IS naudotojo tapatybe ir suteikti jam laikiną slaptažodį, kurį IS naudotojas jungdamasis prie IS turi pasikeisti.

AŠTUNTASIS SKIRSNIS
PRIEMONĖS IR BŪDAI JUNGTIS PRIE IS BEI PRIEIGOS KONTROLĖS BŪDAI

44. Jungtis prie IS leidžiama, jeigu tenkinamos visos šios sąlygos:

44.1. suteiktas unikalus IS naudotojo prisijungimo vardas;

44.2. nustatytas IS naudotojo prieigos prie IS duomenų lygis, kuris buvo pateiktas su atitinkamos IS naudotojo registracijos kortele (jei tokia kortelė patvirtinta);

44.3. daromi įrašai apie visus asmenis, kuriems suteikta prieigos prie IS teisė;

44.4. vykdomas periodinis, bet ne rečiau kaip kartą per 3 mėnesius, IS naudotojų prisijungimo vardų ir informacijos apie juos tikrinimas ir neaktualios informacijos šalinimas.

45. Prieigos prie IS kontrolės priemonės:

45.1. Prieigai kontroliuoti ir IS naudotojo tapatybei nustatyti taikoma prisijungimo vardų, slaptažodžių ir teisių sistema arba IS naudotojai jungiasi naudodamiesi Valstybės informacinių išteklių sąveikumo platforma.

45.2. IS naudotojų veiksmai registruojami IS įvykių žurnaluose. IS naudotojų veiksmai registruojami pagal IS technines ir programines galimybes.

45.3. Išorinio IS naudotojo galimybę prisijungti prie IS inicijuojantis ministerijos struktūrinis padalinys arba įstaiga, kurios darbuotojui reikia suteikti prieigą prie ministerijos IS, teikia prašymą ministerijos ITD arba AISSVG.

45.4. Ministerijos ITD direktoriaus, o jo laikinai nesant – jo funkcijas laikinai atliekančio darbuotojo, o dėl VBAMS – AISSVG vadovo nurodyti ministerijos ITD ar AISSVG darbuotojai su IS išoriniu naudotoju suderina technines prijungimo prie IS sąlygas ir per 5 darbo dienas nuo atsakingo asmens patvirtinimo dienos suteikia išoriniam IS naudotojui prieigą prie IS.

45.5. Lietuvos Respublikos ar užsienio šalies juridiniams ar fiziniams asmenims, kuriems Lietuvos Respublikos teisės aktai ar paslaugų teikimo sutartys numato galimybę prisijungti prie IS ir kuriems tiesiogiai prisijungti yra būtina, suteikiama prieiga prie darbui būtinų IS išteklių.

45.6. IS tvarkytojas nustato IS prieigos kontrolės priemones ir reikalavimus, kuriais būtų tinkamai suderintas apsaugos nuo neteisėtos prieigos priemonių taikymas ir užtikrinta IS naudotojų veiklos poreikius atitinkanti prieiga.

46. Leidžiami nuotolinio IS naudotojų ir administratorių prisijungimo prie IS būdai:

46.1. Nuotolinis prisijungimas prie IS leidžiamas per internetinę prisijungimo sąsają, naudojant dviejų faktorių autentifikaciją bei saugius duomenų perdavimo protokolus.

46.2. Nuotolinis prisijungimas prie IS tarnybinių stočių galimas tik naudojantis virtualiųjų privačiųjų tinklų technologija (angl. *virtual private network, VPN*).

46.3. Jungiantis prie IS, kurios yra Valstybiniame duomenų centre, naudojamas dviejų faktorių autentifikavimas, taip pat naudojamas privilegijuotos prieigos valdymo (angl. *privileged access management, PAM*) sprendimas ir visi administratorių veiksmai stebimi Valstybės skaitmeninių sprendimų agentūros direktoriaus nustatyta tvarka.

III SKYRIUS
BAIGIAMOSIOS NUOSTATOS

47. Apraše nurodyti asmens duomenys tvarkomi IS naudotojų ir administratorių tapatybės nustatymo (identifikavimo) ir autentifikavimo, prieigos teisių suteikimo ir valdymo, IS naudojimo saugumo užtikrinimo ir kontrolės, veiksmų atsekamumo ir audito, komunikacijos su IS naudotojais ir administratoriais, sutartinių įsipareigojimų vykdymo tikslais, laikantis Reglamente (ES) 2016/679 nustatytų reikalavimų.

48. Apraše nurodyti dokumentai ir duomenys tvarkomi ir saugomi vadovaujantis Lietuvos Respublikos dokumentų ir archyvų įstatymo ir jo įgyvendinamųjų teisės aktų nustatyta tvarka ir terminais.

_____

Finansų ministerijos informacinių sistemų
prieigų valdymo tvarkos aprašo
priedas

INFORMACINĖS SISTEMOS NAUDOTOJO REGISTRACIJOS KORTELĖS PRIVALOMŲ DUOMENŲ SARAŠAS

1. Institucijos, įstaigos ar jos struktūrinio padalinio pavadinimas.
2. Informacinės sistemos (toliau – IS) pavadinimas.
3. IS posistemio (-ių) pavadinimai (jei IS turi posistemius).
4. Kortelės pildymo data ir numeris.
5. Kortelės paskirtis.
6. Informacija apie naudotoją:

6.1. vardas, pavardė;

6.2. pareigų pavadinimas;

6.3. darbo elektroninio pašto adresas, darbo ryšio numeris;

6.4. naudotojo kodas IS (jei naudojamas);

6.5. priskiriama naudotojo teisių grupė.

7. Naudotojo struktūrinio padalinio vadovo vardas, pavardė, pareigų pavadinimas, parašas.
8. Naudotojo vardas, pavardė, pareigų pavadinimas, parašas.
9. Naudotojo patvirtinimas dėl susipažinimo su saugos dokumentais (jei IS nėra elektroninio susipažinimo su saugos dokumentais galimybės pirmą kartą jungiantis prie IS).

_____