VALSTYBINIO SOCIALINIO DRAUDIMO FONDO VALDYBOS PRIE SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS DIREKTORIUS

ĮSAKYMAS DĖL 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 KIBERNETINIO SAUGUMO POLITIKOS PATVIRTINIMO

2024 m. birželio 21 d. Nr. V-205
Vilnius

1. T v i r t i n u 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 kibernetinio saugumo politiką (pridedama).

2. P r i p a ž į s t u netekusiu galios 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 kibernetinio saugumo politiką, patvirtintą Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos direktoriaus 2017 m. liepos 17 d. įsakymu Nr. V-349 „Dėl Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos kibernetinės saugumo politikos patvirtinimo“.

3. Į p a r e i g o j u:

3.1. Fondo valdybos Informacinės sistemos eksploatavimo skyrių šį įsakymą paskelbti Valstybinio socialinio draudimo fondo administravimo įstaigų intraneto svetainėje;

3.2. Fondo valdybos Dokumentų tvarkymo skyrių:

3.2.1. šį įsakymą išsiųsti Fondo valdybos direktoriaus pavaduotojams, Fondo valdybos administracijos padaliniams ir Valstybinio socialinio draudimo fondo valdybos teritoriniams skyriams;

3.2.2. Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos darbo reglamento (toliau – Reglamentas), patvirtinto Fondo valdybos direktoriaus 2013 m. liepos 12 d. įsakymu Nr. V-352 „Dėl Valstybinio socialinio draudimo fondo valdybos prie

Socialinės apsaugos ir darbo ministerijos darbo reglamento patvirtinimo“, nustatyta tvarka su šiuo įsakymu Dokumentų valdymo sistemos (toliau – DVS) priemonėmis pasirašytinai supažindinti visus Fondo valdybos darbuotojus – DVS naudotojus ir Valstybinio socialinio draudimo fondo valdybos teritorinių skyrių direktorius;

3.3. Fondo valdybos Personalo valdymo skyrių Reglamento nustatyta tvarka su šiuo įsakymu pasirašytinai supažindinti po šio įsakymo įsigaliojimo priimtus naujus Fondo valdybos darbuotojus ir Valstybinio socialinio draudimo fondo valdybos teritorinių skyrių direktorius.

3.4. Valstybinio socialinio draudimo fondo valdybos teritorinių skyrių direktorius užtikrinti jų vadovaujamos įstaigos darbuotojų – Informacinės sistemos naudotojų pasirašytiną supažindinimą su šiuo įsakymu.

Direktorius Kęstutis Čereška

SUDERINTA
Nacionalinis kibernetinis saugumo centras
prie Krašto apsaugos ministerijos
2024-05-10 raštu Nr. (4.1E) 6K-365

PATVIRTINTA
Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos direktoriaus
2024 m. d.
įsakymu Nr. V-

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 KIBERNETINIO SAUGUMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos (toliau – Fondo valdyba) informacinės sistemos (toliau – IS) Kibernetinio saugumo politika (toliau – Politika) 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 informacinės sistemos (toliau – IS), 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 (toliau abu kartu – Registrai) Fondo valdybos kibernetinio saugumo politiką ir jos įgyvendinimą.

2. Politikos valdymas apima organizacinius ir techninius kibernetinio saugumo reikalavimus, tai yra reikalavimus atpažinties, tapatumo patvirtinimo ir naudojimosi Fondo valdybos IS saugumą ir kontrolę, Fondo valdybos IS naudotojų ir administratorių atliekamų veiksmų auditą ir kontrolę, įsibrovimo aptikimą ir prevenciją, belaidžio tinklo saugumą ir kontrolę, mobiliųjų įrenginių, naudojamų prisijungti prie Fondo valdybos IS, saugumą ir kontrolę, Fondo valdybos svetainės, kuri pasiekiama iš viešųjų elektroninių ryšių tinklų, saugumą ir kontrolę bei Fondo valdybos IS naudojamo interneto saugumą ir kontrolę.

3. Politikoje išdėstyti reikalavimai yra taikoma visiems Fondo valdybos IS naudotojams ir Rangovams.

4. Šioje Politikoje vartojamos sąvokos:

4.1. **Administratorius** – Fondo valdybos darbuotojas, atliekantis duomenų bazių, tarnybinių stočių, tinklo ar kitos kompiuterinės įrangos priežiūrą, užtikrinantis veikimą ir elektroninės informacijos saugą.

4.2. **Darbuotojas** – Fondo administravimo įstaigos valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį.

4.3. **Elektroninė informacija –** Fondo valdybos IS tvarkomi duomenys, dokumentai ir informacija.

4.4. **Fondo administravimo įstaigos** – Fondo valdyba, Valstybinio socialinio draudimo fondo valdybos teritoriniai skyriai.

4.5. **IS naudotojas** – darbuotojas, kuriam suteikta teisė naudotis IS.

4.6. **Fondo valdybos IS** – IS ir Registrai.

4.7. **Kibernetinis saugumas** – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei Fondo valdybos IS veiklai, įvykus šiems incidentams, atkurti.

4.8. **Asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą** - Fondo valdybos direktoriaus įsakymu paskirtas Fondo valdybos darbuotojas, organizuojantis ir užtikrinantis kibernetinio saugumą Fondo valdybos IS.

4.9. **Rangovas** – juridinis ar fizinis asmuo darbų arba paslaugų teikimo sutarties pagrindu teikiantis Fondo valdybos IS posistemių/IT sistemų kūrimo, diegimo, priežiūros, vystymo bei kitas paslaugas.

4.10. **Saugos dokumentai** – Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir saugos dokumentų turinio gairių aprašo patvirtinimo“, numatyti Saugos dokumentai, kurie suderinti su Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos (toliau – NKSC) ir patvirtinti Fondo valdybos direktoriaus įsakymu:

4.10.1. 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 duomenų saugos nuostatai, patvirtinti Fondo valdybos direktoriaus 2018 m. vasario 5 d. įsakymu Nr. V-58 „Dėl Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (2021 m. balandžio 19 d. įsakymo Nr. V-267 redakcija);

4.10.2. Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos naudotojų prieigos teisių administravimo taisyklės, patvirtintos Fondo valdybos direktoriaus 2015 m. rugsėjo 4 d. įsakymu Nr. V-448 „Dėl Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos naudotojų prieigos teisių administravimo taisyklių patvirtinimo“ (toliau – Taisyklės);

4.10.3. 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 veiklos tęstinumo valdymo planas, patvirtintas Fondo valdybos direktoriaus 2015 m. gegužės 25 d. įsakymu Nr. V-256 „Dėl Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos veiklos tęstinumo valdymo plano patvirtinimo“ (2022 m. liepos 8 d. įsakymo Nr. V-261 redakcija);

4.10.4. 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, patvirtintos Fondo valdybos direktoriaus 2015 m. vasario 11 d. įsakymu Nr. V-81 „Dėl Valstybino socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių patvirtinimo“ (2022 m. gegužės 25 d. įsakymo Nr. V-203 redakcija) (toliau – Tvarkymo taisyklės);

4.10.5. Kitos Politikoje vartojamos sąvokos atitinka Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, apraše bei Kibernetinio saugumo įstatyme apibrėžtas sąvokas.

II SKYRIUS
ORGANIZACINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI

PIRMASIS SKIRSNIS
BENDROSIOS NUOSTATOS

5. Fondo valdybos IS infrastruktūra priskiriama prie ypatingos svarbos informacinės struktūros, vadovaujantis ypatingos svarbos informacinės infrastruktūros identifikavimo metodika, patvirtinta Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos Kibernetinio saugumo įstatymo įgyvendinimo“.

6. Fondo valdybos IS naudotojų pareigos ir funkcijos, susijusios su elektroniniu informacijos (kibernetiniu) saugumu, nurodytos Saugos dokumentuose.

7. Fondo valdyboje yra organizuojami mokymai kibernetinio saugumo klausimais tiek Fondo valdybos IS naudotojams, tiek asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą.

8. Asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, kartą per metus dalyvauja mokymuose kibernetinio saugumo klausimais bei periodiškai inicijuoja IS naudotojų mokymą (ne rečiau kaip kartą per metus) kibernetinės ir/ar elektroninės informacijos saugumo klausimais, informuoja juos apie kibernetinio saugumo reikalavimus ir problematiką vienu iš šių būdų:

8.1. elektroniniu paštu;

8.2. teminiuose seminaruose;

8.3. įvairaus pobūdžio atmintinėse.

9. Fondo valdybos IS grėsmių ir pažeidžiamumų, galinčių turėti įtakos Fondo valdybos IS kibernetiniam saugumui, kartu su atitikties vertinimu teisės aktų reikalavimams vertinimas atliekamas ne rečiau kaip kartą per trejus metus, kurį atlieka nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų saugos ekspertai.

10. Fondo valdybos IS grėsmių ir pažeidžiamumų vertinimas atliekamas pagal pasaulyje viešai žinomą ir pripažintą atvirą arba komercinę įsilaužimų testavimo metodiką (*angl. Penetration Testing Methodology*), naudojant automatizuotą (*angl. Input Validation, XSS, SQL injection ir pan.*) ir rankinį (pagal „OWASP Testing Guide v*“ metodiką) pažeidžiamumų paiešką.

11. Fondo valdybos IS grėsmių ir pažeidžiamumų vertinimo apimtis nustatoma atsižvelgiant į galimai pažeidžiamiausias ir daugiausiai pokyčių atliktas Fondo valdybos IS dalis.

12. Nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų saugos ekspertai, atlikę Fondo valdybos IS infrastruktūros grėsmių ir pažeidžiamumų vertinimą, pateikia pažeidžiamumų vertinimo ataskaitą, nurodant pažeidžiamumo rizikos lygį, rekomendacijas pažeidžiamumams ištaisyti. Vertinimo metu nustatyti pažeidžiamumo rizikos lygiai skirstomi:

12.1. Pažeidžiamumai, turintys kritinį lygį, sprendžiami nedelsiant (nelaukiant pažeidžiamumų vertinimo ataskaitos), kai tik nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų saugos ekspertai aptinka ir informuoja Saugos įgaliotinį.

12.2. Pažeidžiamumai, turintys aukšto pažeidžiamumo lygį (nurodyti pažeidžiamumų vertinimo ataskaitoje), sprendžiami kaip galima greičiau, vertinant / atsižvelgiant į pažeidžiamumo išsprendimo sudėtingumą ir Fondo valdybos IS kompleksiškumą (užsitęsus sprendimui, nurodomi ir toliau valdomi Fondo valdybos IS pažeidžiamumų šalinimo plane.

13. Atsižvelgiant į pažeidžiamumų vertinimo ataskaitą, Saugos įgaliotinis parengia Fondo valdybos IS išorinio saugos audito vertinimo metu rastų pažeidžiamumų šalinimo planą, kuriame nurodoma: rastas pažeidžiamumas, pažeidžiama sistema, pažeidžiamumo galima rizika/ kritiškumas/ grėsmė, rekomendacija pažeidžiamumui ištaisyti, atsakingo asmens už pažeidžiamumo ištaisymą vardas ir pavardė, planuojama ištaisymo data. Asmuo, atsakingas už pažeidžiamumų ištaisymą, koordinuoja pataisų testavimą ir kitų elgsenos su pažeidžiamumais priemonių diegimą.

14. Saugos įgaliotinis kontroliuoja Fondo valdybos IS pažeidžiamumų šalinimo plane numatytų pažeidžiamumų šalinimo terminų laikymąsi, parengdamas Fondo valdybos IS išorinio saugos audito vertinimo metu rastų pažeidžiamumų įgyvendinimo ataskaitą.

15. IS naudotojai, aptikę pažeidžiamumą Fondo valdybos IS, praneša Saugos įgaliotiniui.

16. Ne rečiau kaip kartą per metus atliekamas Fondo valdybos IS organizacinių ir techninių kibernetinio saugumo reikalavimų atitikties vertinimas, kurio ataskaita teikiama į Valstybės

informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemą (ARSIS).

17. Ne rečiau kaip kartą per metus organizuojamas ir atliekamas Fondo valdybos IS rizikos veiksnių analizė. Atlikus rizikos veiksnių analizė yra parengiama ataskaita ir nustatomi rizikos mažinimo saugumo techninės, programinės ir (ar) organizacinės priemonės. Rizikos veiksnių analizės ataskaitoje numatytos saugumo gerinimo priemonės apima elektroninės informacijos ir kibernetinio saugumo būklės gerinimą. Patvirtinta Fondo valdybos IS rizikos veiksnių analizė ne vėliau kaip per 5 darbo dienas nuo atlikto rizikos vertinimo teikiama į ARSIS.

18. Kibernetinio incidento valdymo organizavimas reglamentuotas 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 kibernetinių incidentų valdymo plane.

19. Ne rečiau kaip kartą per mėnesį Fondo valdyboje yra atliekama Fondo valdybos IS naudotojų veiksmų audito įrašų analizė.

20. Ne rečiau kaip kartą per mėnesį Fondo valdyboje yra atliekama saugasienių užfiksuotų įvykių analizė ir pastebėtos neatitiktys saugumo reikalavimams šalinamos.

21. Ne rečiau kaip kartą per mėnesį Fondo valdyboje yra įvertinami kibernetiniam saugumui užtikrinti naudojamų priemonių programiniai atnaujinimai, klaidų taisymai ir šie atnaujinimai diegiami.

22. Fondo valdyba, pirkdama paslaugas, darbus ar įrangą, susijusius su Fondo valdybos IS, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose nustato, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams.

23. Kibernetiniam saugumui užtikrinti naudojamų priemonių diegimo ir šių priemonių parametrų keitimas reglamentuotas Tvarkymo taisyklėse;

24. Fondo valdybos IS kibernetinio saugumo būklės gerinimas vykdomas nuolat atliekant kibernetinio saugumo organizacinių ir techninių reikalavimų atitikimą, įgyvendinimą ir kontrolę. Kibernetinio saugumo organizacinių ir techninių reikalavimai apima Fondo valdybos IS auditinių įrašų administravimą, įsibrovimo aptikimą, grėsmių ir pažeidžiamumų valdymą, incidentų valdymą, reikalavimų įgyvendinimo kontrolės ir atitikties vertinimą, elektroninio pašto naudojimą, atsarginių kopijų darymą ir atkūrimą, santykį su tiekėjais, atpažinties, tapatumo patvirtinimo ir naudojimosi saugumą ir kontrolę, naudotojų ir administratorių atliekamų veiksmų auditą ir kontrolę, įsibrovimų aptikimą ir prevenciją, belaidžio tinklo saugumą ir kontrolę, mobilių įrenginių saugumą ir kontrolę, naudojamos interneto svetainės, pasiekiamų iš viešųjų el. tinklų ryšių saugumą ir kontrolę, naudojimosi internetu saugumą ir kontrolę. Fondo valdybos IS kibernetinio saugumo būklės gerinimas apima ir kibernetinio saugumo užtikrinimą, kibernetinių incidentų valdymą, rizikos ir pažeidžiamumų bei atitikties vertinimą Fondo valdybos IS, naudotojų švietimą bei kontrolę.

25. Fondo valdybos IS atsarginių duomenų kopijų darymas ir atkūrimas atliekamas vadovaujantis Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos kopijavimo tvarkos aprašu, patvirtintu Fondo valdybos direktoriaus 2016-11-15 įsakymu Nr. V-598 „Dėl Valstybinio socialinio draudimo fondo valdybos prie socialinės apsaugos ir darbo ministerijos informacinės sistemos kopijavimo tvarkos aprašo patvirtinimo“.

26. Fondo valdybos IS elektroninės informacijos saugumo ir kibernetinio saugumo užtikrinimas palaikant santykius su tiekėjais, kurie dalyvaus vykdant sutartį, reglamentuotas Rangovų prieigos prie Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos tvarkos apraše, patvirtintame 2012-09-13 Fondo valdybos direktoriaus įsakymu Nr. V-432 "Dėl Rangovų prieigos prie Valstybinio socialinio draudimo fondo valdybos prie socialinės apsaugos ir darbo ministerijos informacinės sistemos tvarkos aprašo patvirtinimo".

27. Fondo valdybos IS Saugos dokumentai ir kiti su sauga susiję dokumentai peržiūrimi (persvarstomi) ne rečiau kaip kartą per metus. Keičiami Saugos dokumentai ir kiti su sauga susiję dokumentai su NKSC gali būti nederinami tais atvejais, kai atliekami tik redakciniai pakeitimai. Tokiais atvejais NKSC pateikiamos šių dokumentų kopijos.

28. Fondo valdyba, rengdama sutartis su tiekėju, įtraukia reikalavimus, susijusius su informacijos saugumo, kibernetinio saugumo užtikrinimu, tokia apimtimi, kiek tai susiję su pirkimo objektu ir prieiga prie Fondo valdybos IS.

ANTRASIS SKIRSNIS
ELEKTRONINIO PAŠTO NAUDOJIMAS

29. Vadovaujamasi Valstybinio socialinio draudimo fondo administravimo įstaigų darbuotojų prieigos ir naudojimosi internetu bei elektroniniu paštu taisyklėmis, patvirtintomis Fondo valdybos direktoriaus 2020 m. liepos 28 d. įsakymu Nr. V-375 „Dėl Valstybinio socialinio draudimo fondo administravimo įstaigų darbuotojų prieigos ir naudojimosi internetu bei elektroniniu paštu taisyklių patvirtinimo".

III SKYRIUS
TECHNINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI

PIRMASIS SKIRSNIS
ATPAŽINTIES, TAPATUMO PATVIRTINIMO IR NAUDOJIMOSI IS SAUGUMAS IR KONTROLĖ

30. Fondo valdybos IS naudotojams prieigos ir teisių prie Fondo valdybos IS paslaugų ir išteklių suteikiamos ir valdomos vadovaujantis Taisyklėmis.

31. Fondo valdybos IS naudotojų paskyrų kūrimo, blokavimo, šalinimo bei paskyrų slaptažodžių valdymo politika reglamentuojama Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos aktyvių katalogų (Active Directory) sistemos saugumo nuostatuose, patvirtintų Fondo valdybos direktoriaus 2020 m. rugsėjo 8 d. įsakymu Nr. V-442 „Dėl Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos aktyvių katalogų (Active Directory) sistemos saugumo nuostatų patvirtinimo".

32. Fondo valdybos IS administratorių paskyrų kūrimo, blokavimo ir šalinimo bei paskyrų slaptažodžių valdymo politiką reglamentuoja Fondo valdybos direktoriaus patvirtinta tvarka.

ANTRASIS SKIRSNIS
NAUDOTOJŲ, ADMINISTRATORIŲ, RANGOVŲ ATLIEKAMŲ VEIKSMŲ AUDITAS IR KONTROLĖ

33. Fondo valdybos IS audito įrašų ir saugojimo tvarka:

33.1. Fondo valdybos IS audituose yra fiksuojama ši informacija:

33.1.1. Fondo valdybos programinės įrangos infrastruktūros elementų/komponentų įjungimas / išjungimas ar perkrovimas;

33.1.2. Fondo valdybos IS naudotojų, administratorių ir rangovų prisijungimas (ir nesėkmingi bandymai prisijungti) / atsijungimas;

33.1.3. Fondo valdybos IS naudotojų, administratorių ir rangovų teisių naudotis sistemos / tinklo ištekliais pakeitimai;

33.1.4. Fondo valdybos administratorių ir rangovų, dirbančių per privilegijuotą vartotojų prieigos teisių valdymo programinę įrangą (angl. PAM), atliekami veiksmai galiniuose įrenginiuose

(tarybinėse stotyse) ir (ar) programinės įrangos infrastruktūros elementuose/komponentuose, kurie yra jiems priskirti administruoti, yra filmuojami. Filmuoti įrašai yra laikomi ir saugomi 180 dienų PAM sistemoje. Asmenims, kurių veiksmai yra nufilmuoti, įrašai pasiekiami per PAM Web portalą.

33.1.5. Fondo valdybos programinės įrangos infrastruktūros elementų/komponentų audito funkcijos įjungimas / išjungimas;

33.1.6. Fondo valdybos programinės įrangos infrastruktūros elementų/komponentų audito įrašų trynimas, kūrimas ar keitimas;

33.1.7. Fondo valdybos programinės įrangos infrastruktūros elementų/komponentų sistemos / tinklo parametrų, laiko ir (ar) datos pakeitimai.

33.2. Fondo valdybos IS kiekviename audito duomenų įraše yra fiksuojama ši informacija:

33.2.1. Įvykio data ir tikslus laikas;

33.2.2. Įvykio rūšis / pobūdis;

33.2.3. Fondo valdybos IS naudotojo / administratoriaus ir (arba) Fondo valdybos programinės įrangos infrastruktūros elementų/komponentų, susijusio su įvykiu, duomenys.

33.2.4. Įvykio rezultatas.

33.3. Priemonės, naudojamos Fondo valdybos IS sąsajoje su viešųjų elektroninių ryšių tinklu, nustatytos taip, kad fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais.

33.4. Fondo valdyboje yra įdiegta centralizuota saugumo informacijos ir įvykių valdymo sistema, į kurią yra surenkami įvykiai iš prijungtų Fondo valdybos programinės įrangos infrastruktūros elementų/komponentų, ir centralizuotai saugomi.

33.5. Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant informuojamas Administratorius ir asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą.

33.6. Audito duomenys turi būti saugomi ne trumpiau kaip 60 dienų, užtikrinant visas prasmingas jų turinio reikšmes (pavyzdžiui, Fondo valdybos IS naudotojo, su kuriuo nutraukti darbo santykiai ir kuris pašalintas iš sistemos, atpažinties duomenys išsaugomi visą būtiną audito duomenų saugojimo laiką).

33.7. Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas.

33.8. Audito duomenys kopijuojami pagal Fondo valdybos nustatytą tvarką. Archyve saugomi audito duomenys yra apsaugoti nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.

33.9. Naudojimasis audito duomenimis yra kontroliuojamas ir fiksuojamas. Audito duomenys yra pasiekiami tik Administratoriui ir asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą (peržiūros teisėmis).

33.10. Audito įrašų duomenys analizuojami ne rečiau kaip kartą per mėnesį ir apie analizės rezultatus informuojamas asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą.

33.11. Audituojamų įrašų laiko žymos turi būti sinchronizuotos ne mažiau kaip vienos sekundės tikslumu.

33.12. Turi būti naudojami mažiausiai du laiko sinchronizavimo šaltiniai.

TREČIASIS SKIRSNIS
ĮSIBROVIMO APTIKIMAS IR PREVENCIJA

34. Fondo valdybos IS yra įdiegta įsilaužimo kompiuterių tinklą aptikimo ir prevencijos sistema.

35. Fondo valdybos IS yra įdiegta centralizuota saugumo informacijos ir įvykių valdymo sistema, kurioje fiksuojami audito įrašai, įskaitant ir galimai įtartinus veiklai audito įrašus, automatizuotai yra kuriamas pranešimas apie galimai pavojingą veiklą. Sukurtas pranešimas apie galimai pavojingą veiklą yra klasifikuojamas pagal užfiksuotą įvykį.

36. Įsilaužimo atakų pėdsakai (angl. *attack signature*) atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos.

37. Pagrindinėse tarnybinėse stotyse yra įjungtos ugniasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su Fondo valdybos IS funkcionalumu ir administravimu susijusį, duomenų srautą.

38. Įsilaužimo aptikimo techninio sprendinio įgyvendinimas, konfigūracija ir kibernetinių incidentų aptikimo taisyklės yra saugomos elektronine forma atskirai nuo Fondo valdybos IS techninės įrangos (kartu nurodant atitinkamas datas (įgyvendinimo, atnaujinimo ir panašiai), atsakingus asmenis, taikymo periodus ir panašiai).

39. Fondo valdybos IS elektroninės informacijos perdavimo tinklas yra atskirtas nuo viešųjų ryšių tinklų naudojant saugasienę; saugasienės įvykių žurnalai (angl. *Logs*) yra reguliariai analizuojami, o saugasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos.

40. Fondo valdybos IS tinklo perimetro apsaugai yra naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenkimo kodo.

KETVIRTASIS SKIRSNIS
BELAIDŽIO TINKLO SAUGUMAS IR KONTROLĖ

41. Draudžiama jungtis prie interneto komutuojamomis telefono linijomis (modemu) ir bevielio ryšio įranga.

PENKTASIS SKIRSNIS
MOBILIŲJŲ ĮRENGINIŲ, NAUDOJAMŲ PRISIJUNGTI PRIE IS SAUGUMAS IR KONTROLĖ

42. Vadovaujamasi Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos mobilių įrenginių naudojimo tvarkos aprašu, patvirtintu Fondo valdybos direktoriaus 2016 m. lapkričio 15 d. įsakymu Nr. V-597 „Dėl Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos mobilių įrenginių naudojimo tvarkos aprašo patvirtinimo”.

ŠEŠTASIS SKIRSNIS
FONDO VALDYBOS SVETAINĖS, PASIEKIAMOS IŠ VIEŠŲJŲ ELEKTRONINIŲ RYŠIŲ TINKLŲ, SAUGUMAS IR KONTROLĖ

43. Papildomi atpažinties, tapatumo patvirtinimo ir naudojimosi kontrolės reikalavimai:

43.1. Draudžiama slaptažodžius saugoti programiniame kode.

43.2. Fondo valdybos naudojama svetainė, patvirtinanti nuotolinio prisijungimo tapatumą, draudžia automatiškai išsaugoti slaptažodžius.

44. Fondo valdybos IS yra įgyvendinti svetainės kriptografijos reikalavimai.

44.1. Svetainės administravimo darbai atliekami ne trumpesniu kaip 128 bitų raktu.

44.2. Šifruojant naudojami skaitmeniniai sertifikatai išduodami patikimų sertifikavimo tarnybų. Sertifikato raktas yra ne trumpesnis kaip 2048 bitų.

44.3. naudojamas naujausia TLS (angl. *Transport Layer Security*) standarto versija.

44.4. Fondo valdybos naudojamos svetainės kriptografinės funkcijos įdiegtos tarnybinėje stotyje, kurioje yra Fondo valdybos svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. *Hardware security module*).

44.5. Visi kriptografiniai moduliai geba saugiai sutrikti (angl. *fail securely*).

44.6. Kriptografiniai raktai ir algoritmai yra valdomi pagal Fondo valdybos reikalavimus.

45. Draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai.

46. Fondo valdybos IS yra įdiegta svetainės saugasienė (angl. *Web Application Firewall,* toliau - WAF), kuri yra atnaujinama reguliariai. Įsilaužimo atakų pėdsakai (angl. *attack signature*) atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos.

47. Fondo valdybos IS naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), įterptinių instrukcijų atakų (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), paskirstyto atsisakymo aptarnauti (angl. *DDOS*) ir kitų, priemonės.

48. Fondo valdybos IS naudojama svetainės naudotojo įvedamų duomenų tikslumo kontrolė (angl. *Validation*).

49. Tarnybinė stotis, kurioje yra Fondo valdybos svetainė, nerodo naudotojui klaidų pranešimų apie Fondo valdybos svetainės programinį kodą ar tarnybinę stotį.

50. Fondo valdybos turimos svetainės saugumo priemonės geba automatiškai uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir panašiai).

51. Tarnybinė stotis, kurioje yra Fondo valdybos svetainė, leidžia tik šios svetainės funkcionalumui užtikrinti reikalingus HTTP metodus.

52. Draudžiama naršyti Fondo valdybos svetainės aplankuose (angl. *Directory browsing).*

53. Įdiegta svetainių turinio nesankcionuoto pakeitimo (angl. *Defacement*) stebėsenos sistema.

SEPTINTASIS SKIRSNIS
FONDO VALDYBOS INTERNETO SAUGUMAS IR KONTROLĖ

54. Fondo valdyba, sudarytoje sutartyje su interneto paslaugos teikėju, nurodo:

54.1. Reagavimo į kibernetinius incidentus įprastomis darbo valandomis;

54.2. Reagavimo į kibernetinius incidentus po darbo valandų;

54.3. Nepertraukiamo interneto paslaugos teikimo 24 valandas per parą, 7 dienas per savaitę.

54.4. Interneto paslaugos sutrikimų registravimo:

54.4.1. įprastomis darbo valandomis;

54.4.2. 24 valandas per parą, 7 dienas per savaitę;

54.5. apsaugos nuo Fondo valdybos IS trikdymo taikymo (angl. *Denial of Service, DoS*).

_____