PATVIRTINTA

Valstybinio socialinio draudimo fondo

valdybos prie Socialinės apsaugos ir

darbo ministerijos direktoriaus

2024 m. rugpjūčio 18 d.

įsakymu Nr. V-287

# VALSTYBINIO SOCIALINIO DRAUDIMO FONDO VALDYBOS PRIE SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS INFORMACINĖS SISTEMOS, LIETUVOS RESPUBLIKOS APDRAUSTŲJŲ VALSTYBINIU SOCIALINIU DRAUDIMU IR VALSTYBINIO SOCIALINIO DRAUDIMO IŠMOKŲ GAVĖJŲ REGISTRO BEI LIETUVOS RESPUBLIKOS PENSIJŲ KAUPIMO DALYVIŲ, PENSIJŲ KAUPIMO IR PENSIJŲ IŠMOKŲ SUTARČIŲ REGISTRO SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

### I SKYRIUS

### BENDROSIOS NUOSTATOS

1. Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) reglamentuoja Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos (toliau – Fondo valdyba) valdomų Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinėje sistemoje (toliau – Fondo valdybos IS), Lietuvos Respublikos apdraustųjų valstybiniu socialiniu draudimu ir valstybinio socialinio draudimo išmokų gavėjų registre bei Lietuvos Respublikos pensijų kaupimo dalyvių, pensijų kaupimo ir pensijų išmokų sutarčių registre (toliau – Registrai) tvarkomos elektroninės informacijos saugaus tvarkymo principus.
2. Taisyklės yra parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu 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“.
3. Taisyklėse vartojamos sąvokos:
   1. **Administratorius** – Fondo valdybos darbuotojas, atliekantis IS taikomųjų sistemų, duomenų bazių, tarnybinių stočių, tinklo ar kitos kompiuterinės įrangos priežiūrą, užtikrinantis veikimą ir elektroninės informacijos saugą.
   2. **Darbuotojas** – Fondo administravimo įstaigos valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį.
   3. **Elektroninė informacija –** Fondo valdybos IS ir Registruose tvarkomi duomenys, dokumentai ir informacija.
   4. **Elektroninė paslauga –** paslauga, skirta Fondo valdybos informacinėje sistemoje registruotam elektroninės paslaugos gavėjui, kuriam yra suteikiama galimybė jo buvimo vietoje elektroninėmis ryšio priemonėmis atlikti veiklas, susijusias su socialiniu draudimu, bei gauti reikalingą informaciją toje apimtyje, kiek tai yra susiję su elektroninės paslaugos gavėju.
   5. **Elektroninės paslaugos gavėjas** – draudėjo vadovas, jo įgaliotas darbuotojas, asmens sveikatos priežiūros įstaigos gydytojas, apdraustieji ir išmokų gavėjai bei kiti Lietuvos gyventojai, sulaukę 18 metų, turintys teisę jungtis prie Fondo valdybos IS taikomųjų sistemų, teikiančių elektronines valstybinio socialinio draudimo paslaugas.
   6. **Fondo administravimo įstaigos** - Fondo valdyba, Fondo valdybos teritoriniai skyriai.
   7. **Fondo valdybos teritoriniai skyriai** – Valstybinio socialinio draudimo fondo valdybos teritoriniai skyriai.
   8. **IS naudotojas** – Fondo administravimo įstaigos darbuotojas, kuriam suteikta teisė naudotis IS.
   9. **Saugos įgaliotinis** – Fondo valdybos direktoriaus įsakymu paskirtas Fondo valdybos darbuotojas, koordinuojantis ir prižiūrintis saugos politikos įgyvendinimą Fondo valdybos IS.
   10. **Vieša elektroninė informacija** – tai bendro pobūdžio informacija apie valstybinį socialinį draudimą, Fondo administravimo įstaigų funkcijas ir teikiamas paslaugas, juos reglamentuojančių teisės aktų nuostatos, jų taikymo išaiškinimai, kita bendro pobūdžio informacija, susijusi su Fondo administravimo įstaigomis, kurioje nėra tiesiogiai pateikiami jokie Fondo administravimo įstaigų tvarkomi konkretaus asmens duomenys ir kurioje esančių duomenų negalima susieti su jokiu konkrečiu asmeniu.
   11. **Viešai neskelbtina/ konfidenciali informacija** - visa Fondo valdybos informacija, jei Fondo valdyba raštu nėra patvirtinusi, kad informacija nėra konfidenciali. Konfidencialia taip pat nėra laikoma informacija, kuri yra viešai prieinama.
   12. **Ugniasienė** (angl.[*Firewall*](res://\\ld1063.dll/type=1_word=firewall)) **-** techninė programinė įrangaparemta duomenų filtru, kuri analizuoja bei valdo per ją einantį duomenų srautą ir yra skirta vidinio tinklo saugumui užtikrinti.
4. Fondo valdybos IS ypatingos svarbos elektroninė informacija priskiriama vienai elektroninės informacijos IS naudotojų grupei, kurią sudaro visi Fondo administravimo įstaigų IS naudotojai.
5. Fondo valdybos IS saugumo lygis nustatomas pagal tvarkomos elektroninės informacijos saugumo principų, konfidencialumo, vientisumo ir prieinamumo, galimus pažeidimo padarinius. Taikytinos saugumo priemonės pasirenkamos pagal reikalaujamą saugumo lygį:
   1. Aukštas saugumo lygis taikomas tvarkomos elektroninės informacijos, esančios Fondo administravimo įstaigų informacinėje duomenų bazėje, ir duomenų centrų tinklo infrastruktūros apsaugai ir administratorių kompiuterizuotoms darbo vietoms.
   2. Vidutinis saugumo lygis taikomas Fondo administravimo įstaigų lokalios aktyvinės tinkloįrangos apsaugai.
   3. Žemas saugumo lygis taikomas Fondo administravimo įstaigų atskiruose kompiuterizuotose darbo vietose sukauptų duomenų/informacijos apsaugai.
6. Fondo administravimo įstaigų patalpos skirstomos į zonas:
   1. Ypatingo saugumo zona – tai duomenų centrų patalpos;
   2. Padidinto saugumo zona – tai patalpos, kuriose yra tarnybinės stotys, kompiuterinio tinklo, komutacinė įranga;
   3. Vidutinio saugumo zona - tai patalpos, kuriose dirba Fondo valdybos IS administratoriai;
   4. Kitos patalpos.

### II SKYRIUS

### TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

1. Bendrieji Fondo valdybos IS elektroninės informacijos techniniai saugos reikalavimai:
   1. Fondo valdybos IS elektronines paslaugas teikiančių taikomųjų sistemųįvykių žurnaluose (angl. *Event log*) registruojami duomenys apie Fondo valdybos IS elektronines paslaugas teikiančių taikomųjų sistemų tarnybinių stočiųįjungimą, išjungimą, Fondo valdybos IS elektronines paslaugas teikiančių taikomosiose sistemose registruotų IS naudotojų ar paslaugos gavėjo sėkmingus ir nesėkmingus bandymus registruotis, jų vykdomus veiksmus, nurodant IS naudotojo ar paslaugos gavėjo identifikatorių, atlikto veiksmo laiką ir kitus elektroninės informacijos saugai svarbius įvykius. Įvykių žurnalai saugomi 1 (vienerius) metus atskiroje tarnybinėje stotyje. Elektroninių paslaugų įvykių žurnalų duomenys analizuojami įvykus elektroninės informacijos saugos incidentui.
   2. Fondo valdybos IS priežiūra vykdoma naudojant unikalią administratoriaus sisteminę paskyrą. Naudojantis šia paskyra kitų Fondo valdybos IS naudotojų funkcijų atlikti negalima.
   3. Fondo valdybos IS naudotojai autentifikuojami kompiuteriniame tinkle. Kiekvienas naudotojas IS unikaliai atpažįstamas – IS naudotojas turi patvirtinti savo tapatybę slaptažodžiu. Fondo valdybos IS asmens kodas nenaudojamas kaip IS naudotojo identifikatorius. IS naudotojams nesuteikiamos administratoriaus teisės.
   4. Elektroninės paslaugos gavėjai gali būti autentifikuojami elektroninės bankininkystės arba elektroninio parašo pagalba arba telefonu per skambučių informacinį centrą (SIC).
   5. Nuotolinis (ne iš Fondo administravimo įstaigos patalpų) prisijungimas darbuotojams prie Fondo valdybos IS yra draudžiamas, išskyrus atvejus, kai prie tarnybinio elektroninio pašto jungiamasi nuotoliniu būdu ir kai leidimas nuotolinei prieigai prie Fondo valdybos IS darbuotojui suteiktas Fondo valdybos direktoriaus patvirtintame Valstybinio socialinio draudimo fondo administravimo įstaigų valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartį, nuotolinio darbo tvarkos apraše nustatyta tvarka.
   6. Slaptažodžio sudarymo reikalavimai, ekrano užsklandos įsijungimo sąlygos ir kiti saugumo parametrai nustatyti Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos Aktyvių katalogų (Active Directory) sistemos saugumo nuostatuose.
   7. Popieriniai dokumentai ar jų kopijos darbo vietoje turi būti padedami į pašaliniams asmenims neprieinamą vietą.
   8. IS naudotojui neatliekant jokių veiksmų Fondo valdybos IS taikomojoje programinėje įrangoje ne ilgiau 15 min., taikomoji programinė įranga užsirakina. Tęsiant darbą taikomojoje programinėje įrangoje, IS naudotojai savo tapatybę pakartotinai patvirtina slaptažodžiu.
   9. Fondo valdybos IS taikomųjų sistemų neveikimo laikas yra nustatytas kiekvienos Fondo valdybos taikomosios sistemos kritiškumo apraše, vadovaujantis Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinių technologijų sistemų kritiškumo vertinimo tvarkos aprašu, patvirtintu Fondo valdybos direktoriaus 2007 m. rugpjūčio 10 d. įsakymu Nr. V-359 „Dėl Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinių technologijų sistemų kritiškumo klasifikavimo tvarkos aprašo patvirtinimo“ (Fondo valdybos direktoriaus 2008 m. spalio 30 d. įsakymu Nr. V-521 redakcija).
   10. IS naudotojai negali naudotis sistemos ištekliais prieštaraujančiais įstatymams tikslais.
   11. Fondo valdybos IS taikomojoje programinėje įrangoje yra įdiegtos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemonės (filtrai).
   12. Naudojamos specializuotos taikomosios sistemos, perspėjančios administratorius, kai techninėje įrangoje iki nustatytos ribos sumažėja laisvos atminties ar vietos diske, ilgą laiką apkraunama kompiuterių tinklo sąsaja, IS naudotojo darbą imituojančios procedūros vyksta per lėtai ir pan.
   13. Fondo administravimo įstaigų darbuotojų kompiuterizuotose darbo vietose naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (USB, CD/DVD). Šios laikmenos negali būti naudojamos veikloms, nesusijusioms su darbo funkcijomis.
   14. Išorinės duomenų laikmenos, iš kurių elektroninė informacija yra perkeliama į Fondo valdybos IS, turi būti patikrinamos antivirusine programa;
   15. Programinė įranga naudojama/paleidžiama iš išorinių duomenų laikmenų yra draudžiama.
   16. Tarnybinės stotys sinchronizuojamos su Active Directory laiko tarnyba, o Active Directory – su išorine laiko tarnyba.
   17. Fondo valdybos IS yra įdiegta centralizuota įsibrovimo susekimo sistema (angl. *Instrusion Detection System*).
   18. Elektroninė informacija, kurią IS naudotojai sukuria Fondo valdybos IS, yra Fondo valdybos nuosavybė.
   19. Įgalioti asmenys, užtikrinantys saugumą ar atliekantys techninę tinklo priežiūrą / administravimą Fondo valdyboje, bet kuriuo metu gali stebėti ar patikrinti įrangą, sistemas ir tinklu siunčiamą informaciją.
   20. Kompiuterinėse darbo vietose ir tinkluose draudžiama:
       1. Fondo valdybos kompiuterinių išteklius naudoti veiklai, kuri yra neteisėta pagal Lietuvos, Europos Sąjungos ar tarptautinę teisę;
       2. įdiegti į tinklą ar tarnybines stotis kenkėjiškas programas (pvz., virusai, „kirminai“, „Trojos arkliai“, elektroninio pašto laiškai – „bombos“ ir kt.), kurios padeda neteisėtai prisijungti prie IS, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jų veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę ja naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims.
       3. platinti nepageidaujamus laiškus, klaidinančią ar žeidžiančią informaciją;
       4. naudoti informaciją, kai ji nėra skirta ją naudojančiam asmeniui;
       5. įsiregistruoti tarnybinėje stotyje / tinkle, naudojantis IS naudotojo vardu ir slaptažodžiu, kuriais IS naudotojas nėra įgaliotas naudotis.
       6. iš anksto nesuderinus su Saugos įgaliotiniu skenuoti prievadus ar saugumo sistemas;
       7. bet kokia forma vykdyti tinklo stebėjimą, kurio metu perimama elektroninė informacija, neturinti atsidurti stebėjimą atliekančio IS naudotojo kompiuteryje;
       8. nesilaikyti bet kurios tarnybinės stoties, tinklo ar paskyros IS naudotojo tapatybės nustatymo ar saugumo procedūrų;
       9. paleisti bet kurią programą, programinį kodą/ komandą ar siųsti bet kurios rūšies žinutes, siekiant sutrukdyti ar nutraukti IS naudotojo, bet kuriomis priemonėmis užmegztą vietos ryšį ar ryšį internetu, vietiniu arba išoriniu tinklu;
   21. IS naudotojai privalo saugoti ir neatskleisti kitiems asmenims jiems suteiktų slaptažodžių ir neleisti pasinaudoti savo, kaip sistemos IS naudotojo, vardu.
   22. IS naudotojams draudžiama skolinti tiek įprastinius (durų, seifų ir pan.), tiek elektroninius (elektroninės įėjimo/išėjimo kortelės ir pan.) raktus.
   23. Bendri (mainų) prieigos katalogai nenaudojami kompiuterizuotose darbo vietose, o reikalui esant suteikiama autorizuota prieiga.
2. Kompiuterinės įrangos saugos priemonės:
   1. taikomųjų programų veikimui naudojama ne mažiau kaip dviejų taikomųjų sistemų tarnybinių stočių sistema, automatiškai paskirstanti IS naudotojų jungimąsi prie vienos ar kitos tarnybinės stoties. Duomenims saugoti naudojamos duomenų saugyklos.
   2. Pagrindinės tarnybinės stotys, svarbiausi duomenų perdavimo tinklo mazgai ir ryšio linijos yra dubliuojami ir jų būklė nuolat stebima;
   3. Duomenų centrų kompiuterinės įrangos gedimus registruoja atsakingi darbuotojai priežiūros paslaugų tiekėjų  pagalbos tarnybose pagal atitinkamą sutartį;
   4. Duomenų centrų įrangos techninių gedimų registravimui naudojamos įrangos gamintojų patvirtintos priemonės, siunčiančios pranešimus tiesiogiai įrangos gamintojui.
3. Sisteminės ir taikomosios programinės įrangos saugos priemonės:
   1. Fondo valdybos atskirose tarnybinėse stotyse ir Fondo administravimo įstaigų kompiuterizuotose darbo vietose veikia centralizuotai įdiegta ir nuolat atnaujinama antivirusinė ir ugniasienės programinė įranga. Šios priemonės yra nuolat stebimos ir jos informuoja apie pradelstą atsinaujinimo laiką.
   2. Operacinei sistemai ir kitai sisteminei programinei įrangai atnaujinti naudojama centralizuota programinė įranga (pavyzdžiui, MS WSUS (*angl. Windows Server Update Services*) ir pan.). Diegiami tik kritiniai (*angl. Critical*) ir saugos (*angl. Security*), ir tik gamintojų rekomenduojami atnaujinimai:
      1. visose tarnybinėse stotyse saugumo atnaujinimai įdiegiami operatyviai po to, kai gamintojas šiuos atnaujinimus patalpina savo internetiniame portale, o kiti atnaujinimai diegiami esant poreikiui.
      2. kompiuterizuotų darbo vietų operacinių sistemų atnaujinimai diegiami centralizuotai nuolat.
   3. Programinės įrangos valdymui naudojama programinė įranga SCCM (*angl. System Center Configuration Manager*):
      1. Fondo valdybos tarnybinėse stotyse naudojama tik legali, patikimų gamintojų programinė įranga:
         1. diegiama ir naudojama tik iš oficialių gamintojų ar jų įgaliotų atstovų gauta programinė įranga;
         2. programinė įranga prižiūrima laikantis gamintojo rekomendacijų;
         3. programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka tik administratoriai ir / arba pagal sutartis tiekėjo kvalifikuoti specialistai;
         4. programinės įrangos testavimas atliekamas naudojant atskirą testavimo aplinką.
      2. Fondo administravimo įstaigų darbuotojų kompiuterizuotose darbo vietose:
         1. IS naudotojams draudžiama diegti programinę įrangą;
         2. naudojama tik legali ir darbo funkcijoms reikalinga programinė įranga:
         3. programinė įranga, nesusijusi su Fondo valdybos veikla ir IS naudotojų funkcijomis, yra draudžiama.
   4. Leistinos programinės įrangos sąrašą, patvirtintą Fondo valdybos direktoriaus, ne rečiau kaip kartą per metus Saugos įgaliotinis peržiūri ir jei reikalinga atnaujina. Leistinos programinės įrangos sąrašas skelbiamas Fondo valdybos intranete, skiltyje „Veikla/ Palaikanti veikla/ Informacijos saugumas“.
   5. Atsiradus naujos darbo funkcijoms reikalingos programinės įrangos poreikiui, IS naudotojo tiesioginis vadovas kreipiasi į Saugos įgaliotinį, kuris įvertina programinės įrangos reikalingumą ir vykdo 9.4 punktą.
4. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:
   1. Fondo valdybos elektroninės informacijos perdavimo tinklas yra atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę. Ugniasienių įvykių žurnalai (*angl. Logs*) analizuojami esant poreikiui. Ugniasienių saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos.
   2. Fondo valdybos duomenų centrui taikomas trijų lygių tinklo saugumas: išorė/aplikacijos/duomenų bazės, kiekvieną iš lygių atskiriant ugniasienėmis (*angl. Firewall*).
   3. Fondo valdybos IS elektroninės informacijos perdavimo tinklas yra segmentuotas pagal IS sudedamųjų dalių atliekamas funkcijas ir turi priskirtus IP adresų intervalus:
      1. tarnybinių stočių tinklas, skirtas taikomųjų programų tarnybinėms stotims;
      2. IS naudotojų kompiuterizuotų darbo vietų tinklai, skirti nutolusių vidinių IS naudotojų kompiuterinėms darbo vietoms ir lokaliai kompiuterinei įrangai;
      3. IS kūrimo ir testavimo tinklas, skirtas kūrimo ir testavimo darbams naudojamoms tarnybinėms stotims;
      4. administratorių tinklas, skirtas darbuotojų, turinčių informacinės sistemos ir (ar) tarnybinių stočių administratoriaus teises;
      5. elektroninės informacijos perdavimo tinklo aptarnavimo ir saugumo potinklis, skirtas tinklo stebėjimo, aptarnavimo, antivirusinių sistemų tarnybinėms stotims;
      6. demilitarizuotos zonos tinklas, skirtas tarnybinėms stotims, kurios turi ryšį su viešaisiais telekomunikacijų tinklais.
   4. Internete ar kitame tinkle esanti informacija ar resursai, taip pat informacija ir resursai Fondo valdybos kompiuteriniame tinkle iš Internet ar kitų tinklų, pasiekiama tik per Fondo valdybos lokaliame tinkle esančius „vartus“, kurie yra kontroliuojami.
   5. Vadovaujantis Asmens duomenų teikimo automatiniu būdu pagal sutartis tvarkos apraše, patvirtintame Fondo valdybos direktoriaus 2010 m. lapkričio 19 d. įsakymu Nr. V-495 „Dėl Asmens duomenų teikimo automatiniu būdu pagal sutartis tvarkos aprašo patvirtinimo“, Fondo valdybos IS gavėjams pagal Fondo valdybos ir duomenų gavėjo sudarytą duomenų teikimo sutartį, duomenys teikiami elektroniniu būdu saugiais šifruotais duomenų perdavimo kanalais, jungiančiais konkretų informacinės sistemos duomenų gavėją bei Fondo valdybos informacinės sistemos tarnybines stotis.
5. Patalpų ir aplinkos saugumo užtikrinimo priemonės (įėjimo kontrolė, elektros tiekimas, aplinkos drėgnumas, darbo vietos temperatūra, priešgaisrinė sauga, vaizdo kameros):
   1. Už elektros tiekimą, tinkamus elektros parametrus, elektros tinklo įžeminimą, aplinkos drėgnumą, darbo vietos temperatūrą atsako nekilnojamo turto valdytojas Valstybės įmonė „Turto bankas“ (toliau – TB)
   2. Fondo administravimo įstaigų patalpose įėjimo kontrolės, priešgaisrinė saugos, vaizdo kamerų reikalavimus nustato Fondo valdybos Viešųjų pirkimų ir ūkio valdymo skyrius, o šių reikalavimų įgyvendinimą vykdo TB pagal sudarytą paslaugų sutartį.
   3. Patalpų ir aplinkos saugumo užtikrinimo priemonių priežiūrą ir remontą vykdo TB.
   4. Viešųjų pirkimų ir ūkio valdymo skyriaus atsakingi specialistai vykdo TB paslaugų monitoringą ir dalyvauja su TB profilaktiniuose patikrinimuose bei informuoja TB apie priemonių trūkumus bei gedimus.
   5. Patekti į Fondo administravimo įstaigų padidinto ar ypatingo saugumo zonas galima tik iš anksto (ne vėliau kaip prieš 1 d. d.) suderinus su Fondo valdybos Informacinės sistemos eksploatavimo skyriaus (toliau – ISES) atsakingu darbuotoju.
   6. Ypatingo saugumo zonai taikomi reikalavimai:
      1. Fondo valdybos duomenų centrų patalpos:
         1. Tarnybinės stotys, aktyvinė tinklo įranga (angl. core switch, ugniasienės, šifratoriai ir pan.) ir duomenų saugyklos laikomos tik duomenų centrams pritaikytose patalpose, kuriose:
            1. įrengta elektroninė perimetro kontrolės sistema;
            2. įrengtos vaizdo stebėjimo sistemos, pagrįstos skaitmeninio įrašo sistema;
            3. įrengta kondicionavimo sistema;
            4. įrengta atskirų patalpų apsaugos signalizacija. Visose patalpose įrengti įsilaužimo davikliai prijungti prie pastato signalizacijos ir apsaugos tarnybų;
            5. įrengta gaisro automatinė gesinimo dujomis sistema;
            6. ribojama fizinė prieiga prie tinklo kabelių, skirstytuvų, atšakų, kartotuvų ir antgalių;
            7. kompiuterių ryšio linijos apsaugotos nuo elektros linijų avarijų naudojant apsauginius įtaisus su įžeminimo tašku;
         2. Visa duomenų centre esanti įranga pajungiama per vieningą nepertraukiamo maitinimo šaltinį (UPS). Elektros maitinimas tiekiamas iš dviejų nepriklausomų elektros šaltinių ir įrengiamas vietinis elektros generatorius;
         3. Elektros generatorius automatiškai įsijungia po 15 - 20 sekundžių dingus elektros įtampai, o sistema automatiškai informuoja atsakingus darbuotojus apie gedimą sms žinute. Elektros generatorius vieną kartą per mėnesį tikrinamas imituojant elektros energijos dingimą;
         4. Nuolat matuojamas ir nuolat stebimas aplinkos drėgnumas automatizuotos sistemos. Rodmenims padidėjus arba sumažėjus daugiau nei technikos gamintojo nurodytos leistinos normos, sistema automatiškai informuoja atsakingus darbuotojus apie nuokrypius sms žinute;
         5. Automatinė gaisro gesinimo dujomis sistema tikrinama kartą per metus pagal sudarytą sutartį.
         6. Į duomenų centrų patalpas gali patekti tik Fondo valdybos direktoriaus įsakyme nurodyti darbuotojai. Bet kokie darbai atliekami tik dalyvaujant darbuotojui, turinčiam leidimą patekti į duomenų centrų patalpas;
         7. Duomenų centro patalpos raktai saugomi apsaugos darbuotojo poste arba pas Fondo valdybos direktoriaus įsakyme nurodytą atsakingą asmenį/is. Atsarginiai duomenų centro patalpų raktai saugomi kitame pastate nei pagrindiniai raktai.
      2. Reikalavimai Fondo administravimo įstaigų vietiniams kompiuterių tinklams:
         1. lokali aktyvinė tinklo įranga ir komutacinės spintos yra atskiroje patalpoje, kuri priskiriama padidinto saugumo zonai.
         2. centralizuotai valdomi atsižvelgiant į tarptautinių standartų reikalavimus;
         3. naudojami valdomi aktyviniai tinklo elementai, kurių būklė pastoviai centralizuotai stebima;
         4. tinklo sieniniai lizdai yra sunumeruoti;
         5. palaikoma tinklo jungčių aktuali detali dokumentacija, kurioje yra pateikiamas lizdų išdėstymo planas;
         6. įdiegtas 802.1x tinklo saugos protokolas.
   7. Padidinto saugumo zonai taikomi reikalavimai:
      1. Į Fondo administravimo įstaigų padidinto saugumo zonas gali patekti ir už šių patalpų raktų saugojimą atsakingas yra:
         1. ISES atsakingas darbuotojas, kai patalpos yra pastate, kuriame yra ir jo pastovi darbo vieta;
         2. Fondo valdybos Viešųjų pirkimų ir ūkio valdymo atsakingas darbuotojas, gavęs el. paštu sutikimą iš ISES atsakingo darbuotojo, kai patalpos yra pastate, kuriame yra ir jo pastovi darbo vieta ir tame pastate nėra dirbančio ISES darbuotojo;
         3. Teritorinio skyriaus direktoriaus įsakymu paskirtas to teritorinio skyriaus darbuotojas, gavęs el. paštu sutikimą iš ISES atsakingo darbuotojo, kai  tame pastate nėra fiziškai dirbančio nei ISES, nei Viešųjų pirkimų ir ūkio valdymo skyriaus darbuotojo.
      2. Fondo administravimo įstaigų padidinto saugumo zonos patalpose yra:
         1. Įrengta kondicionavimo sistema;
         2. Visa aktyvinė tinklo įranga pajungiama per nepertraukiamo maitinimo šaltinį (UPS);
         3. Temperatūra stebima nuotoliniu būdu;
         4. Atjungtos nenaudojamos tinklo jungtys;
         5. Fizinė prieiga prie tinklo kabelių, skirstytuvų, atšakų, kartotuvų ir antgalių yra ribojama užrakinant;
         6. Įrengta patalpų apsaugos ir priešgaisrinė sistema;
         7. Naudojami valdomi aktyviniai tinklo elementai, kurių būklė pastoviai centralizuotai stebima;
      3. Ne darbo metu patalpose įjungiama apsaugos sistema;
      4. Patalpos rakinamos. Pastato /patalpos apsaugos sistemos monitoringą vykdo paslaugos tiekėjas.
   8. Vidutinio saugumo zonai taikomi reikalavimai:
      1. Fondo valdybos patalpose, esančios administratorių patalpos:
         1. Įrengta elektroninė įėjimo kontrolės sistema.
         2. Kiekvienas administratorius turi asmeninę elektroninę praėjimo kortelę ir įeidamas arba išeidamas pasižymi įėjimo/išėjimo skaitytuvuose.
   9. Kitų patalpų zonai taikomi reikalavimai:
      1. Fondo valdybos patalpose, išskyrus, administratorių patalpas:
         1. Įrengta elektroninė įėjimo iš lauko kontrolės sistema.
         2. Kiekvienas darbuotojas turi asmeninę elektroninę praėjimo kortelę ir įeidamas arba išeidamas pasižymi įėjimo/išėjimo skaitytuvuose.
         3. Visi darbuotojų įėjimai ir išėjimai į patalpas fiksuojami ir laikomi elektronine forma.
         4. Pagal sutartis paslaugas atliekantiems rangovams išduodamos elektroninės praėjimo kortelės, kurios privalo būti pažymimos tiek įeinant, tiek ir išeinant iš Fondo valdybos patalpų. Kitu atveju, tai yra neturint elektroninės praėjimo kortelės, apie savo atvykimą ir išvykimą rangovai pasirašo asmenų registracijos žurnale. Lankytojams ir/ar svečiams nėra išduodamos elektroninės praėjimo kortelės. Už lankytojų ir/ar svečių apsilankymą atsakingas Viešųjų pirkimų ir ūkio valdymo skyriaus darbuotojas (budėtojas) pasirašo įėjimo punkto lankytojų registracijos žurnale už kiekvieną lankytoją ir/ar svečią, fiksuojant jo atvykimo, išvykimo laiką ir atvykimo tikslą.
         5. Įrengtos vaizdo stebėjimo sistemos, pagrįstos skaitmeninio įrašo sistema.
         6. Įrengta patalpų apsaugos ir priešgaisrinė sistema.
         7. Po darbo patalpose įjungiama apsaugos sistema ir patalpos rakinamos. Pastato apsaugos sistemos monitoringą vykdo paslaugos tiekėjas.
      2. Fondo valdybos teritorinių skyrių patalpose:
         1. Įrengtos vaizdo stebėjimo sistemos, pagrįstos skaitmeninio įrašo sistema.
         2. Įrengta patalpų apsaugos ir priešgaisrinė sistema.
         3. Po darbo patalpose įjungiama apsaugos sistema ir patalpos rakinamos. Pastato apsaugos sistemos monitoringą vykdo paslaugos tiekėjas.
      3. Fondo administravimo įstaigų, kompiuterizuotoms darbo vietoms:
         1. TB užtikrina nuo +15◦C iki +35◦C (temperatūrų kitimas ne didesnis kaip 15◦C per val.) temperatūrinis režimas;
         2. nėra uždengtos ventiliacinės angos;
         3. TB užtikrina drėgnumą nuo 15% iki 80%, nevyksta kondensacija;
         4. vibracija neviršija 0,5g smūgių nuo 5Hz iki 200Hz dažnumu;
         5. TB užtikrina vienfazį, kintamos (50Hz) srovės 230V nominalios įtampos šaltinį;
         6. elektros maitinimas yra atskiras nuo buitinio elektros tinklo;
         7. visiems kompiuteriams įjungtas BIOS sąrankos slaptažodis, kuris prilyginamas administratoriaus slaptažodžiui ir žinomas tik atsakingiems asmenims.
         8. kompiuterizuotų darbo vietų operacinės sistemos registrai užrakinami.

### III SKYRIUS

### SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

1. Elektroninės informacijos įvedimo, keitimo, atnaujinimo ir naikinimo tvarka:
   1. Įvesti, keisti ir atnaujinti Fondo valdybos IS ir Registrų elektroninę informaciją gali tik autorizuoti IS naudotojai ir elektroninių paslaugų gavėjai;
   2. IS naudotojai ir elektroninių paslaugų gavėjai atlieka Fondo valdybos IS ir Registrų elektroninės informacijos tvarkymo veiksmus priklausomai nuo jiems suteiktų prieigos teisių;
   3. Elektroninė informacija gali būti įvesta, pakeista, atnaujinta Fondo valdybos IS ir Registruose tik teisėtu pagrindu;
   4. Fondo administravimo įstaigų informacinėje duomenų bazėje elektroninės informacijos keitimą ne per taikomąsias sistemas atlieka tik tie Fondo valdybos IS naudotojai, kurie yra nurodyti Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos specialistų, turinčių teisę koreguoti duomenis informacinėje duomenų bazėje, sąraše, patvirtintame Fondo valdybos direktoriaus įsakymu;
   5. Fondo valdybos IS ir Registrai turi įvestos elektroninės informacijos tikslumo, užbaigtumo ir tikrinimo priemones.
2. IS naudotojų ir elektroninių paslaugų gavėjų veiksmų registravimo tvarka:
   1. IS naudotojas ir elektroninių paslaugų gavėjas atlieka tik tuos duomenų tvarkymo veiksmus, prie kurių yra suteiktos prieigos teisės;
   2. IS naudotojų ir elektroninių paslaugų gavėjų elektroninės informacijos tvarkymo veiksmai Fondo valdybos IS registruojami, nurodant prisijungimo identifikatorių, datą, laiką, trukmę.
3. Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka reglamentuota Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos kopijavimo tvarkos apraše.
4. Duomenys gaunami ir teikiami išorės informacinėms sistemoms ir registrams, vadovaujantis Bendruoju duomenų apsaugos reglamentu (BDAR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu bei asmens duomenų teikimo sutartimis, numatant teikimo būdus, apimtis, reguliarumą, terminus bei kitus saugos reikalavimus.
5. Siekiant išvengti elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo:
   1. Draudžiama kopijuoti, keisti, naikinti ar perduoti Fondo valdybos IS elektroninę informaciją asmeniniais tikslais ar kitais tikslais nesusijusioms su tiesioginėmis pareigų funkcijomis;
   2. Visi viešai neskelbtini/ konfidencialūs dokumentai bei dokumentai, kuriuose yra asmens duomenys, tapę nebereikalingi, turi būti sunaikinti. Jokie popieriniai dokumentai ar jų projektai, kurie nėra skirti viešam naudojimui, negali būti išmesti nesusmulkinti;
   3. IS naudotojai, pastebėję saugos dokumentų reikalavimų pažeidimus nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones, privalo nedelsdami pranešti administratoriui;
   4. Administratorius apie saugos pažeidimus informuoja Saugos įgaliotinį ir imasi visų įmanomų prevencinių veiksmų saugos pažeidimo užkardymui.
6. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarką reglamentuoja Informacinių technologijų keitimų valdymo tvarkos aprašas.
7. Taikomosios programinės įrangos keitimų diegimai atliekami:
   1. Planiniai – pagal Fondo valdybos direktoriaus pavaduotojo, kuruojančio IT sritį, patvirtintą Fondo valdybos informacinės sistemos taikomųjų sistemų programinės įrangos keitimų diegimo grafiką (priedas – grafiko forma);
   2. Neplaniniai – pagal poreikį, suderinus su Fondo valdybos Informacinės sistemos plėtros skyriaus vedėju bei ISES atsakingais už taikomosios programinės įrangos keitimų diegimą asmenimis. Apie neplaninius taikomosios programinės įrangos keitimų diegimus IS naudotojų tikslinę grupę informuoja Fondo valdybos informacinės sistemos Paslaugų valdymo sistemos Paslaugų tarnyba.
8. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarką reglamentuoja Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos mobilių įrenginių naudojimo tvarkos aprašas.

### IV SKYRIUS

### REIKALAVIMAI, KELIAMI INFORMACINIŲ SISTEMŲ FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TIEKĖJAMS

1. Reikalavimai, keliami patalpoms, įrangai, informacinių sistemų priežiūrai, duomenų perdavimui tinklais bei paslaugų teikėjų prieigos prie informacinės sistemos lygiai ir sąlygos nurodyti Rangovų prieigos prie Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugo ir darbo ministerijos informacinės sistemos tvarkos apraše.
2. Tiekėjas turi laikytis organizacinių ir techninių kibernetinio saugumo reikalavimų, nustatytų Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.
3. Tiekėjas, teikdamas paslaugas, privalo laikytis pateiktų jam susipažinti dokumentų, susijusių su Fondo valdybos IS sauga, reikalavimų.

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

# Valstybinio socialinio draudimo fondo valdybos prie

# Socialinės apsaugos ir darbo ministerijos informacinės

# sistemos saugaus elektroninės informacijos tvarkymo

# taisyklių

# priedas

**Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos**

TVIRTINU

(Pareigos)

(parašas)

(Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos taikomųjų sistemų programinės įrangos keitimų diegimo grafiko forma)

**VALSTYBINIO SOCIALINIO DRAUDIMO FONDO VALDYBOS PRIE SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS INFORMACINĖS SISTEMOS TAIKOMŲJŲ SISTEMŲ PROGRAMINĖS ĮRANGOS KEITIMŲ PLANINIO DIEGIMO GRAFIKAS**

202 - - Nr.

Vilnius

| **Eil. Nr.** | **Taikomosios sistemos pavadinimas** | **Savaitės dienos** | | | | | | | | | | | | **Periodiškumas (kartų per savaitę/mėnesį)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **I** | | **II** | | **III** | | **IV** | | **V** | | **VI** | **VII** |
| 7:00 - 8:00 | 18:00 –  19:00 | 7:00 – 8:00 | 18:00 –  19:00 | 7:00 – 8:00 | 18:00 –  19:00 | 7:00 – 8:00 | 18:00 –  19:00 | 7:00 – 8:00 | 18:00 –  19:00 | 7:00 –  19:00 | 7:00 –  19:00 |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
| 1. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

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