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

FINANSŲ MINISTERIJOS TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Finansų ministerijos tinklų ir informacinių sistemų kibernetinio saugumo politikos apraše (toliau – Saugumo politikos aprašas) nustatoma Lietuvos Respublikos finansų ministerijos (toliau – ministerija) veiklos, susijusios su ministerijos tinklų ir informacinių sistemų, kurias sudaro ministerijos valdomos ir tvarkomos valstybės informacinės sistemos (toliau – IS), vidaus administravimo IS (toliau – AIS), interneto ir intraneto svetainės, (toliau – TIS) kibernetine apsauga, organizavimo tvarka, bendrieji kibernetinio saugumo reikalavimai ir įpareigojimai, kurių turi laikytis visi ministerijos valstybės tarnautojai ir pagal darbo sutartis dirbantys darbuotojai (toliau kartu – ministerijos darbuotojai), kurie yra TIS naudotojai, bei trečiosios šalys, kurios teikia paslaugas ministerijos TIS, (toliau – trečioji šalis).

2. Saugumo politikos apraše vartojamos sąvokos suprantamos taip, kaip apibrėžiamos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos elektroninių ryšių įstatyme, 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 standarte LST EN ISO/IEC 27000:2020 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Apžvalga ir aiškinamasis žodynas“.

3. Saugumo politikos aprašo tikslas – nustatyti TIS kibernetinio saugumo principus ir valdymo kryptis, siekiant užtikrinti TIS duomenų ir informacijos konfidencialumą, vientisumą bei prieinamumą, veiklos tęstinumą ir teisės aktuose reglamentuotų kibernetinio saugumo reikalavimų įgyvendinimą.

4. Ministerijos veiklos užtikrinant kibernetinį saugumą tikslai:

4.1. užtikrinti TIS patikimą bei saugų veikimą, įskaitant duomenų ir informacijos konfidencialumą, vientisumą ir prieinamumą;.

4.2. įgyvendinti nuoseklų kibernetinio saugumo rizikų, pokyčių, spragų ir pataisų valdymą, užtikrinant technologinių sprendimų atitiktį saugumo reikalavimams bei licencijuotos, patikrintos programinės įrangos naudojimą;

4.3. vykdyti TIS kibernetinio saugumo incidentų prevenciją, reaguoti į kibernetinio saugumo incidentus ir juos operatyviai valdyti;

4.4. užtikrinti kibernetinių incidentų aptikimą, valdymą ir veiklos tęstinumą galimų incidentų atveju;

4.5. ugdyti ministerijos darbuotojų atsakomybę bei kompetencijas kibernetinio saugumo srityje, organizuojant mokymus ir diegiant kibernetinės higienos principus.

5. TIS duomenų kibernetinio saugumo užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų TIS kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė;

5.2. duomenų, esančių TIS, konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.3. TIS tvarkyti naudojamos techninės ir programinės įrangos kontrolės užtikrinimas;

5.4. TIS paslaugų ir naudojimosi IS duomenimis kontrolės užtikrinimas;

5.5. IS tvarkomų asmens duomenų apsauga;

5.6. TIS veiklos tęstinumo užtikrinimas;

5.7. IS naudotojų mokymas.

II SKYRIUS
KIBERNETINĮ SAUGUMĄ REGLAMENTUOJANTYS TEISĖS AKTAI

6. Teisės aktai, kuriais vadovaujantis tvarkomas ir užtikrinamas ministerijos TIS kibernetinis saugumas:

6.1. Kibernetinio saugumo įstatymas;

6.2. Valstybės informacinių išteklių valdymo įstatymas;

6.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

6.4. Reglamentas (ES) 2016/679;

6.5. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nutarimas Nr. 818);

6.6. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

6.7. Lietuvos standartai LST ISO/IEC ISO 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ ir LST EN ISO/IEC 27002 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“ bei kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys informacijos saugą;

6.8. kiti teisės aktai, reglamentuojantys duomenų ir kibernetinio saugumo valdymą, saugų TIS ir (ar) valstybės informacinių išteklių naudojimą.

7. Finansų ministro tvirtinami kibernetinio saugumo politikos įgyvendinimą ministerijoje reglamentuojantys dokumentai (toliau – kibernetinio saugumo dokumentai), kuriais privalo vadovautis visi ministerijos darbuotojai ir trečiosios šalys:

7.1. Saugumo politikos aprašas;

7.2. Finansų ministerijos informacinių sistemų prieigų valdymo tvarkos aprašas;

7.3. Finansų ministerijos tinklų ir informacinių sistemų veiklos tęstinumo valdymo planas (toliau – TIS veiklos tęstinumo valdymo planas);

7.4. Finansų ministerijos kibernetinių incidentų valdymo planas.

III SKYRIUS
KIBERNETINĮ SAUGUMĄ UŽTIKRINANČIŲ ASMENŲ FUNKCIJOS

8. Finansų ministras paskiria:

8.1. kibernetinio saugumo vadovą – Kibernetinio saugumo įstatymo 15 straipsnio 5 dalyje nurodytus reikalavimus atitinkantį ministerijos darbuotoją, kuris atsakingas už ministerijai Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytų reikalavimų įgyvendinimą ir atlieka

Kibernetinio saugumo reikalavimų aprašo, patvirtinto Nutarimu Nr. 818, (toliau – Kibernetinio saugumo reikalavimų aprašas) 20 punkte nustatytas funkcijas ir kituose Lietuvos Respublikos teisės aktuose, reglamentuojančiuose kibernetinį saugumą, ir kibernetinio saugumo dokumentuose jam priskirtas funkcijas;

8.2. saugos įgaliotinį – Kibernetinio saugumo įstatymo 15 straipsnio 5 dalyje nurodytus reikalavimus atitinkantį ministerijos darbuotoją, kuris atsakingas už ministerijai Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytų reikalavimų įgyvendinimą ir atlieka Kibernetinio saugumo reikalavimų aprašo 20 punkte nustatytas funkcijas ir kituose Lietuvos Respublikos teisės aktuose, reglamentuojančiuose kibernetinį saugumą, ir kibernetinio saugumo dokumentuose jam priskirtas funkcijas;

8.3. IS administratorius – ministerijos darbuotojus, kurie prižiūri ir atlieka su priežiūra susijusias Kibernetinio saugumo reikalavimų aprašo 21 punkte nustatytas funkcijas;

8.4. IS infrastruktūros administratorius – ministerijos darbuotojus, kurie prižiūri ministerijos tinklus, techninę ir programinę įrangą, AIS ir jos infrastruktūrą, užtikrina jos veikimą ir kibernetinę saugą, atlieka su šia priežiūra susijusias Kibernetinio saugumo reikalavimų aprašo 21 punkte nustatytas funkcijas.

9. Kibernetinio saugumo vadovas, koordinuodamas ir prižiūrėdamas Saugumo politikos apraše ir kituose kibernetinio saugumo dokumentuose nustatytų reikalavimų įgyvendinimą, atlieka šias funkcijas:

9.1. užtikrina, kad kibernetinio saugumo dokumentai atitiktų Lietuvos Respublikos teisės aktus, reglamentuojančius kibernetinį saugumą;

9.2. užtikrina, kad kibernetinio saugumo dokumentai būtų parengti ir periodiškai atnaujinami;

9.3. organizuoja TIS rizikos ir atitikties vertinimus, rengia ir teikia tvirtinti finansų ministrui:

9.3.1. rizikos vertinimo ataskaitą ir, jei rizikos vertinimo metu nustatoma šalinamų trūkumų, rizikos valdymo planą;

9.3.2. atitikties vertinimo ataskaitą ir nustatytų neatitikčių šalinimo planą (jei buvo nustatyta neatitikčių);

9.4. organizuoja rizikos vertinimą ir dalyvauja rizikos vertinimo procese, teikia tvirtinti finansų ministrui rizikos vertinimo ataskaitas ir rizikos valdymo planus;

9.5. organizuoja TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymą, teikia tvirtinti finansų ministrui TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo rezultatų ataskaitą;

9.6. organizuoja ministerijos darbuotojų mokymus kibernetinio saugumo klausimais;

9.7. koordinuoja (išskyrus atvejus, kai tokia funkcija pavesta TIS veiklos tęstinumo valdymo plane nurodytai veiklos tęstinumo valdymo grupei) TIS kibernetinio saugumo incidentų, įvykusių TIS, tyrimą, bendradarbiauja su kompetentingomis įstaigomis, tiriančiomis elektroninių ryšių tinklų kibernetinio saugumo incidentus, neteisėtas veikas, susijusias su kibernetiniais incidentais;

9.8. teikia IS administratoriui, IS infrastruktūros administratoriui, vietiniam IS naudotojų administratoriui, IS veiklos administratoriui, saugos įgaliotiniui ir (ar) IS naudotojams privalomus vykdyti nurodymus, susijusius su kibernetinio saugumo dokumentuose nustatytų reikalavimų įgyvendinimu;

9.9. atlieka kitas Saugumo politikos apraše ir kituose kibernetinio saugumo dokumentuose bei kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

10. IS saugos įgaliotinio funkcijos:

10.1. užtikrinti, kad reikalavimai, nustatyti Saugumo politikos apraše ir kituose kibernetinio saugumo dokumentuose, būtų įgyvendinami TIS;

10.2. dalyvauti kibernetinio saugumo incidentų tyrimuose, rengiant informaciją apie incidentus bei teikiant duomenis kibernetinio saugumo vadovui;

10.3. dalyvauti organizuojant TIS atitikties Kibernetinio saugumo reikalavimų aprašui vertinimą, rengti ir teikti kibernetinio saugumo vadovui atitikties vertinimo ataskaitą ir nustatytų neatitikčių šalinimo planą;

10.4. dalyvauti rizikos vertinimo procese, rengti ir teikti kibernetinio saugumo vadovui rizikos vertinimo ataskaitas ir rizikos valdymo planus;

10.5. organizuoti TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymą, rengti ir teikti kibernetinio saugumo vadovui TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo rezultatų ataskaitas;

10.6. organizuoti ir vykdyti kibernetinio saugumo priemonių diegimą ir stebėseną;

10.7. teikti IS valdytojui siūlymus dėl:

10.7.1. IS administratorių, vietinių IS naudotojų administratorių skyrimo ir reikalavimų jiems nustatymo;

10.7.2. kibernetinio saugumo dokumentų priėmimo, keitimo ar pripažinimo netekusiais galios;

10.8. teikti nurodymus IS administratoriams, infrastruktūros administratoriams ir kitiems atsakingiems asmenims, siekiant laiku nustatyti ir pašalinti saugumo spragas;

10.9. teikti kibernetinio saugumo vadovui reguliarias priskirtų TIS būklės, incidentų ir rizikos valdymo veiksmų ataskaitas;

10.10. vykdyti techninių saugumo sprendimų priežiūrą ir užtikrinti, kad TIS atitiktų nustatytus saugumo ir gerosios praktikos reikalavimus;

10.11. dalyvauti rengiant, testuojant ir įgyvendinant TIS veiklos tęstinumo valdymo planus;

10.12. supažindinti suinteresuotus asmenis (naudotojus, administratorius, paslaugų teikėjus) su kibernetinio saugumo dokumentais ir kitais teisės aktais, reglamentuojančiais kibernetinį saugumą, taip pat su atsakomybe už reikalavimų nesilaikymą;

10.13. koordinuoti ministerijos darbuotojų ir kitų suinteresuotų asmenų mokymus, susijusius su kibernetiniu saugumu, informuoti juos apie duomenų saugos problemas, užtikrinti ministerijos darbuotojų informuotumą apie kibernetines grėsmes ir prevencines priemones;

10.14. atlikti kitas Lietuvos Respublikos teisės aktuose, reglamentuojančiuose kibernetinį saugumą, ir kibernetinio saugumo dokumentuose jam priskirtas funkcijas.

11. IS administratoriaus funkcijos:

11.1. diegti ir (arba) prižiūrėti programinės įrangos diegimą, atnaujinimą ir veikimą;

11.2. registruoti jam priskirtos IS naudotojus, skirti registravimo vardus, nustatyti IS naudotojams prieigos prie IS teises;

11.3. rengti pasiūlymus dėl IS kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir IS kibernetinio saugumo užtikrinimo;

11.4. užtikrinti priskirtos IS ar jos komponentų (posistemių, duomenų bazių valdymo sistemų, taikomųjų programų sistemų) veikimą, priežiūrą ir IS kibernetinį saugumą, rengti IS sąrankos aprašymo dokumentacijos atnaujinimą, nustatyti IS pažeidžiamas vietas, parinkti ir diegti saugos priemones bei užtikrinti jų atitiktį TIS kibernetinio saugumo reikalavimams;

11.5. informuoti kibernetinio saugumo vadovą ir (arba) IS saugos įgaliotinį apie IS kibernetinio saugumo incidentus, teikti pasiūlymus dėl šių incidentų pašalinimo;

11.6. daryti jam priskirtos IS duomenų bazės atsargines kopijas, atlikti informacijos atkūrimo iš kopijų bandymus (IS administratoriui, kuriam priskirta ši funkcija);

11.7. teikti kibernetinio saugumo vadovui ir (arba) IS saugos įgaliotiniui pasiūlymus dėl kibernetinio saugumo dokumentų priėmimo, keitimo ar pripažinimo netekusiais galios;

11.8. tvarkant duomenis, įskaitant asmens duomenis, dokumentus ir jų kopijas, saugoti tų duomenų ir informacijos paslaptį, neatskleisti, neperduoti tvarkomų duomenų ir informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija. Ši pareiga galioja ir nutraukus su ministerijos IS duomenų, informacijos, dokumentų ir jų kopijų tvarkymu susijusią veiklą;

11.9. neperduoti neįgaliotiems asmenims prisijungimo vardų ir slaptažodžių, IS naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitus IS duomenis, ir nesudaryti kitų sąlygų susipažinti su IS tvarkomais duomenimis;

11.10. atlikti kitas Lietuvos Respublikos teisės aktuose, reglamentuojančiuose kibernetinį saugumą, ir kibernetinio saugumo dokumentuose jam priskirtas funkcijas.

12. IS infrastruktūros administratoriaus funkcijos:

12.1. administruoti IS veikimą užtikrinančią techninę ir programinę įrangą, infrastruktūrą bei informacinių technologijų paslaugas, užtikrinti IS infrastruktūros veikimą, informacinių technologijų paslaugų teikimą ir registruoti jų naudotojus, skirti registravimo vardus ir suteikti prieigos prie IS infrastruktūros išteklių teises;

12.2. administruoti priskirtus IS komponentus (kompiuterius, serverius, operacines sistemas, užkardas (angl. *firewall*), įsilaužimo aptikimo sistemas, duomenų perdavimo tinklus, duomenų perdavimo tinklų techninę įrangą, spausdinimo techninę įrangą, vaizdo stebėjimo techninę įrangą), parengti ir atnaujinti IS komponentų sąrankos aprašymo dokumentaciją, vykdyti pažeidžiamų vietų nustatymą ir saugos priemonių parinkimą bei užtikrinti jų atitiktį kibernetinio saugumo dokumentų reikalavimams;

12.3. užtikrinti kompiuterizuotų darbo vietų veikimą, diegti ir konfigūruoti kompiuterizuotų darbo vietų programinę įrangą, diegti kompiuterizuotų darbo vietų programinės įrangos atnaujinimus, stebėti ir analizuoti kompiuterizuotų darbo vietų veikimą;

12.4. pagal ministerijos Informacinių technologijų departamento direktoriaus tvirtinamą Rezervinio kopijavimo į išorines laikmenas procedūrų vadovą daryti atsargines kopijas (fizinių serverių, virtualiųjų serverių ir kitų komponentų), IS administratorių sukurtų atsarginių kopijų įrašymą į magnetines laikmenas ir užtikrinti nutolusioje patalpoje, archyve esančių kopijų saugojimą;

12.5. rengti pasiūlymus dėl IS kūrimo, palaikymo, priežiūros ir TIS kibernetinio saugumo reikalavimų įgyvendinimo;

12.6. informuoti kibernetinio saugumo vadovą ir (arba) IS saugos įgaliotinį apie TIS kibernetinio saugumo incidentus ir teikti pasiūlymus dėl šių incidentų pašalinimo;

12.7. tvarkant IS duomenis, įskaitant asmens duomenis, dokumentus ir jų kopijas, saugoti tų duomenų ir informacijos paslaptį, neatskleisti, neperduoti tvarkomų duomenų ir informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija. Ši pareiga galioja ir nutraukus su ministerijos IS duomenų, informacijos, dokumentų ir jų kopijų tvarkymu susijusią veiklą;

12.8. neperduoti neįgaliotiems asmenims prisijungimo vardų ir slaptažodžių, IS naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitus IS tvarkomus duomenis, ir nesudaryti kitų sąlygų susipažinti su jais;

12.9. teikti kibernetinio saugumo vadovui ir (arba) IS saugos įgaliotiniui siūlymus dėl Saugumo politikos aprašo ir kitų kibernetinio saugumo dokumentų priėmimo, keitimo ar pripažinimo netekusiais galios;

12.10. užtikrinti tinkamą kibernetinio saugumo dokumentuose nustatytų funkcijų, susijusių su IS priežiūra ir informacinių technologijų paslaugų teikimu, atlikimą;

12.11. registruoti AIS naudotojus, skirti registravimosi vardus, suteikti naudotojų prieigos teises;

12.12. atlikti kitas Lietuvos Respublikos teisės aktuose, reglamentuojančiuose kibernetinį saugumą, ir kibernetinio saugumo dokumentuose jam priskirtas funkcijas.

13. Ministerijos saugumo operacijų centro funkcijos nustatytos Finansų ministerijos kibernetinių incidentų valdymo plane.

14. Veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės funkcijos nustatytos TIS veiklos tęstinumo valdymo plane.

15. IS saugos įgaliotinio, IS administratoriaus, IS infrastruktūros administratoriaus veiksmai įvykus kibernetiniam incidentui reglamentuojami TIS veiklos tęstinumo valdymo plane.

IV SKYRIUS
MINISTERIJOS DARBUOTOJŲ IR TREČIŲJŲ ŠALIŲ ĮSIPAREIGOJIMAI

16. Ministerijos darbuotojai per bendrąją dokumentų valdymo sistemą (DBSIS) pasirašytinai supažindinami su kibernetinio saugumo dokumentais. Už supažindinimą su kibernetinio saugumo dokumentais atsakingas IS saugos įgaliotinis. Jeigu kibernetinio saugumo dokumentai pakeičiami, IS saugos įgaliotinis organizuoja ministerijos darbuotojų supažindinimą su šiais pakeistais dokumentais.

17. Ministerija, vadovaudamasi Kibernetinio saugumo reikalavimų aprašu, siekdama mažinti galimas kilti rizikas TIS paslaugų, darbų ar įrangos pirkimams, susijusiems su TIS projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, trečiosioms šalims (įskaitant subtiekėjus) nustato reikalavimus pagal Finansų ministerijos tinklų ir informacinių sistemų bei juose esančių duomenų kibernetinio saugumo užtikrinimo taisyklėse (priedas) nustatytus reikalavimus ir juos numato sutartyse su trečiųjų šalių paslaugų teikėjais (įskaitant subteikėjus).

18. IS saugos įgaliotinis sudaro trečiųjų šalių paslaugų teikėjų (įskaitant subteikėjus) sąrašą, jį tvarko ir, pasikeitus sutartims, ar įvykus reikšmingiems pokyčiams arba reikšmingiems incidentams, susijusiems su trečiųjų šalių paslaugų teikėjais (įskaitant subteikėjus), šį sąrašą peržiūri ir atnaujina periodiškai, bet ne rečiau kaip kartą per metus.

19. Atlikdami TIS sąrankos pakeitimus, IS administratoriai ir IS infrastruktūros administratoriai turi laikytis IS pokyčių valdymo tvarkos, nustatytos Finansų ministerijos valdomų ir (arba) tvarkomų informacinių sistemų pokyčių valdymo tvarkos apraše, patvirtintame Lietuvos Respublikos finansų ministro 2014 m. liepos 18 d. įsakymu Nr. 1K-224 „Dėl Finansų ministerijos valdomų ir (arba) tvarkomų informacinių sistemų pokyčių valdymo tvarkos aprašo patvirtinimo“.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

20. IS valdytojas privalo užtikrinti žmogiškųjų ir finansinių išteklių skyrimą kibernetinio saugumo valdymui užtikrinti.

21. Kibernetinio saugumo dokumentai turi būti peržiūrimi ir atnaujinami bent kartą per metus arba įvykus TIS esminiams pokyčiams (TIS architektūros ar infrastruktūros keitimai, naujų modulių diegimas ar ženklus esamų modulių funkcinių galimybių keitimas, visų kompiuterizuotų darbo vietų operacinės įrangos diegimas ir pan.).

22. Už NKC informavimą apie kibernetinio saugumo dokumentų pakeitimus, atliekamą Kibernetinio saugumo reikalavimų aprašo 5 punkte nustatyta tvarka, atsakingas kibernetinio saugumo vadovas.

23. Kibernetinio saugumo dokumentuose nurodyti asmens duomenys tvarkomi siekiant užtikrinti Saugumo politikos aprašo nuostatų įgyvendinimą (kibernetinio saugumo incidentų prevenciją, nustatymą, tyrimą ir jų padarinių šalinimą, TIS prieigos kontrolės administravimą, IS veiklos tęstinumą, techninių įrašų (žurnalų) tvarkymą ir TIS veikimo saugumo užtikrinimą), laikantis Reglamente (ES) 2016/679 nustatytų reikalavimų.

24. Saugumo politikos apraše nurodyti dokumentai ir duomenys tvarkomi ir saugomi vadovaujantis Lietuvos Respublikos dokumentų ir archyvų įstatymo ir jo įgyvendinamųjų teisės aktų nustatyta tvarka ir terminais.

25. Jeigu ministerijos darbuotojas tyčia arba dėl didelio neatsargumo pažeidžia kibernetinio saugumo dokumentų reikalavimus, dėl kurių kyla reali grėsmė TIS saugumui, duomenų konfidencialumui, vientisumui ar prieinamumui, toks pažeidimas gali būti laikomas šiurkščiu darbo pareigų pažeidimu.

_____

Finansų ministerijos tinklų ir
informacinių sistemų kibernetinio
saugumo politikos aprašo
priedas

FINANSŲ MINISTERIJOS TINKLŲ IR INFORMACINIŲ SISTEMŲ BEI JUOSE ESANČIŲ DUOMENŲ KIBERNETINIO SAUGUMO UŽTIKRINIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Finansų ministerijos tinklų ir informacinių sistemų bei juose esančių duomenų kibernetinio saugumo užtikrinimo taisyklėse (toliau – Kibernetinio saugumo užtikrinimo taisyklės) reglamentuojama tvarka ir reikalavimai, kad būtų užtikrinamas saugus duomenų tvarkymas ir kibernetinio saugumo reikalavimų įgyvendinimas Lietuvos Respublikos finansų ministerijos (toliau – ministerija) valdomose ir tvarkomose valstybės informacinėse sistemose (toliau – IS): Valstybės biudžeto, apskaitos ir mokėjimų sistemoje, kurios veikla reglamentuota Valstybės biudžeto, apskaitos ir mokėjimų sistemos nuostatuose, patvirtintuose Lietuvos Respublikos finansų ministro 2006 m. balandžio 6 d. įsakymu Nr. 1K-152 „Dėl Valstybės biudžeto, apskaitos ir mokėjimų sistemos steigimo, valdymo ir naudojimo“, Europos Sąjungos struktūrinės paramos kompiuterinės informacinės valdymo ir priežiūros sistemos, kurios veikla reglamentuota Europos Sąjungos struktūrinės paramos kompiuterinės informacinės valdymo ir priežiūros sistemos nuostatuose, patvirtintuose Lietuvos Respublikos finansų ministro 2006 m. liepos 20 d. įsakymu Nr. 1K-263 „Dėl Europos Sąjungos struktūrinės paramos kompiuterinės informacinės valdymo ir priežiūros sistemos nuostatų patvirtinimo“, Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinėje sistemoje, kurios veikla reglamentuota Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinės sistemos nuostatuose, patvirtintuose Lietuvos Respublikos finansų ministro 2011 m. gegužės 13 d. įsakymu Nr. 1K-182 „Dėl Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinės sistemos nuostatų patvirtinimo“, Strateginio valdymo informacinėje sistemoje (toliau – SVIS), kurios veikla reglamentuota Strateginio valdymo informacinės sistemos nuostatuose, patvirtintuose Lietuvos Respublikos finansų ministro 2023 m. kovo 29 d. įsakymu Nr. 1K-114 „Dėl Strateginio valdymo informacinės sistemos steigimo“, Atvirųjų finansų informacinėje sistemoje, kurios veikla reglamentuota Atvirųjų finansų informacinės sistemos nuostatuose, patvirtintuose Lietuvos Respublikos finansų ministro 2020 m. sausio 22 d. įsakymu Nr. 1K-7 „Dėl Atvirųjų finansų informacinės sistemos steigimo“, vidaus administravimo IS (toliau – AIS), elektroninių ryšių tinkle, interneto ir intraneto svetainėse (toliau kartu – TIS).

2. IS pagal jose tvarkomų duomenų svarbą skirstomos į 4 rūšis, kurios nustatomos vadovaujantis Valstybės informacinių išteklių svarbos vertinimo metodika, patvirtinta Lietuvos Respublikos ekonomikos ir inovacijų ministro 2023 m. liepos 19 d. įsakymu Nr. 4-418 „Dėl Valstybės informacinių išteklių svarbos nustatymo metodikos patvirtinimo“, (Kibernetinio saugumo užtikrinimo taisyklių 1 priedas). Kibernetinio saugumo užtikrinimo taisyklių 1 priede nurodytos IS, kurios priskirtos ypatingos svarbos rūšiai ir laikomos kritinėmis ministerijos veiklos tęstinumui užtikrinti.

3. IS tvarkoma informacija pagal turinį skirstoma taip:

3.1. nevieša informacija – informacija, kurios skelbimas ar viešas teikimas ribojamas Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo, 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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 asmens duomenų teisinės apsaugos įstatymo, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo, Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo ir kitų teisės aktų, reglamentuojančių duomenų saugą, taip pat IS nuostatuose reglamentuojami duomenys, kurie yra neviešinami;

3.2. vieša informacija – valstybės ir tarnybos paslapties nesudaranti informacija, kurios skelbimas ar viešas teikimas neribojamas teisės aktais, išskyrus IS nuostatuose nurodytus atvejus, kai duomenys neteikiami viešai.

4. IS tvarkytojai ir (arba) tvarkytojo atstovai yra atsakingi už jiems priskirtos IS tvarkomų duomenų teisingumą ir vientisumą.

5. Už IS duomenų tvarkymą atsakingi visi asmenys, kurie naudojasi IS.

6. IS duomenys, kuriuos IS naudotojai sukaupė atlikdami savo funkcijas, yra IS valdytojo nuosavybė.

II SKYRIUS
IS VALDYTOJO, IS TVARKYTOJŲ, TIS ADMINISTRATORIŲ IR IS NAUDOTOJŲ FUNKCIJOS IR ATSAKOMYBĖS

7. IS valdytojas, atsakingas už IS kibernetinio saugumo įgyvendinimo organizavimą ir įgyvendinimą, atlieka IS nuostatuose nustatytas funkcijas, taip pat:

7.1. tvirtina dokumentus, reglamentuojančius TIS kibernetinio saugumo politikos įgyvendinimą ministerijoje, (toliau – kibernetinio saugumo dokumentai), kitus dokumentus, susijusius su TIS duomenų kibernetiniu saugumu;

7.2. prižiūri ir kontroliuoja, kad IS būtų tvarkomos vadovaujantis IS nuostatais, TIS kibernetinio saugumo dokumentais ir kitais duomenų (įskaitant asmens duomenis) kibernetinę saugą reglamentuojančiais teisės aktais;

7.3. priima sprendimus dėl techninių ir programinių priemonių, būtinų TIS kibernetiniam saugumui užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

7.4. koordinuoja IS tvarkytojų darbą įgyvendinant IS duomenų kibernetinio saugumo reikalavimus;

7.5. nagrinėja IS tvarkytojų pasiūlymus dėl IS kibernetinio saugumo priemonių tobulinimo ir priima sprendimus dėl jų;

7.6. priima sprendimus dėl IS kibernetinio saugumo priemonių finansavimo;

7.7. užtikrina duomenų tvarkymo bei duomenų teikimo IS duomenų gavėjams teisėtumą ir kibernetinį saugumą;

7.8. atlieka kitas Lietuvos Respublikos kibernetinio saugumo įstatyme, Valstybės informacinių išteklių valdymo įstatyme nustatytas funkcijas.

8. IS tvarkytojai, atsakingi už IS kibernetiniam saugumui reikalingas priemones ir jų panaudojimą, atlieka IS nuostatuose nustatytas funkcijas, taip pat:

8.1. užtikrina šiuo finansų ministro įsakymu patvirtinto Finansų ministerijos tinklų ir informacinių sistemų kibernetinio saugumo politikos aprašo (toliau – Saugumo politikos aprašas) ir kitų kibernetinio saugumo dokumentų tinkamą įgyvendinimą IS tvarkytojo įstaigos tvarkomose IS;

8.2. užtikrina IS duomenų kibernetinį saugumą IS tvarkytojo įstaigos tvarkomose IS;

8.3. užtikrina duomenų, esančių IS duomenų bazėse, sistemų kataloguose, saugą;

8.4. užtikrina saugų duomenų perdavimą elektroninių ryšių tinklais;

8.5. teikia IS valdytojui pasiūlymus dėl IS kibernetinio saugumo tobulinimo;

8.6. planuoja ir įgyvendina priemones, mažinančias IS duomenų atskleidimo ir praradimo riziką bei užtikrinančias prarastų duomenų atkūrimą ir duomenų apsaugą nuo klastojimo;

8.7. užtikrina nepertraukiamą IS veikimą;

8.8. užtikrina IS duomenų tvarkymo bei duomenų teikimo IS duomenų gavėjams teisėtumą;

8.9. valdo IS kibernetinio saugumo incidentus;

8.10. atlieka kitas IS valdytojo pavestas kibernetinio saugumo dokumentuose ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, jiems priskirtas funkcijas.

9. Už TIS priežiūrą, administravimą ir kibernetinio saugumo užtikrinimą jų administruojamose IS atsakingi IS administratoriai, tinklų ir infrastruktūros – IS infrastruktūros administratoriai. Atliekant šias funkcijas, techniniai įrašai, prieigos duomenys ar kiti TIS duomenys nenaudojami ministerijos valstybės tarnautojų ir pagal darbo sutartis dirbančių darbuotojų (toliau kartu – ministerijos darbuotojai) veiklos, elgesio ar darbo našumo stebėsenai, jie naudojami tik tiek, kiek būtina TIS kibernetinio saugumo incidentų prevencijai, nustatymui, tyrimui ir jų padarinių šalinimui užtikrinti.

10. Vietinis IS naudotojų administratorius – IS tvarkytojo arba kitos IS naudojančios organizacijos darbuotojas, atliekantis teisės aktuose, reglamentuojančiuose kibernetinį saugumą, ir kibernetinio saugumo dokumentuose jam priskirtas funkcijas:

10.1. registruoja savo įstaigos IS naudotojus, skiria registravimosi vardus (prisijungti prie IS), nustato IS naudotojams prieigos prie IS teises (tam tikrais atvejais tai gali atlikti ministerijos IS administratorius);

10.2. informuoja IS administratorių apie galimus IS kibernetinio saugumo incidentus, teikia jam pasiūlymus dėl šių incidentų pašalinimo;

10.3. tvarkydamas asmens duomenis saugo tų duomenų ir informacijos paslaptį, neatskleidžia, neperduoda tvarkomų duomenų ir informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija. Ši pareiga galioja ir nutraukus su IS duomenų, informacijos, dokumentų ir jų kopijų tvarkymu susijusią veiklą;

10.4. neperduoda neįgaliotiems asmenims prisijungimo vardų ir slaptažodžių, IS naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitus IS tvarkomus duomenis, ir neturi teisės sudaryti sąlygų susipažinti su šiais duomenimis.

11. IS veiklos administratorius – viename iš ministerijos struktūrinių padalinių dirbantis ministerijos darbuotojas, atsakingas už tam tikros IS veiklą, priežiūrą ir plėtrą ir paskirtas atsakingu už jam priskirtos IS veiklos administravimą:

11.1. atlieka IS duomenų struktūros ir formos konfigūravimo darbus, susijusius su IS veikla;

11.2. administruoja IS duomenis, kurie susiję su veiklos procesais, formuoja ataskaitas ir viešojoje erdvėje (interneto svetainėje, turinio valdymo sistemoje ar kt.) atnaujina duomenis apie savo administruojamą IS;

11.3. tikrina IS procesų ir duomenų teisingumą, rengia ir teikia IS valdytojui siūlymus dėl IS veikimo;

11.4. administruoja su IS tvarkytojais susijusią informaciją, įskaitant atsakingų asmenų administravimą ir tvirtinimą;

11.5. tvarkydamas IS duomenis, įskaitant asmens duomenis, saugo tų duomenų ir informacijos paslaptį, neatskleidžia, neperduoda tvarkomų duomenų ir informacijos nė vienam asmeniui, kuris nėra įgaliotas naudotis šiais duomenimis ir informacija. Ši pareiga galioja ir nutraukus su IS duomenų, informacijos, dokumentų ir jų kopijų tvarkymu susijusią veiklą;

11.6. neperduoda neįgaliotiems asmenims registravimosi vardų (prisijungti prie IS) ir slaptažodžių ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitus IS tvarkomus duomenis, ir nesudaro kitų sąlygų susipažinti su šiais duomenimis;

11.7. atlieka kitas Lietuvos Respublikos teisės aktuose, reglamentuojančiuose kibernetinį saugumą, ir kibernetinio saugumo dokumentuose jam priskirtas funkcijas.

12. IS vidiniai naudotojai – ministerijos darbuotojai ir IS išoriniai naudotojai – kiti asmenys, kuriems suteikta teisė naudotis ministerijos tvarkomais IS duomenimis, atlieka šias funkcijas:

12.1. naudoja TIS, vadovaudamiesi Saugumo politikos aprašu, Kibernetinio saugumo užtikrinimo taisyklėmis, IS duomenų teikimo sutartimis, IS naudojimo instrukcijomis ir pareigybių aprašymais;

12.2. tvarko tik tuos IS duomenis ir tik ta apimtimi, kuri būtina jų funkcijoms atlikti, ir tik pagal jiems suteiktas prieigos teises. Draudžiama naudoti duomenis kitais nei jų funkcijoms atlikti būtinais tikslais;

12.3. pastebėję kibernetinį incidentą ar TIS sutrikimą, neveikiančių arba netinkamai veikiančių IS duomenų saugumo užtikrinimo priemonių, privalo nedelsdami apie tai pranešti IS administratoriui, IS infrastruktūros administratoriui ir (arba) IS saugos įgaliotiniui;

12.4. tvarkydami duomenis, įskaitant asmens duomenis, dokumentus ar jų kopijas, saugo tų duomenų ir informacijos paslaptį, neatskleidžia, neperduoda tvarkomų duomenų nė vienam asmeniui, kuris nėra įgaliotas naudotis šiais duomenimis. Ši pareiga galioja ir nutraukus su IS duomenų, dokumentų ir jų kopijų tvarkymu susijusią veiklą;

12.5. neperduoda neįgaliotiems asmenims prisijungimo vardų ir slaptažodžių, IS naudotojo tapatybės kodų ar kitos informacijos, leidžiančios naudojantis programinėmis ir techninėmis priemonėmis sužinoti asmens duomenis ar kitus IS tvarkomus duomenis, ir nesudaro kitų sąlygų susipažinti su šiais duomenimis;

12.6. atlieka kitas Lietuvos Respublikos teisės aktuose, reglamentuojančiuose kibernetinį saugumą, ir kibernetinio saugumo dokumentuose jiems priskirtas funkcijas;

12.7. vykdo kibernetinio saugumo vadovo, IS saugos įgaliotinio, IS administratoriaus ir IS infrastruktūros administratoriaus, IS veiklos administratoriaus nurodymus, susijusius su IS naudojimu ir IS kibernetiniu saugumu.

13. IS administratoriai, IS infrastruktūros administratoriai, IS veiklos administratoriai ir vietiniai IS naudotojų administratoriai atsakingi už tinkamą kibernetinio saugumo dokumentuose nustatytų funkcijų atlikimą. Atliekant šias funkcijas, techniniai įrašai, prieigos duomenys ar kiti TIS duomenys nenaudojami ministerijos darbuotojų veiklos, elgesio ar darbo našumo stebėsenai. Jie naudojami tik tiek, kiek būtina TIS kibernetinio saugumo incidentų prevencijai, nustatymui, tyrimui ir jų padarinių šalinimui užtikrinti.

14. IS administratoriai, IS infrastruktūros administratoriai, vietiniai IS naudotojų administratoriai, IS veiklos administratoriai ir IS naudotojai pasirašo nustatytos formos asmens, prižiūrinčio arba besinaudojančio Finansų ministerijos informacine sistema, įsipareigojimą (Kibernetinio saugumo užtikrinimo taisyklių 2 priedas) arba esant IS techninėms galimybėms (elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą) susipažįsta su Kibernetinio saugumo užtikrinimo taisyklėse nustatytais reikalavimais, sutinka jų laikytis ir yra atsakingi už visus veiksmus naudodamiesi IS.

III SKYRIUS
TIS RIZIKOS IR ATITIKTIES VERTINIMAS

15. IS saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) interneto svetainėje skelbiamas rekomendacijas dėl metinio rizikų vertinimo, taip pat į IS valdytojo ar jo įgalioto asmens tvirtinamą TIS rizikos vertinimo ir valdymo tvarkos aprašą (toliau – TIS rizikos vertinimo ir valdymo tvarkos aprašą), kasmet organizuoja TIS rizikos vertinimą. Įdiegus IS pokyčius (sistemos pakeitimai, konfigūracijų pakeitimai, programinės įrangos versijų naujinimas, papildymas naujomis taikomosiomis programomis, taikomųjų programų pašalinimas ir kt.) arba atlikus esminius organizacinius ar sisteminius pokyčius ir nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis TIS rizikos vertinimas.

16. Organizuodamas TIS rizikos vertinimą kibernetinio saugumo subjekto vadovas paskiria už rizikos vertinimą atsakingus asmenis. Atsakingu asmeniu gali būti skiriamas IS saugos įgaliotinis arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros ir nuolatinio tobulinimo paslaugas teikiančiu subjektu.

17. TIS rizikos vertinimo metu įvertinami rizikos veiksniai, galintys turėti įtakos TIS duomenų saugai ir kibernetiniam saugumui, jų galima žala, pasireiškimo tikimybė ir pobūdis, galimi rizikos valdymo būdai, rizikos priimtinumo kriterijai.

18. Svarbiausi TIS rizikos veiksniai:

18.1. subjektyvūs netyčiniai (duomenų tvarkymo klaidos ir apsirikimai, duomenų ištrynimas, klaidingas duomenų teikimas, fiziniai duomenų technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kt.);

18.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis IS duomenims gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo ar kibernetinio saugumo pažeidimai, vagystės ir kt.);

18.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

19. TIS rizikos veiksniai vertinami vadovaujantis NKSC interneto svetainėje pateiktomis rekomendacijomis, TIS rizikos vertinimo ir valdymo tvarka bei tarptautinio standarto ISO/IEC 27005:2022 „Informacijos sauga, kibernetinė sauga ir privatumo apsauga – Informacijos saugos rizikos valdymo gairės“ ir NIST SP 800-30 Rev. 1 „Rizikos vertinimo atlikimo gairės“ gairėmis.

20. TIS rizikos įvertinimo rezultatai ir priemonės, reikalingos siekiant išvengti rizikos veiksnių, išdėstomi TIS rizikos vertinimo ataskaitoje, kuri teikiama IS valdytojo vadovui arba jo įgaliotam asmeniui. Jeigu IS valdytojo vadovas paskiria įgaliotą asmenį, ataskaita teikiama ir IS valdytojo vadovui.

21. TIS rizikos vertinimo ataskaita rengiama vertinant rizikos veiksnius, galinčius turėti įtakos TIS duomenų saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus.

22. TIS rizikos vertinimo ataskaitoje rizikos veiksniai ir nustatyta rizikos tikimybė išdėstomi prioriteto tvarka pagal svarbą, kuri nustatoma atsižvelgiant į atliktą rizikos vertinimą.

23. Atsižvelgdamas į TIS rizikos vertinimo ataskaitą, IS valdytojo vadovas arba jo įgaliotas asmuo prireikus tvirtina TIS rizikos valdymo planą, kuris turi atitikti Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, (toliau – Kibernetinio saugumo reikalavimų aprašas) 12 punkte nustatytus reikalavimus.

24. Siekiant užtikrinti Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše ir kibernetinio saugumo dokumentuose nustatytų kibernetinio saugumo reikalavimų įgyvendinimą ir kontrolę, ne rečiau kaip kartą per metus organizuojamas ministerijos atitikties reikalavimams, nustatytiems kibernetinio saugumo subjektui Kibernetinio saugumo įstatyme, jo įgyvendinamuosiuose teisės aktuose, vertinimas (toliau – atitikties vertinimas). Atitikties vertinimas atliekamas vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“.

25. Atlikus atitikties vertinimą rengiami ir IS valdytojo vadovo arba jo įgalioto asmens tvirtinami:

25.1. atitikties vertinimo ataskaita;

25.2. nustatytų neatitikčių šalinimo planas (jei buvo nustatyta neatitikčių), kuriame paskirti atsakingi vykdytojai, reikalingi ištekliai ir nustatyti įgyvendinimo terminai.

26. Jeigu IS valdytojo vadovas yra paskyręs įgaliotą asmenį, šie dokumentai papildomai teikiami ir įgaliotam asmeniui koordinavimo tikslais, tačiau įgaliotas asmuo negali būti vienintelis jų gavėjas.

27. IS valdytojas privalo reguliariai, ne rečiau kaip kartą per 3 metus, atlikti nepriklausomą TIS kibernetinio saugumo auditą, vadovaudamasis Kibernetinio saugumo įstatymo 14 straipsnio 8 dalimi.

28. Kibernetinio saugumo reikalavimų veiksmingumo vertinimas atliekamas vadovaujantis Kibernetinio saugumo reikalavimų aprašo II skyriaus aštuntajame skirsnyje nustatyta tvarka ir turi būti organizuojamas ne rečiau kaip kartą per metus.

29. Kibernetinio saugumo vadovas TIS rizikos vertinimo ataskaitos ir rizikos valdymo plano patvirtinimo duomenis teikia Kibernetinio saugumo reikalavimų aprašo 13 punkte nustatyta tvarka.

30. Atsižvelgiant į atlikto TIS rizikos vertinimo rezultatus, taip pat jeigu Atitikties vertinimo metu nustatoma kibernetinių incidentų valdymo ir šalinimo, institucijos nepertraukiamos veiklos užtikrinimo trūkumų, atitinkamai turi būti tobulinama TIS veiklos tęstinumo valdymo tvarka. Pagal šią tvarką patvirtinto plano veiksmingumo išbandymo rezultatai išdėstomi plano veiksmingumo išbandymo ataskaitoje ir pastebėtų trūkumų ataskaitoje. IS saugos įgaliotinis veiklos tęstinumo valdymo plano išbandymo ataskaitos patvirtinimo duomenis pateikia Kibernetinio saugumo reikalavimų aprašo 29 punkte nustatyta tvarka.

31. TIS kibernetinio saugumo priemonės (techninės, programinės, organizacinės ir kitos TIS duomenų saugos priemonės) parenkamos vadovaujantis šiais principais:

31.1. priemonės diegimo kaina turi atitikti tvarkomų duomenų vertę;

31.2. liekamoji rizika turi būti sumažinta iki priimtino lygio;

31.3. atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, įdiegiamos prevencinės, detekcinės ir korekcinės kibernetinio saugumo priemonės.

IV SKYRIUS
TIS KIBERNETINIO SAUGUMO UŽTIKRINIMAS

PIRMASIS SKIRSNIS
BENDRIEJI TIS KIBERNETINIO SAUGUMO REIKALAVIMAI

32. Organizaciniai ir techniniai kibernetinio saugumo reikalavimai nustatomi pagal Kibernetinio saugumo reikalavimų aprašą, vadovaujantis Kibernetinio saugumo subjektų

identifikavimo pagal specialiuosius kriterijus metodika, patvirtinta Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, ir Saugumo politikos aprašo II skyriuje nurodytais teisės aktais ir standartais.

33. Organizacinių ir techninių TIS kibernetinio saugumo priemonių užtikrinimas turi būti grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos TIS kibernetiniam saugumui, rizikos vertinimu. Kibernetinio saugumo priemonės turi būti diegiamos atsižvelgiant į naujausius technikos laimėjimus, vadovaujantis gamintojo teikiama bent viena gerosios saugumo praktikos rekomendacija.

ANTRASIS SKIRSNIS
TIS ĮRANGOS IR PATALPŲ SAUGUMO REIKALAVIMAI

34. Kompiuterinės įrangos saugos priemonės:

34.1. Registruojama visa ministerijos kompiuterinė ir programinė įranga, fiksuojama jos buvimo vieta ministerijos pastate, atliekama metinė jos inventorizacija.

34.2. Ministerijos kompiuterinės įrangos konfigūraciją nustato ir ją aprašo ministerijos Informacinių technologijų departamento (toliau – ITD) Informacinių technologijų infrastruktūros skyriaus (toliau – ITIS) vadovas arba jo įgaliotas pagal darbo sutartį dirbantis ITIS darbuotojas (toliau kartu – ITIS darbuotojas).

34.3. Ministerijos kompiuterinės įrangos priežiūrą ir remontą atlieka ITIS darbuotojas arba kompiuterinės įrangos remonto paslaugas teikiantys paslaugų teikėjai pagal pasirašytas sutartis.

34.4. Kompiuterinės įrangos naudotojams draudžiama išnešti kompiuterinę įrangą iš ministerijos patalpų. Ši nuostata netaikoma ministerijos darbuotojams, naudojantiems nešiojamuosius kompiuterius, papildomai įrangai, išduotai darbui nuotoliniu būdu, ir ITD darbuotojams, atliekantiems savo funkcijas.

35. Siekiant apsaugoti nurašomoje, remontuojamoje kompiuterinėje įrangoje ir nebenaudojamose keičiamose ir nešiojamose duomenų laikmenose (standžiuosiuose diskuose, magnetinėse juostose, CD, DVD, USB atmintinėse, išmaniuosiuose įrenginiuose ir kitose laikmenose) esančius duomenis, ministerijoje taikomi šie saugos reikalavimai:

35.1. Išmontuojant ministerijos kompiuterinę įrangą ar naikinant duomenų laikmenas, iš jų privalo būti neatkuriamai ištrinti visi duomenys.

35.2. Duomenų laikmenos turi būti sunaikintos taip, kad toliau jų nebūtų galima naudoti.

35.3. Naudotus ministerijos kompiuterius perduodant patikėjimo teise kitoms valstybės institucijoms, įstaigoms ar organizacijoms, ITIS vadovo pavedimu juose esantys duomenys turi būti ištrinti taip, kad jų nebūtų įmanoma atkurti.

35.4. Išvežant remontuoti sugedusią ministerijos kompiuterinę įrangą, turi būti išimamos informacijos laikmenos (standieji diskai ir t. t.). Jeigu nėra galimybės išimti informacijos laikmenų, kompiuterinė įranga remontuojama tik suderinus tai su ITD direktoriumi – ITD direktoriui leidus perduoti ministerijos kompiuterinę įrangą remontuoti, ITIS vadovo pavedimu joje esanti informacija turi būti neatkuriamai ištrinama.

36. Ministerijos patalpose įrengtų TIS naudotojų kompiuterizuotų darbo vietų (toliau – KDV) saugos reikalavimai:

36.1. Turi būti naudojamos antivirusinės programos, kurių virusų parašų bazės atnaujinamos ne rečiau kaip kartą per parą, įdiegti naujausi operacinių sistemų saugos atnaujinimai.

36.2. KDV turi būti paruoštos vadovaujantis naudojamos programinės įrangos ir naudojamų IS gamintojų keliamais našumo, saugos ir kitais reikalavimais.

36.3. Turi būti naudojami slaptažodžiu apsaugoti prisijungimai.

36.4. TIS naudotojui neatliekant jokių veiksmų, KDV turi užsirakinti, kad toliau naudotis IS būtų galima tik pakartotinai patvirtinus savo tapatybę. Ilgiausias neaktyvumo laikas, kuriam pasibaigus TIS naudotojų ryšio sesijos automatiškai nutraukiamos, turi būti ne ilgesnis kaip 15 minučių. Šis reikalavimas netaikomas, jeigu, atlikus ryšių ir informacinių sistemų rizikos vertinimą, nustatomos kitos nustatytą riziką atitinkančios techninės kibernetinio saugumo priemonės.

36.5. Turi būti diegiama tik ministerijoje leistinos programinės įrangos sąraše nurodyta programinė įranga (sisteminė programinė įranga į sąrašą neįtraukiama). Leistinos programinės įrangos sąrašą tvirtina ITD direktorius, o sąrašas peržiūrimas ir atnaujinamas periodiškai, ne rečiau kaip vieną kartą per metus.

36.6. IS kompiuterinės įrangos apskaita atliekama naudojant AIS, programinės įrangos apskaita – naudojant kitus įrankius. Už AIS informacijos pildymą atsakingas ITIS vadovo paskirtas darbuotojas.

36.7. Kompiuterinei įrangai turi būti įrengtas elektros srovės tiekimas per atskirą nuo kitų elektros srovės naudotojų automatinį jungiklį.

36.8. Ministerijoje nešiojamieji kompiuteriai išduodami ir naudojami vadovaujantis ministerijos kanclerio tvirtinamomis Finansų ministerijos nešiojamųjų kompiuterių saugojimo, išdavimo ir naudojimo taisyklėmis.

36.9. Ministerijos TIS naudotojams draudžiama keisti ministerijos kompiuterinės įrangos sudėtį ir konfigūracijos parametrus.

36.10. Išvežamą remontuoti ministerijos kompiuterinę įrangą iš ministerijos patalpų išnešantį asmenį privalo išlydėti ITIS darbuotojas.

36.11. Už Kibernetinio saugumo užtikrinimo taisyklių 36.1–36.10 papunkčiuose nurodytų reikalavimų vykdymo kontrolę atsakingas ITIS vadovas.

36.12. KDV turi būti naudojamos tik ministerijos ITIS išduotos išorinės duomenų laikmenos (USB, CD, DVD ir kt.) ir kiti nešiojamieji ar išmanieji įrenginiai, kurie yra išduoti tik darbo funkcijoms atlikti. Ministerijos darbuotojas privalo naudotis visomis saugumo priemonėmis, kad apsaugotų nešiojamąjį kompiuterį ir duomenų laikmenas nuo vagystės, praradimo arba pažeidimo.

37. Ministerijos IT ir KDV elektros tiekimo užtikrinimo reikalavimai:

37.1. Visa ministerijos kompiuterinė įranga turi būti įžeminta.

37.2. Turi būti įrengti visos ministerijos kompiuterinės įrangos maitinimo įtampos automatiniai saugikliai ir jungikliai.

37.3. IS kompiuterinė įranga ir TIS administruoti naudojami kompiuteriai turi būti prijungti prie nepertraukiamo maitinimo šaltinių, prijungtų prie automatinio paskirstymo skydo, kuris maitinamas iš pastato elektros tinklo ir rezervinio elektros generatoriaus.

37.4. Apsaugai nuo elektros tiekimo sutrikimų ir elektros energijos tiekimui užtikrinti įrengtas atsarginis elektros srovės generatorius.

37.5. Prie IS administratorių ir IS infrastruktūros administratorių KDV kompiuterinės įrangos jungiami nepertraukiamo maitinimo šaltiniai.

37.6. Nepertraukiamo maitinimo šaltiniai turi būti periodiškai prižiūrimi.

38. Pagrindinės ministerijos TIS kompiuterinės įrangos: ministerijos patalpose esančių tarnybinių stočių, užkardų (saugasienių), maršrutizatorių, komutatorių, duomenims kopijuoti skirtos įrangos (toliau kartu – pagrindinė TIS kompiuterinė įranga), IS administratorių ir IS infrastruktūros administratorių KDV sauga užtikrinama šiomis priemonėmis:

38.1. Slaptažodžiai, leidžiantys dirbti su pagrindine TIS kompiuterine įranga, administruoti ministerijos TIS, nustatyti kompiuterinės įrangos konfigūraciją, žinomi tik ITD direktoriaus patvirtintiems IS administratoriams ir IS infrastruktūros administratoriams.

38.2. Pagrindinės ministerijos TIS kompiuterinės įrangos gedimai turi būti registruojami Kibernetinio saugumo užtikrinimo taisyklių 3 priede nustatytos formos TIS kompiuterinės įrangos gedimų registravimo žurnale. Už žurnalo pildymą atsakingas IS infrastruktūros administratorius.

38.3. Pagrindinė TIS kompiuterinė įranga turi būti ministerijos duomenų centro patalpoje arba gali būti perkelta į valstybinį duomenų centrą.

38.4. Prižiūrėti pagrindinę ministerijos TIS kompiuterinę įrangą, atlikti IS administratoriaus ir IS infrastruktūros administratoriaus funkcijas gali tik ITD direktoriaus patvirtinti administratoriai, turintys tinkamą kvalifikaciją. Ministerija, kaip IS valdytoja, turi užtikrinti šių darbuotojų kvalifikacijos tobulinimą.

38.5. Kibernetinei saugai užtikrinti turi būti automatiškai fiksuojami (įrašomi ir saugojami) šie žurnaliniai įrašai:

38.5.1. pagrindinės ministerijos TIS kompiuterinės įrangos įjungimas, išjungimas ar perkrovimas;

38.5.2. IS naudotojų ir IS administratorių autentifikavimo įvykiai;

38.5.3. IS naudotojų, IS administratorių paskyrų sukūrimas, prieigų prie TIS pakeitimai;

38.5.4. administratorių atliekami veiksmai;

38.5.5. operacinėse sistemose sukurtos ir atliktos sisteminės užduotys (angl. *scheduled task*);

38.5.6. grupinių politikų pakeitimai;

38.5.7. užkardų (saugasienių) taisyklių pakeitimai;

38.5.8. žurnalinių įrašų rinkimo funkcijos įjungimas, išjungimas;

38.5.9. operacinių sistemų laiko ir datos pakeitimai;

38.5.10. saugumo sistemų (antivirusinių, įsibrovimo aptikimo sistemų) įjungimas ir išjungimas;

38.5.11. operacinėse sistemose vykstančių procesų ar paslaugų įvykiai;

38.5.12. TIS galinių įrenginių autentifikavimo įvykiai;

38.5.13. žurnalinių įrašų peržiūrėjimas, trynimas, kūrimas ar keitimas.

38.6. Pagrindinės TIS kompiuterinės įrangos dokumentacija saugoma ITD. Už jos atnaujinimą ir saugojimą atsakingas ITIS darbuotojas.

39. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

39.1. IS programinę ir kompiuterinę įrangą diegia finansų ministro paskirti atitinkamos IS administratoriai arba IS infrastruktūros administratoriai.

39.2. Slaptažodžiai, suteikiantys teisę dirbti su IS programine įranga, žinomi tik IS administratoriui (-iams). Slaptažodžiai, suteikiantys teisę dirbti su IS sistemine programine įranga, žinomi tik atitinkamos IS administratoriui ir IS infrastruktūros administratoriui (-iams).

39.3. Sisteminės ir taikomosios programinės įrangos atnaujinamos atsiradus jų saugumo spragoms, gavus gamintojo ar diegėjo rekomendacijas.

39.4. IS programinės įrangos atnaujinimai iš pradžių testuojami IS testinėje aplinkoje, ištestavus diegiami į darbinę IS aplinką, vadovaujantis kiekvienos IS priežiūros ir (ar) plėtros paslaugų teikimo reglamentu.

39.5. IS veikimo sutrikimo įvykiai fiksuojami elektroniniuose darbo protokoluose arba žurnaluose, kurie ne rečiau kaip vieną kartą per mėnesį peržiūrimi. Už elektroninių darbo protokolų arba žurnalų peržiūrą atsakingi atitinkamos IS administratoriai. Už peržiūros kontrolę atsako ITD Informacinių sistemų skyriaus vedėjas ar kito struktūrinio padalinio vadovas, kuriam pavaldus IS

administratorius. IS veikimo sutrikimo ir veiklos įvykių žurnaliniai įrašai turi būti saugomi ne trumpiau kaip 12 mėnesių nuo įrašo padarymo dienos.

40. Elektroninių ryšių tinklo saugumo užtikrinimo priemonės:

40.1. Ministerijos elektroninių ryšių tinklo sauga užtikrinama šiomis priemonėmis:

40.1.1. Pagrindiniai ministerijos kompiuterių tinklo komutaciniai mazgai turi būti išdėstyti atskirose rakinamose ministerijos patalpose. Teisė patekti į šias patalpas suteikiama ITD IS infrastruktūros administratoriams ir darbuotojui, atsakingam už telekomunikacijų tinklo priežiūrą.

40.1.2. Kitiems asmenims patekti į patalpas, kuriose išdėstyti pagrindiniai ministerijos kompiuterių tinklo komutaciniai mazgai, galima tik gavus ITD direktoriaus arba ITIS vadovo sutikimą ir tik lydimiems ITIS darbuotojo.

40.2. Prisijungti prie ministerijos kompiuterių tinklo naudojamos paskyros, saugomos katalogų tarnybos duomenų bazėje (angl. *active directory*), pagal kurias nustatomos ministerijos kompiuterių tinklo naudotojo teisės.

40.3. Taikomas ministerijos kompiuterių tinklo segmentavimas, jame atskiriant TIS valdymo ir administravimo potinklį, tinklinių daugiafunkcių įrenginių bei spausdintuvų ir skenerių potinklį, darbo vietų potinklį, testavimo potinklį, leidžiantis greitai keisti tinklo konfigūraciją ir užtikrinti kibernetinį saugumą.

40.4. Ministerijos kompiuterių tinklo kabeliai turi būti įmontuoti į specialius uždengtus lovelius.

40.5. Ministerijos kompiuterių tinklas įrengtas laikantis ne žemesnės kaip 5E kategorijos kompiuterių tinklams keliamų reikalavimų.

40.6. Ministerijos kompiuterių tinklo ir kitos įrangos išdėstymas fiksuojamas ITD saugomose schemose, kurios turi būti atnaujinamos, jei atliekami išdėstymo pakeitimai. Už schemų atnaujinimą atsakingas ITIS darbuotojas.

40.7. IS infrastruktūros administratorius, esant galimybei, privalo užtikrinti, kad būtų atsarginiai ministerijos kompiuterių tinklo komutacijos įrenginiai.

40.8. Ministerijoje nustatytas leistinas ministerijos kompiuterių tinklo adresų intervalas. Kiekvienam ministerijos kompiuteriui priskirtas ministerijos kompiuterių tinklo adresas yra fiksuojamas AIS.

40.9. Visos nenaudojamos ministerijos kompiuterių tinklo jungtys turi būti neaktyvios.

40.10. Perduodant IS informaciją viešaisiais kompiuterių tinklais, duomenų sauga turi būti užtikrinama naudojant šifravimą, saugųjį valstybinį duomenų perdavimo tinklą, virtualųjį privatų tinklą (angl. *virtual private network*) ar kitas kibernetinį saugumą užtikrinančias priemones.

40.11. Nuotolinis IS naudotojų prisijungimas prie IS leidžiamas per internetinę IS naudotojo sąsają, naudojant saugius duomenų perdavimo protokolus ir dviejų faktorių autentifikaciją.

41. Patalpų, kuriose saugoma ministerijos TIS, (ministerijos duomenų centras, IS tarnybinių stočių patalpos ir patalpos, kuriose saugomos atsarginės kopijos) saugumo užtikrinimo priemonės:

41.1. Įėjimas į šias patalpas apribotas elektroninėmis įeigos kontrolės priemonėmis ir patekimas į jas galimas tik teisę patekti į šias patalpas turintiems ministerijos darbuotojams (ITIS vadovui ir IS infrastruktūros administratoriams, kuriems pagal pareigybės reikalavimą yra pareiga užtikrinti TIS veikimą).

41.2. Įrengta ministerijos duomenų centro apsaugos sistema, prijungta prie bendros pastato apsaugos sistemos.

41.3. Ministerijos duomenų centro raktas (mechaniniam durų atidarymui) saugomas užklijuotame voke ministerijos pastato apsaugos poste (toliau – apsaugos postas). Šiuo raktu apsaugos darbuotojui leidžiama pasinaudoti tik vykdant instrukcijose nurodytus veiksmus, kai į ministerijos

duomenų centro patalpas negalima patekti naudojantis elektroniniu raktu. Pasinaudojęs mechaniniu raktu, apsaugos posto darbuotojas privalo informuoti ITIS vadovą.

41.4. Kiti asmenys į šias patalpas gali įeiti tik lydimi ITIS vadovo ar IS infrastruktūros administratoriaus. Ministerijos duomenų centre apsilankę asmenys registruojami Kibernetinio saugumo užtikrinimo taisyklių 4 priede nustatytos formos ministerijos duomenų centre apsilankiusių asmenų registravimo žurnale ministerijos duomenų centro lankytojų identifikavimo, registracijos ir apskaitos tikslais. Žurnalą pildo asmenis lydėję ITD darbuotojai, įgalioti patekti į ministerijos duomenų centrą.

41.5. Šiose patalpose įrengtos apsauginės langų žaliuzės (jei patalpoje yra langų).

41.6. Pagrindinė TIS kompiuterinė įranga, išskyrus kopijų tarnybines stotis, turi būti eksploatuojama specialiai tam įrengtose ministerijos duomenų centro patalpose, kuriose yra:

41.6.1. plieno lakštų nedegios durys be užrašų ant jų;

41.6.2. pašalinti daiktai, kurie neturėtų būti patalpoje pagal tos patalpos paskirtį;

41.6.3. įrengta techninių parametrų stebėjimo sistema;

41.6.4. įrengta dubliuota oro kondicionavimo ir vėdinimo sistema tinkamai temperatūrai ir tarnybinių stočių gamintojų nustatytam santykiniam oro drėgnumui palaikyti;

41.6.5. įrengta priešgaisrinės sistemos signalizacija, kurios davikliai įjungti į apsaugos poste esančią centralę, ir automatinės gaisro gesinimo sistemos, taip pat yra ugnies gesintuvai, skirti elektroninei įrangai gesinti;

41.6.6. elektros energijos tiekimo, vėdinimo ir klimato kontrolės, gaisro gesinimo ir gaisrinės saugos įranga, kuri prižiūrima laikantis šios įrangos gamintojo rekomendacijų, o šios įrangos techniniai patikrinimai atliekami ne rečiau kaip kartą per mėnesį.

41.7. Informacija ir pranešimai apie ministerijos duomenų centro įrangos veikimą teikiami apsaugos postui. Apsaugos poste esantis apsaugos darbuotojas privalo stebėti ministerijos duomenų centro įrangos veikimą kontroliuojančios specialios įrangos teikiamus pranešimus ir atlikti instrukcijose nurodytus veiksmus.

42. Visos kompiuterinės įrangos laikas turi būti sinchronizuojamas per ne mažiau kaip 2 vidines laiko tarnybines stotis, kurios savo ruožtu sinchronizuojamos su ne mažiau kaip 2 išorinėmis laiko tarnybinėmis stotimis.

43. ITIS vadovas yra atsakingas už ministerijos duomenų centro priežiūros instrukcijų atnaujinimą įvykus įrangos pokyčiams.

44. Programinės įrangos, skirtos TIS apsaugoti nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

44.1. IS tarnybinėse stotyse turi būti įdiegtos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai ir operatyviai atnaujinamos automatiniu būdu. Ilgiausias leidžiamas priemonių neatnaujinimo laikas – 5 darbo dienos. Kompiuterio operacinės sistemos kritinės pataisos diegiamos ne vėliau kaip per 5 darbo dienas nuo jų išleidimo dienos.

44.2. IS tarnybinėse stotyse, kuriose turi būti užtikrinta didelė greitaveika (pvz., duomenų bazių tarnybinės stotys) ir kurios yra izoliuotame kompiuterių tinklo segmente, kenksmingos programinės įrangos aptikimo priemonės gali būti nediegiamos.

44.3. Antivirusinės programinės įrangos virusų parašų bazės automatinio atnaujinimo ir kompiuterių operacinių sistemų kritinių pataisų diegimo terminai netaikomi toms KDV, kurios laikinai nenaudojamos. Pradėjus naudoti KDV, visos pataisos įdiegiamos per 3 darbo dienas.

45. Programinės įrangos, įdiegtos KDV ir tarnybinėse stotyse, naudojimo nuostatos:

45.1. Turi būti naudojama tik legali IS funkcijoms atlikti būtina programinė įranga.

45.2. Turi būti naudojama gamintojo palaikymą turinti programinė įranga.

45.3. Programinė įranga turi būti prižiūrima ir nuolat atnaujinama.

45.4. Operacinių sistemų ir taikomųjų programų sąranka parenkama tokiu būdu, kad būtų užtikrintas didžiausias saugumo lygis, sustabdomi nereikalingi darbui procesai.

45.5. IS naudotojų paskyros yra ribotų teisių, kurios neleidžia įdiegti papildomos programinės įrangos ir keisti sistemos, kompiuterio ar programinės įrangos sisteminių nustatymų, nebent tai nustatyta IS naudotojo pareigybės aprašyme. IS administratoriaus teisės gali būti suteikiamos išimties tvarka, pateikiant prašymą ITD, nurodant motyvuotą pagrindą.

45.6. Programinę įrangą diegia, atnaujina ir kontroliuoja IS infrastruktūros administratoriai arba IS administratoriai (pagal atliekamas funkcijas). Paslaugų teikėjai programinę įrangą gali atnaujinti tik dalyvaujant IS infrastruktūros administratoriui arba IS administratoriui.

45.7. Serveriuose, IS administratorių, IS infrastruktūros administratorių, ministerijos darbuotojų KDV naudojama ITD direktoriaus sprendimu į ministerijoje naudojamos tipinės programinės įrangos sąrašą įtraukta programinė įranga.

45.8. Programinės įrangos, nesusijusios su ministerijos veikla ar naudojamų IS funkcijomis, (žaidimų, bylų siuntimo, pokalbių programų ir pan.) naudojimas draudžiamas.

45.9. Programinės įrangos testavimas negali būti vykdomas su realiais ir (ar) asmens duomenimis, išskyrus būtinus atvejus, kai naudojamos organizacinės ir techninės duomenų saugumo priemonės, kuriomis užtikrinamas realių asmens duomenų saugumas. Priešingu atveju asmens duomenys turi būti nuasmeninami arba užšifruojami. Testavimui atlikti naudojamos testinės aplinkos.

45.10. Programinės įrangos atnaujinimai, prieš diegiant juos gamybinėje aplinkoje, turi būti ištestuoti testinėje aplinkoje.

45.11. Turi būti įgyvendinta prievolė sudaryti slaptažodžius vadovaujantis slaptažodžių sudarymo reikalavimais, nustatytais šiuo finansų ministro įsakymu patvirtintame Finansų ministerijos informacinių sistemų prieigų valdymo tvarkos apraše (toliau – IS prieigų valdymo tvarkos aprašas). IS naudotojų slaptažodžiai turi būti keičiami ne rečiau kaip kas 3 mėnesius, IS administratorių, IS infrastruktūros administratorių, IS veiklos administratorių ir vietinių IS naudotojų administratorių slaptažodžiai – ne rečiau kaip kas 2 mėnesius.

45.12. Turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie IS duomenų, atliktus veiksmus, tačiau šių veiksmų registravimas ir techninių įrašų tvarkymas nenaudojamas ministerijos darbuotojų veiklos, elgesio ar darbo našumo stebėsenai vykdyti. Šie duomenys tvarkomi tik tiek, kiek būtina programinės įrangos incidentų prevencijai, nustatymui, tyrimui ir jų padarinių šalinimui užtikrinti.

46. TIS kibernetinei saugai užtikrinti operacinių sistemų, TIS techninės įrangos žurnalinių įrašų saugojimo, fiksavimo ir analizės veiksmams registruoti skirti žurnaliniai įrašai turi būti saugomi ne trumpiau nei 12 mėnesių nuo įrašo padarymo dienos. Turi būti stebimas gaunamųjų ir siunčiamųjų tinklo duomenų srautas, antivirusinės programinės įrangos, įsibrovimų aptikimo ir prevencijos sistemos ar užkardos (saugasienės) veikimas, TIS konfigūracinių ir atsarginių kopijų failų prieigos ar pakeitimo veiksmų įrašai saugomi ir analizuojami tam pritaikytoje specializuotoje audito įrašų analizės ir saugojimo sistemoje (angl. *security information and event management*) (toliau – SIEM). Šioje sistemoje visi nurodyti veiksmai nepertraukiamai automatizuotu būdu stebimi, apie galimus nukrypimus nuo normalios srauto būsenos informuojamas paskirtas ministerijos saugumo operacijų centro (toliau – SOC) darbuotojas, atsakingas už žurnalinių įrašų stebėjimą ir reagavimą į incidentus.

47. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu, išskyrus laikino slaptažodžio perdavimą, kuris gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jeigu IS naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių IS naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

48. Draudžiama TIS techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti ir sudaryti pagal slaptažodžių sudarymo reikalavimus.

49. Ministerijos TIS veiklos tęstinumui užtikrinti TIS kompiuterinės įrangos administravimo slaptažodžius ir IS administravimo slaptažodžius saugo ITD direktorius atskiruose užklijuotuose vokuose. Ant voko pasirašo ITD direktorius ir IS infrastruktūros administratorius, o už IS slaptažodžius pasirašo atitinkamos IS administratorius. Saugomi duomenys atnaujinami pasikeitus slaptažodžiams. Už pateiktų saugoti slaptažodžių teisingumą atsako IS infrastruktūros ir IS administratorius (-iai).

50. Ministerijos TIS dokumentacija saugoma ITD. Už jos atnaujinimą ir saugojimą atsakingas atitinkamos IS administratorius ir IS infrastruktūros administratorius.

51. Kompiuterių tinklo ir tinklo filtravimo įrangos (užkardų (saugasienių), turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos:

51.1. TIS duomenų perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant užkardas, užkardų įvykių žurnalai turi būti reguliariai analizuojami.

51.2. Ypatingos svarbos ir svarbioms valstybės informacinių išteklių (toliau – VII) rūšims priskirtoms IS turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: struktūrizuotų užklausų kalbos įsiskverbties (angl. *SQL injection*), įterptinių instrukcijų atakų (angl. *cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), paskirstyto atsisakymo aptarnauti (angl. *DDOS*) ir kitos priemonės. Pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP)*) interneto svetainėje *www.owasp.org*.

51.3. TIS tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešajame ryšių tinkle naršančių TIS naudotojų kompiuterinę įrangą nuo kenksmingo kodo.

51.4. IS serveriai ir administruoti naudojami kompiuteriai negali turėti tiesioginio ryšio su internetu, jei toks ryšys nėra būtinas IS veikimui užtikrinti.

51.5. Prie ypatingos svarbos ir svarbioms VII rūšims priskirtų IS serveriai turi būti atskiruose loginiuose kompiuterių tinkluose. Vidinis ministerijos kompiuterių tinklas turi būti segmentuotas, jame atskiriant TIS valdymo ir administravimo potinklį, tinklinių daugiafunkcių įrenginių bei spausdintuvų ir skenerių potinklį, darbo vietų potinklį, testavimo potinklį.

51.6. Turi būti ribojama arba blokuojama prieiga prie operacinės sistemos prievadų.

51.7. Turi būti naudojama duomenų srautų analizės ir kontrolės įranga, padedanti nustatyti galimų informacijos saugos incidentų priežastis, taip pat naudojama saugos incidentų prevencijai.

52. Ypatingos svarbos ir svarbioms VII rūšims priskirtų IS tarnybinių stočių, kuriose yra svetainės, svetainių saugos parametrai turi būti teigiamai įvertinti naudojant NKSC rekomenduojamą testavimo priemonę.

53. IS ir (ar) jos infrastuktūros priežiūros funkcijas perduodant trečiajai šaliai Valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka, konkrečios IS programinės ir techninės įrangos keitimo ir (ar) atnaujinimo tvarka aprašoma paslaugų teikimo sutartyse.

54. Internetu prieinamos IS neturi rodyti IS naudotojui klaidų pranešimų apie IS programinį kodą ar serverį.

55. Turi būti uždrausta naršyti svetainės aplankuose (angl. *directory browsing*).

56. Turi būti įgyvendinti svetainės kriptografijos reikalavimai:

56.1. Turi būti naudojami oficialiai pripažinti saugaus ilgio raktai.

56.2. Atliekant svetainės administravimo darbus ryšio saugumas turi būti užtikrintas naudojant šifravimą ar virtualųjį privatų tinklą (angl. *virtual private network (VPN))*, turi būti naudojamas TLS (angl. *transport layer security*) standartas (1.3 versija arba naujesnė), oficialiai pripažinti saugaus ilgio raktai.

56.3. Šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų.

56.4. Pagal Kibernetinio saugumo reikalavimų apraše nustatytus reikalavimus turi būti naudojamas tinkamas TLS standartas.

56.5. Svetainės kriptografinės funkcijos turi būti įdiegtos serverio, kuriame yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. *hardware security module*).

56.6. Visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. *fail securely*).

57. Tarnybinėse stotyse draudžiama saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai.

58. Belaidžio tinklo naudojimas:

58.1. Naudojami tik techninius kibernetinio saugumo reikalavimus atitinkantys belaidžio tinklo įrenginiai.

58.2. Belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, kontroliuojamoje zonoje.

58.3. Prisijungti prie belaidžio tinklo turi būti taikomas ryšių ir IS naudotojų tapatumo patvirtinimo EAP (angl. *extensible authentication protocol*) arba TLS protokolas ir uždrausti visi nebūtini valdymo protokolai.

58.4. Belaidis ryšys turi būti šifruojamas pagal gerąją saugumo praktiką rekomenduojamu šifravimo ilgio raktu, naudojami visuotinai saugiais pripažįstami raktai ir protokolų versijos. Belaidės prieigos stotelėje turi būti pakeisti standartiniai gamintojo raktai.

59. Ministerijos darbuotojams suteikiamas nuotolinis prisijungimas prie ministerijos TIS:

59.1. Jungiantis prie ministerijos vidinio tinklo išteklių nuotoliniu būdu, turi būti naudojamas šifruotas prisijungimas ir papildomos tapatybės patvirtinimo priemonės – dviejų lygių autentifikacija.

59.2. Nuotolinio prisijungimo teisė ministerijos darbuotojams suteikiama vadovaujantis Nuotolinio darbo Lietuvos Respublikos finansų ministerijoje taisyklėmis, patvirtintomis Lietuvos Respublikos finansų ministro 2018 m. spalio 1 d. įsakymu Nr. 1K-331 „Dėl Nuotolinio darbo Lietuvos Respublikos finansų ministerijoje taisyklių patvirtinimo“, (toliau – Nuotolinio darbo taisyklės).

59.3. Viešaisiais ryšių tinklais perduodamos informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualųjį privatų tinklą (VPN).

59.4. Ministerijos darbuotojų nustatytų pareigų (funkcijų) ar dalies jų atlikimo darbo laiko ne nuolatinėje darbo vietoje sąlygos ir tvarka reglamentuota Nuotolinio darbo taisyklėse.

TREČIASIS SKIRSINIS
TIS DUOMENŲ SAUGOS UŽTIKRINIMAS

60. Tvarkyti TIS duomenis gali tik IS naudotojai, IS administratoriai, IS infrastruktūros administratoriai, IS veiklos administratoriai, vietiniai IS naudotojų administratoriai ir paslaugų, susijusių su IS, teikėjai, susipažinę su Saugumo politikos aprašu, Finansų ministerijos informacinių sistemų prieigų valdymo tvarkos aprašu ir sutikę laikytis juose nustatytų saugos reikalavimų.

61. IS duomenys įrašomi, atnaujinami, keičiami ir naikinami vadovaujantis IS nuostatais, Saugumo politikos aprašu, Kibernetinio saugumo užtikrinimo taisyklėmis ir kitais teisės aktais, reglamentuojančiais duomenų tvarkymą.

62. IS naudotojų duomenis įrašyti, keisti, atnaujinti gali tik IS administratorius, administruojantis IS naudotojus, arba vietinis IS naudotojų administratorius, jei tai numatyta IS nuostatuose.

63. IS naudotojų veiksmai automatiškai registruojami IS programinės įrangos elektroninių žurnalų įrašuose, kurie apsaugoti nuo neteisėto jame esančios informacijos panaudojimo, pakeitimo, iškraipymo ar sunaikinimo ir perduodami į centralizuotai valdomą SIEM. IS programinės įrangos elektroninių žurnalų įrašai prieinami tik atsakingiems SOC darbuotojams, IS administratoriams ir (arba) IS infrastruktūros administratoriams.

64. Saugaus duomenų perkėlimo ir teikimo susijusioms IS, duomenų gavimo iš jų užtikrinimo tvarka:

64.1. IS duomenys teikiami vadovaujantis Lietuvos Respublikos visuomenės informavimo įstatymu, Valstybės informacinių išteklių valdymo įstatymu ir Reglamentu (ES) 2016/679, IS nuostatais, Saugumo politikos aprašu ir kitais kibernetinio saugumo dokumentais.

64.2. IS valdytojas ir (arba) tvarkytojas sprendžia, ar duomenų gavėjas turi teisinį pagrindą gauti IS duomenis.

64.3. Jeigu duomenys teikiami pagal Valstybės informacinių išteklių valdymo įstatymo 28 straipsnio 4 dalies 1 punktą, IS duomenis teikia IS valdytojo ir (arba) tvarkytojo paskirti atsakingi ministerijos darbuotojai, raštu atsakydami į rašytinį duomenų gavėjo prašymą, nepriklausomai nuo to, kokia forma (popieriuje ar elektroninėse laikmenose) duomenys teikiami.

64.4. Jeigu duomenys teikiami pagal Valstybės informacinių išteklių valdymo įstatymo 28 straipsnio 4 dalies 2 ir (ar) 3 punktus, duomenys iš susijusių registrų, IS teikiami (arba gaunami) susijusiems registrams, IS tik pagal duomenų teikimo ir gavimo sutartis nustatant duomenų naudojimo tikslus ir sąlygas, duomenų teikimo ar gavimo būdus, laiką ir periodiškumą, perduodamų duomenų specifikacijas ir tvarką. Duomenų teikimo sutarties projektą rengia IS valdytojo ir (arba) tvarkytojo paskirti atsakingi ministerijos darbuotojai. Duomenų teikimo sutartis pasirašoma laikantis šių reikalavimų:

64.4.1. IS duomenys duomenų gavėjams perduodami vadovaujantis IS nuostatais ir kitais duomenų saugą užtikrinančiais ir reglamentuojančiais teisės aktais.

64.4.2. Duomenų teikėjai IS duomenis turi teikti teisės aktų nustatytais būdais, apimtimi, reguliarumu ir terminais.

64.4.3. Visi faktai apie keitimąsi duomenimis fiksuojami ir tvarkomi IS žurnaliniuose įrašuose, esančiuose IS elektroninėje duomenų bazėje (angl. *log files*), ir saugomi ne trumpiau kaip 12 mėnesių nuo šių įrašų padarymo pradžios.

64.4.4. Jeigu teikiami asmens duomenys, nurodomas asmens duomenų naudojimo tikslas, teikiamų asmens duomenų apimtis, asmens duomenų teikimo (gavimo) teisinis (-iai) pagrindas (-ai), asmens duomenų teikimo sąlygos ir tvarka, organizacinės ir techninės kibernetinio saugumo priemonės, asmens duomenų teikėjo ir gavėjo atsakomybės.

64.4.5. IS duomenų teikėjai ir (arba) gavėjai už duomenų tvarkymo teisėtumą ir gautų arba teikiamų duomenų saugą atsako teisės aktuose, reglamentuojančiuose saugų duomenų tvarkymą, nustatyta tvarka.

64.4.6. Duomenims teikti ir (ar) gauti iš kitų valstybės institucijų naudojamasi Kertinio valstybės telekomunikacijų centro teikiama paslauga – Saugiuoju valstybiniu duomenų perdavimo

tinklu (Saugusis tinklas) arba ribojant prieigą pagal IP adresą, jei teikėjas ar gavėjas nėra šio tinklo naudotojas.

64.5. Jeigu duomenys teikiami pagal Valstybės informacinių išteklių valdymo įstatymo 28 straipsnio 4 dalies 4 punktą, duomenų teikimo sutartys nesudaromos, o IS duomenų teikėjai ir (arba) gavėjai už duomenų tvarkymo teisėtumą ir gautų arba teikiamų duomenų saugą atsako teisės aktuose, reglamentuojančiuose saugų duomenų tvarkymą, nustatyta tvarka.

65. Prieigos prie IS duomenų teises gali suteikti IS administratorius arba vietinis IS naudotojų administratorius. IS naudotojams suteikiamos tik jų funkcijoms atlikti būtinos teisės.

66. IS naudotojai jungiasi prie IS naudodami tik IS programinę įrangą, technines ir programines priemones, užtikrinančias saugų duomenų perdavimą kompiuterių tinklais.

67. Prieigos prie IS duomenų valdymas reglamentuotas IS prieigos valdymo tvarkos apraše.

68. Prieiga prie IS suteikiama tik registruotiems ir turintiems teisę naudotis IS naudotojams.

69. IS naudotojui turi būti leista atlikti tik tuos veiksmus, kuriuos atlikti jam yra suteiktos teisės.

70. Visi IS naudotojo atliekami duomenų keitimo veiksmai fiksuojami žurnaliniuose įrašuose (angl. *log files*).

71. Neaktyvumo dirbant su IS laikas, kuriam pasibaigus IS naudotojų ryšio sesijos automatiškai nutraukiamos, nustatytas IS prieigos valdymo tvarkos apraše. Automatinis IS sesijos nutraukimas, tapatybės kodo blokavimas taikomi ten, kur tai leidžia naudojamos technologijos.

72. Kiekvienas atitinkamos IS tvarkytojas atsako už duomenų, kurie jam prieinami naudojant IS, tvarkymo teisėtumą ir tvarkomų duomenų saugą.

73. Pasibaigus IS naudotojo valstybės tarnybos santykiams ar darbo sutarčiai, teisė naudotis IS turi būti panaikinta. IS naudotojui prieiga prie IS turi būti ribojama ar sustabdoma, kai vyksta IS naudotojo veiklos tyrimas, IS naudotojas turi ilgesnės trukmės (motinystės, tėvystės) atostogas ar nedarbingumą, ilgesnį nei 2 mėnesiai, arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos.

74. Prieiga prie ministerijos IS programinio išeities kodo suteikiama tik IS priežiūros, plėtros ar palaikymo paslaugas teikiančio paslaugų teikėjo darbuotojui, pasirašiusiam asmens, dalyvaujančio vykdant sutartį, įsipareigojimą (Kibernetinio saugumo užtikrinimo taisyklių 5 priedas).

75. Siekiant apsaugoti nuo neteisėtos veikos – duomenų kopijavimo, keitimo, perdavimo ar naikinimo (toliau – neteisėta veika), naudojamos šios priemonės:

75.1. IS naudotojai, IS priežiūrą atliekantys paslaugų teikėjo darbuotojai, kilus įtarimui, kad naudojant IS duomenis vykdoma neteisėta veika, privalo nedelsdami apie tai informuoti IS administratorių. IS administratorius privalo reaguoti į tokį pranešimą, apie tai informuoti saugos įgaliotinį ir imtis visų įmanomų veiksmų, reikalingų neteisėtai veikai užkirsti.

75.2. IS administratorius privalo naudoti visas turimas ir įmanomas technines, programines ir administracines priemones, skirtas ministerijos tvarkomiems IS duomenims apsaugoti nuo neteisėtos veikos.

75.3. IS programinės įrangos veikimas stebimas automatizuotomis žurnalinių įrašų stebėjimo priemonėmis SOC ir Valstybinio duomenų centro (toliau – VDC) paslaugų teikėjo priemonėmis. Pastebėjus įtartiną veiklą apie tai informuojamas IS administratorius ir IS saugos įgaliotinis. SOC darbuotojas, atsakingas už žurnalinių įrašų stebėjimą, analizuodamas sisteminius saugumo įrašus, įvykių valdymo sistemos įrašus ir pastebėjęs įtartinus veiksmus IS, apie galimus saugos pažeidimus turi informuoti atitinkamų IS administratorius, saugos įgaliotinį ir kibernetinio saugumo vadovą.

75.4. Saugos įgaliotinis kasmet organizuoja patikrinimą, kurio metu ministerijoje patikrinama ne mažiau kaip dešimtadalis ministerijos IS naudotojų KDV, ar juose įdiegta programinė įranga įtraukta į leistinos programinės įrangos sąrašą.

76. Susirašinėjant el. paštu ar kitais ryšio kanalais siunčiama jautri ar nevieša informacija, taip pat informacija su asmens duomenimis turi būti užšifruota slaptažodžiu, kuris perduodamas kitu ryšio kanalu, nei siunčiami duomenys, (pvz., telefonu ar SMS žinute).

KETVIRTASIS SKIRSINIS
TIS DUOMENŲ ATSARGINIŲ KOPIJŲ VALDYMO TVARKA

77. Atsarginių duomenų kopijų darymo, tikrinimo, saugojimo ir duomenų atkūrimo iš atsarginių kopijų tvarka:

77.1. Ministerijos kopijavimo įrenginiai ir tam skirtos tarnybinės stotys neprieinami iš bendro ministerijos kompiuterių tinklo.

77.2. Jeigu IS nelaikomos VDC, IS duomenų atsargines kopijas kuria ir už jų teisingą duomenų atkūrimą iš IS duomenų atsarginių kopijų yra atsakingi atitinkamos IS administratoriai, priešingu atveju rezervinės kopijos daromos VDC paslaugos teikėjo pagal pasirašytas paslaugų teikimo sutartis.

77.3. IS duomenų atsarginės kopijos kuriamos arba iškart sukurtos perkeliamos į nutolusią tarnybinę stotį.

77.4. IS duomenų atsarginės kopijos, esančios nutolusioje tarnybinėje stotyje, įrašomos į išorines duomenų laikmenas (juosteles).

77.5. Nuolatinis atsarginių kopijų kūrimas vykdomas vadovaujantis ITD direktoriaus tvirtinamu atitinkamos IS atsarginių kopijų kūrimo procedūrų vadovu.

77.6. Už IS atsarginių kopijų kūrimo procedūrų vadovo parengimą ir atnaujinimą atsako atitinkamos IS administratorius.

77.7. IS atsarginių kopijų kūrimo procedūrų vadove turi būti nustatyta:

77.7.1.1. atsarginių kopijų kūrimo tvarka;

77.7.1.2. atsarginių kopijų kūrimo grafikas;

77.7.1.3. atsarginių kopijų tipai (angl. *full, incremental*);

77.7.1.4. atsarginių kopijų atkūrimo tvarka.

77.8. Nuolatinis sukurtų atsarginių kopijų įrašymas į išorines duomenų laikmenas atliekamas vadovaujantis ITD direktoriaus tvirtinamo Rezervinio kopijavimo į išorines laikmenas procedūrų vadovu.

77.9. Magnetinės ar kitos duomenų laikmenos, kuriose saugomos duomenų atsarginės kopijos, saugomos patalpoje, nutolusioje nuo ministerijos duomenų centro ir IS tarnybinių stočių patalpos, nedegiame metaliniame seife. Už atsarginių kopijų įrašymą į magnetines ar kitas duomenų laikmenas ir jų saugojimą atsakingas paskirtas IS infrastruktūros administratorius.

77.10. IS duomenų bazių tarnybines stotis ir dubliuojančią duomenų kopijavimo įrangą privaloma laikyti skirtingose ministerijos patalpose.

77.11. Duomenys iš atsarginių kopijų atkuriami vadovaujantis ITD direktoriaus tvirtinamu IS atsarginių kopijų kūrimo procedūrų vadovu.

77.12. IS veikla ir IT paslaugos atkuriamos vadovaujantis IS veiklos tęstinumo atkūrimo prioritetais, jei vienu metu sutrinka daugiau nei vienos IS veikla.

77.13. TIS veikla atkuriama vadovaujantis šiuo finansų ministro įsakymu patvirtintu Finansų ministerijos tinklų ir informacinių sistemų veiklos tęstinumo valdymo planu.

V SKYRIUS
TIS TIEKIMO GRANDINĖS SAUGUMO VALDYMUI, PASLAUGŲ, DARBŲ AR ĮRANGOS PIRKIMUI BEI ŠIŲ PASLAUGŲ TEIKĖJAMS TAIKOMI REIKALAVIMAI

78. Perkant su TIS, jų projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu susijusias paslaugas, darbus ar prekes, pirkimo dokumentuose nustatoma, kad šių paslaugų teikėjas, darbų vykdytojas ar prekių tiekėjas užtikrina jų atitiktį Kibernetinio saugumo reikalavimų apraše nustatytiems reikalavimams. Perkamos paslaugos, darbai ar prekės turi atitikti teisės aktų ir standartų, kuriais vadovaujamasi užtikrinant duomenų saugą ir kibernetinį saugumą, reikalavimus, kurie iš anksto nustatomi paslaugų teikimo, darbų atlikimo ar prekių tiekimo pirkimo dokumentuose.

79. Jeigu TIS priežiūros paslaugų teikėjas paslaugoms teikti pasitelkia trečiąją šalį, IS tvarkytojo ir paslaugų teikėjo sutartyje nustatyti saugumo reikalavimai turi būti taikomi ir trečiajai šaliai ir turi būti įtraukti į paslaugų teikėjo ir trečiosios šalies sutartį.

80. Ministerijos TIS kibernetinio saugumo priemonės, taip pat reikalavimai paslaugų teikėjui, paslaugų teikėjo atsakomybė, susijusi su TIS techninės ir (arba) programinės įrangos diegimu, nuoma ir priežiūra, paslaugos, būtinos TIS veikimui užtikrinti, nustatomi paslaugų teikimo sutartyje. Kartu nustatomi ir reikalavimai, keliami paslaugų teikėjų patalpoms, įrangai, TIS priežiūrai, duomenų perdavimui tinklais ir kitoms paslaugoms.

81. TIS priežiūros paslaugų sutartyse, kurios susijusios su prieigos suteikimu prie ministerijos TIS, juose esančių duomenų (įskaitant asmens duomenis) apdorojimu, perdavimu ar valdymu, turi būti nustatyti paslaugų teikėjų įsipareigojimai laikytis ministerijos TIS kibernetinio saugumo reikalavimų, ir pasirašomi Kibernetinio saugumo užtikrinimo taisyklių 5 priede nustatytos formos asmens, dalyvaujančio vykdant sutartį, įsipareigojimai. IS priežiūros paslaugas gali teikti tik šias paslaugų sutartis vykdančių paslaugų teikėjų darbuotojai ar paslaugų subteikėjų darbuotojai, pasirašę šį įsipareigojimą.

82. Pasikeitus sutarties sąlygoms, pasibaigus sutarčiai su IS priežiūros paslaugos teikėju ar atsiradus kitiems IS nuostatuose, kibernetinio saugumo dokumentuose nurodytų sąlygų pokyčiams, atsakingas už sutarties vykdymą asmuo privalo organizuoti TIS priežiūros paslaugos teikėjui suteiktos prieigos prie IS sąlygų atnaujinimą arba panaikinimą.

83. Prieš atliekant paslaugų, darbų ar įrangos, susijusių su TIS projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, įsigijimą, atsakingi ministerijos darbuotojai turi įvertinti veiklos poreikius, teisės aktų reikalavimus, kibernetinio saugumo reikalavimus. Norint įsigyti naujų prekių ar paslaugų turi būti parengti šioms prekėms ar paslaugoms taikomi techniniai reikalavimai, kibernetinio saugumo reikalavimai ir įsigijimo sąlygos.

84. Įsigyjamų TIS techniniai reikalavimai nustatomi techninėje specifikacijoje (toliau – specifikacija). Specifikacijoje turi būti nurodyti atliktos reikalavimų analizės rezultatai, numatytos TIS funkcinės galimybės, duomenų srautai ir sąsajų poreikiai, nustatyti funkciniai ir nefunkciniai reikalavimai, įskaitant kibernetinio saugumo reikalavimus. Specifikacijoje turi būti įtraukti privalomi apsaugos nuo kenkimo programinės įrangos (virusų, šnipinėjimo programų), filtravimo, pašto apsaugos, tinklo saugumo ir kiti kibernetinio saugumo reikalavimai.

85. Rengiamoje specifikacijoje turi būti nustatyti kibernetinio saugumo reikalavimai:

85.1. saugiam programavimui, jei TIS yra kuriamos;

85.2. saugumo sistemoms, skirtoms TIS apsaugoti nuo kenkimo programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.);

85.3. kompiuterių tinklo filtravimo įrangai (užkardų (saugasienių), turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.);

85.4. duomenų perdavimo tinklo saugumui;

85.5. kitoms priemonėms, naudojamoms kibernetiniam saugumui užtikrinti;

85.6. kiti kibernetinio saugumo reikalavimai, kurie ITD darbuotojų, atsakingų už IS priežiūrą, nurodomi kaip būtini, kad būtų įsigyta saugi TIS programinė ar techninė įranga.

86. Prekių ar paslaugų, reikalingų TIS priežiūrai, įsigijimo metu:

86.1. įsigyjamos tokios kūrimo paslaugos, kurios turi visiškai tenkinti specifikacijoje nustatytus saugaus programavimo reikalavimus;

86.2. įsigyjama tokia programinė ar techninė įranga, kuri turi visiškai tenkinti tokiai įrangai specifikacijoje nustatytus kibernetinio saugumo reikalavimus;

86.3. atliekami TIS programinės ar techninės įrangos diegimo ir konfigūravimo darbai, kurie turi visiškai tenkinti tokioms paslaugoms specifikacijoje nustatytus kibernetinio saugumo reikalavimus;

86.4. atliekami TIS programinės ar techninės įrangos testavimo testinėje aplinkoje veiksmai. Testavimo metu turi būti atliktas TIS programinės ar techninės įrangos bei programinio kodo saugumo vertinimas, kurio tikslas nustatyti esamas ir žinomas saugumo spragas. Testavimo rezultatai fiksuojami, neatitikimai šalinami prieš pradedant TIS programinės ar techninės įrangos bandomąjį eksploatavimą;

86.5. atliekamas TIS programinės ar techninės įrangos diegimas į gamybinę aplinką. Sukurtą produktą į gamybinę aplinką gali diegti tik įgalioti ministerijos darbuotojai ir (ar) trečiosios šalys, prižiūrimos įgaliotų ministerijos darbuotojų;

86.6. atliekamas TIS programinės ar techninės įrangos bandomasis eksploatavimas, kurio metu vertinamos programinės ar techninės įrangos funkcinės galimybės;

86.7. vykdomi TIS naudotojų mokymai;

86.8. rengiama TIS tinkamumo eksploatuoti ir kita dokumentacija.

87. Prekių ar paslaugų įsigijimas laikomas baigtu, kai ministerijos struktūriniai padaliniai ir atsakingi ministerijos darbuotojai patvirtina, kad TIS įsigijimas ir diegimas sėkmingai baigtas ir prekė ar paslauga yra saugi (visiškai atitinka specifikacijoje nustatytus kibernetinio saugumo reikalavimus) ir tinkama naudoti gamybinėje aplinkoje.

88. TIS eksploatavimo metu gamybinėje aplinkoje atliekama nuolatinė jų veikimo stebėsena, reguliariai atnaujinami filtrai, atliekami saugumo vertinimai ir rizikų analizė. Pokyčių valdymas vykdomas pagal Finansų ministerijos valdomų ir (arba) tvarkomų informacinių sistemų pokyčių valdymo tvarkos aprašo, patvirtinto Lietuvos Respublikos finansų ministro 2014 m. liepos 18 d. įsakymu Nr. 1K-224 „Dėl Finansų ministerijos valdomų ir (arba) tvarkomų informacinių sistemų pokyčių valdymo tvarkos aprašo patvirtinimo“, (toliau – Pokyčių valdymo tvarkos aprašas) nuostatas.

89. TIS eksploatavimo metu atsakingi ministerijos struktūriniai padaliniai, ministerijos darbuotojai ir (ar) trečiosios šalys, teikiančios TIS priežiūros paslaugas, turi užtikrinti nuolatinę jų priežiūrą, laiku reaguoti į jų sutrikimus ar neveikimą bei laiku šalinti atsiradusias klaidas, susijusias su TIS sutrikimais ar neveikimu.

90. TIS eksploatavimo metu periodiškai vykdomi TIS skenavimai.

91. TIS gyvavimo ciklo metu užtikrinant TIS įsigijimą, kūrimą, priežiūrą, plėtrą ir likvidavimą turi būti vadovaujamasi Lietuvos Respublikos teisės aktų, reglamentuojančių valstybės informacinių išteklių valdymą, reikalavimais, tarptautiniais standartais bei gerosiomis pasaulinėmis praktikomis. Už visų etapų įgyvendinimą turi būti paskirti atsakingi ministerijos darbuotojai, į atitinkamus etapus įtrauktas kibernetinio saugumo vadovas ar saugos įgaliotinis.

92. Paslaugų teikėjų prieigos prie TIS sąlygos:

92.1. IS administratorius ir IS infrastruktūros administratorius privalo supažindinti TIS priežiūros paslaugos teikėją su suteiktos prieigos prie TIS reikalavimais ir sąlygomis.

92.2. IS administratorius atsako už programinių, techninių ir kitų prieigos prie ministerijos TIS išteklių organizavimą, suteikimą ir panaikinimą ministerijos TIS priežiūros paslaugos teikėjui.

92.3. IS administratorius užtikrina, kad IS priežiūros paslaugų teikėjo darbuotojai nebūtų palikti vieni ministerijos patalpose.

92.4. IS administratorius ir IS infrastruktūros administratorius, esant poreikiui, suteikia TIS priežiūros paslaugos teikėjui tik tokią prieigą prie ministerijos TIS darbinės aplinkos tam tikram laikotarpiui konkretiems darbams atlikti, kuri yra būtina TIS priežiūros paslaugoms suteikti. Prieigos TIS priežiūros paslaugų teikėjui suteikimas ir (ar) panaikinimas registruojamas Kibernetinio saugumo užtikrinimo taisyklių 6 priede nustatytos formos prieigos prie ministerijos TIS žurnale. Žurnalą pildo prieigą suteikęs ir (ar) panaikinęs IS administratorius ar IS infrastruktūros administratorius.

VI SKYRIUS
TIS SAUGUMO SPRAGŲ VALDYMAS IR ATSKLEIDIMAS

93. Spragų valdymo objektai yra TIS elementai, esantys:

93.1. fiziniuose (įskaitant telkinius, angl. *cluster*) ir virtualiuosiuose serveriuose (toliau – Serveriai), esančiuose ministerijos patalpose arba trečiųjų šalių ar paslaugų teikėjų duomenų centre;

93.2. trečiųjų šalių debesijos infrastruktūroje (angl. *infrastructure as a service*, *IaaS*), kai tokias paslaugas užsako ministerija;

93.3. KDV techninėje įrangoje, kurią valdo ministerija;

93.4. programose (angl. *applications*), kurias valdo ministerija;

93.5. duomenų bazėse, kurias valdo ministerija;

93.6. tinklo techninėje įrangoje, kurią valdo ministerija;

93.7. įrenginiuose esančiuose valdikliuose ir davikliuose (daiktų interneto valdikliai ir davikliai (angl. *internet of things, IoT*)), kuriuos valdo ministerija.

94. Ministerija, atlikusi esminius valdomų ir tvarkomų TIS techninės ar programinės įrangos, programinio kodo, KDV ir kitos įrangos pakeitimus (pvz., TIS architektūros ar infrastruktūros keitimus, naujų modulių diegimą ar ženklų esamų modulių funkcinių galimybių keitimą, visų KDV operacinės įrangos diegimą ir pan.), perkeliant juos į gamybinę aplinką, savarankiškai ar su trečiųjų šalių pagalba turi nustatyti, įvertinti ir pašalinti juose esamas ar žinomas saugumo spragas, t. y. atlikti TIS saugumo vertinimą ir, esant poreikiui, atlikti kibernetinio saugumo rizikos vertinimą TIS rizikos vertinimo ir valdymo tvarkos apraše nustatyta tvarka.

95. Ministerijos TIS saugumo vertinimai turi būti atlikti kartu su TIS funkcinių galimybių, apkrovos ir (ar) kitais vertinimais ar iš karto po šių vertinimų.

96. Draudžiama ministerijoje atlikus TIS esminius pakeitimus TIS ir valdomas jų dalis (valdomą ir tvarkomą techninę ir programinę įrangą, programinį kodą, KDV ir kitą įrangą) diegti į gamybinę aplinką, prieš tai neatlikus jų saugumo vertinimo ar kibernetinio saugumo rizikos vertinimo.

97. Draudžiama ministerijos valdomą TIS techninę ir programinę įrangą, programinį kodą, tinklo įrangą, KDV ir kitą įrangą diegti į gamybinę aplinką, jei yra nustatyta kritinio ir aukšto rizikos lygio saugumo spragų ar apie jas žinoma.

98. TIS, KDV ir kitų vietų skenavimas ar kitų saugumo spragų nustatymo būdų (pvz., įsilaužimų testavimas) įgyvendinimas turi būti periodinis, o visų TIS spragų skenavimas,

vadovaujantis Kibernetinio saugumo įstatymo ir jo įgyvendinamųjų teisės aktų reikalavimais, turi būti atliekamas ne rečiau kaip kas 6 mėnesius. Kartu su TIS saugumo vertinimu taip pat turi būti atliktas ir elektroninio pašto saugumo vertinimas.

99. IS saugos įgaliotinis turi parengti ir su kibernetinio saugumo vadovu suderinti TIS spragų nustatymo planą. Spragų nustatymo plano pagrindu saugos įgaliotinis turi organizuoti saugumo vertinimus, esant poreikiui, tam pasitelkti paslaugų teikėjus, organizuodamas tokių paslaugų įsigijimus.

100. Už saugumo vertinimo įgyvendinimą yra atsakingas ministerijos darbuotojas, kuriam kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis paveda atlikti saugumo vertinimą, arba trečioji šalis, su kuria ministerija yra sudariusi paslaugų teikimo sutartį dėl kibernetinio saugumo vertinimo atlikimo.

101. Ministerijos valdomose TIS esamos ir žinomos saugumo spragos gali būti nustatomos pagal ministerijos valdomų TIS techninės ar programinės įrangos gamintojų, informacijos ir kibernetinio saugumo forumų ar kitų šaltinių, NKSC paviešinus atitinkamą informaciją, informaciją apie žinomas tokias techninės ar programinės įrangos saugumo spragas.

102. TIS saugumo vertinimai gali būti atliekami naudojant automatizuotus skenavimo įrankius (angl. *vulnerability management scanner*) (toliau – VMS) bei atitinkamus juodosios dėžės (angl. *blackbox*), pilkosios dėžės (angl. *graybox*) ar baltosios dėžės (angl. *whitebox*) metodus, taip pat naudojant nekomercinės organizacijos „Open Worldwide Application Security Project“ (OWASP) išleistą ir atnaujinamą saugumo spragų vertinimo (aktualios versijos) metodiką.

103. Draudžiama naudoti nepatikimus VMS įrankius (ir) nepatikimų gamintojų skurtus ir palaikomus VMS įrankius. TIS saugumo vertinimo metu naudojami VMS įrankiai turi būti suderinti su kibernetinio saugumo vadovu ar IS saugos įgaliotiniu.

104. TIS saugumo vertinimo metu, atliekant TIS skenavimą ar įsilaužimų testavimą, turi būti atliktas:

104.1. išorinio tinklo saugumo vertinimas – įsibrovimo iš interneto, išorės perimetro, žiniatinklio, interneto svetainių, mobiliųjų programų saugumo vertinimas;

104.2. vidinio tinklo saugumo vertinimas – vidinio tinklo bei vidiniame tinkle esančios techninės ir programinės įrangos ir informacinių technologijų paslaugų saugumo vertinimas;

104.3. KDV, belaidžio tinklo, spausdintuvų ir kitų vietų saugumo vertinimas;

104.4. pagal poreikį programinio kodo saugumo vertinimas.

105. Skenavimo metu, naudojant VMS įrankius, automatizuotai skenuojami tinklai ir informacinės sistemos, nustatomos esamos saugumo spragos, įvertinama, ar jos nėra netikros ir (ar) neteisingai identifikuotos (angl. *false positive*), ir, vadovaujantis TIS spragų vertinimo klasifikatoriumi (angl. *Common Vulnerability Scoring System)* (toliau – CVSS), parengtu pagal tarptautiniu mastu pripažintą tarptautinės organizacijos FIRST (angl. *Forum of Incident Response and Security Teams*) techninį standartą, skirtą TIS saugumo spragoms įvertinti (aktuali versija *https://www.first.org/cvss/v4-0/*), spragos priskiriamos atitinkamam rizikos lygiui, nurodytam lentelėje.

Lentelė. TIS saugumo spragų vertinimo pagal CVSS klasifikatorių balai ir spragų šalinimo laikas

Saugumo spragos rizikos lygis	**CVSS balas nuo–iki**	**Įtaka**	**Ilgiausias saugumo spragos šalinimo laikas nuo jos nustatymo momento**
Kritinis (angl. *critical*)	10–9	Neigiamai paveikiama visos ministerijos ir visų jos klientų veikla	3 kalendorinės dienos

Aukštas (angl. *high*)	8,9–7	Neigiamai paveikiama visos ministerijos ir kelių jos klientų veikla	15 kalendorinių dienų
Vidutinis (angl. *medium*)	6,9–4	Neigiamai paveikiami visi vidiniai ministerijos procesai ir (ar) visi ministerijos darbuotojai	30 kalendorinių dienų
Žemas (angl. *low*)	3,9–0,1	Neigiamai paveikiami keli vidiniai ministerijos procesai ir (ar) keli ministerijos darbuotojai	365 kalendorinės dienos

106. Įsilaužimų testavimas vykdomas papildomai naudojant VMS įrankius ir rankiniu būdu, tikrinant galimybes išnaudoti surastas saugumo spragas bei nustatant jų įtaką TIS.

107. Išorinio tinklo saugumo vertinimas turi apimti bent:

107.1. informacijos apie tikrinamą objektą surinkimą iš viešai prieinamų šaltinių. Informacija surenkama naudojantis įvairiomis paieškos sistemomis, programine įranga, interneto ištekliais, katalogais, viešomis duomenų bazėmis;

107.2. perimetro tinklo mazgų, pasiekiamų iš interneto, nustatymą;

107.3. perimetro tinklo mazguose veikiančių operacinių sistemų nustatymą ir atitinkamų iki šios dienos žinomų saugumo spragų patikrinimą;

107.4. perimetro tinklo mazguose veikiančių tarnybų nustatymą ir atitinkamų iki šios dienos žinomų saugumo spragų patikrinimą bei konfigūracijos analizę;

107.5. įsilaužimo testą, kuris atliekamas nustačius tinklo spragų;

107.6. išorinės paslaugos slaptažodžių auditą, jeigu aptinkama iš interneto pasiekiamų tarnybų, reikalaujančių vartotojo autentifikavimo, (tikrinama, ar naudojami patikimi slaptažodžiai, ar įmanoma juos atspėti arba parinkti, taip pat ar įmanoma atspėti TIS naudotojus);

107.7. antivirusinės sistemos galimybių susidoroti su žalingu kodu vertinimą;

107.8. tinklo mazgų atsparumo paslaugos trikdymo DoS (angl. *Denial of Service*) atakoms vertinimą.

108. Vidinio tinklo saugumo vertinimas turi apimti bent:

108.1. aktyvios tinklo įrangos konfigūracijos tikrinimą;

108.2. tarnybinių stočių saugumo tikrinimą;

108.3. KDV saugumo tikrinimą;

108.4. duomenų bazių valdymo sistemų tikrinimą;

108.5. svarbių slaptažodžių auditą – tikrinimą, ar naudojami patikimi slaptažodžiai, ar įmanoma juos atspėti arba parinkti.

109. TIS programinės įrangos saugumo įvertinimas turi apimti bent:

109.1. naudojamų technologijų (platformos, programavimo įrankių ir priemonių) identifikavimą;

109.2. paslaugų konfigūracijos tikrinimą (pvz., darbinės direktorijos pakeitimas, TIS naudotojų teisių padidinimas, informacijos atskleidimas per klaidų pranešimus ir pan.);

109.3. saugumo spragų paiešką (pvz., duomenų tikrinimas (angl. *input validation*), struktūruotos užklausų kalbos įterpimas (angl. *SQL injection*), buferio perpildymas (angl. *buffer overflow*) ir pan.) manipuliuojant pateikiamais duomenimis ar duomenų paketais ir įvertinant, kaip į iškraipytus duomenis reaguoja programinė įranga;

109.4. komunikacijų tarp skirtingų TIS elementų saugumo įvertinimą;

109.5. trūkumų ieškojimą tomis teisėmis ir sąlygomis, kuriomis dirba ministerijos darbuotojai ir (ar) trečiųjų šalių atstovai;

109.6. tinklalapių prieigos ir tinklo paslaugų (angl. *web service*) tikrinimą, kurį atliekant rankiniu būdu turi būti įvertinta bent:

109.6.1. įvairūs įterpimai (struktūruotos užklausų kalbos SQL, kompiuterinės žymėjimo kalbos XML, lengvos katalogų prieigos protokolo LDAP (angl. *lightweight directory access protocol*), dinaminės interpretuojamos programavimo kalbos PHP, komandų ir t. t.);

109.6.2. autorizacijos ir sesijos valdymo saugumas, perėmimo galimybės;

109.6.3. perduodamų ar priimamų duomenų perėmimo galimybės ir manipuliavimas jais;

109.6.4. TIS naudotojų teisės.

110. Atliekant KDV saugumo vertinimą turi būti įvertinta ne mažiau kaip 5 ministerijos TIS administratorių KDV, ne mažiau kaip 5 skirtingų tipų TIS naudotojų KDV ir ne mažiau kaip 5 skirtingų tipų TIS naudotojų darbo vietos.

111. Programinio kodo saugumo vertinimo metu turi būti automatizuotais VMS įrankiais ir rankiniu būdu įvertintas programinis kodas, norint nustatyti, ar jame nėra esamų ir (ar) žinomų saugumo spragų ar netinkamų konfigūracijų (pvz., angl. *backdoor*).

112. Informacija apie TIS spragas taip pat gali būti gauta iš išorės ir naudojama kaip tinkamas šaltinis, jei jos gavimo būdas visiškai atitinka Kibernetinio saugumo įstatymo 25 straipsnyje nustatytus reikalavimus.

113. Nustatytos TIS spragos turi būti vertinamos pagal CVSS klasifikatorių.

114. Atsakingas ministerijos darbuotojas ar paslaugų teikėjas, atlikęs ministerijos TIS saugumo vertinimą, turi parengti saugumo vertinimo ataskaitą, kurioje turi detaliai aprašyti nustatytas saugumo spragas, pateikdamas jų aptikimą patvirtinančius įrodymus, jų išnaudojimo galimybes ir rizikos lygį pagal CVSS klasifikatorių, kuris pateiktas Kibernetinio saugumo užtikrinimo taisyklių 105 punkto lentelėje.

115. Saugumo vertinimo ataskaitoje prie kiekvienos saugumo spragos taip pat privaloma pateikti išsamias nustatytų saugumo spragų pašalinimo rekomendacijas.

116. Saugos įgaliotinis su saugumo vertinimo ataskaita supažindina saugumo vertinimą inicijavusius ministerijos darbuotojus ir TIS, kuriuose nustatyta saugumo spragų, duomenų valdytojus, pagal saugumo vertinimo ataskaitą parengia spragų šalinimo planą, su kuriuo supažindina atitinkamos IS administratorius.

117. Saugumo vertinimo metu nustatytas saugumo spragas turi šalinti IS administratorius, atsakingas už tą sistemą, kurioje buvo nustatyta saugumo spragų, jei reikia, pasitelkdamas šios sistemos paslaugų teikėjus (jei sudaryta priežiūros ar vystymo paslaugų teikimo sutartis).

118. Kibernetinio saugumo vadovas ar saugos įgaliotinis TIS saugumo vertinimo metu nustatytas saugumo spragas registruoja ministerijos pagalbos tarnybos IS, kur informacija nuolat atnaujinama, siekiant užtikrinti tinkamą saugumo spragų valdymą.

119. Ministerijos darbuotojai, atsakingi už saugumo spragų šalinimą, organizuoja ir įgyvendina ministerijos TIS saugumo spragų šalinimą, vadovaudamiesi Kibernetinio saugumo užtikrinimo taisyklių 105 punkto lentelėje nurodytais saugumo spragų šalinimo terminais (kibernetinio saugumo vadovo ar saugos įgaliotinio sprendimu žemos rizikos saugumo spragos gali būti nešalinamos).

120. Jeigu TIS saugumo spragų šalinimo priemonių nėra, ministerijos darbuotojai, atsakingi už saugumo spragų šalinimą, pasitarę su saugos įgaliotiniu, planuoja ir įgyvendina kitas galimas saugumo spragų šalinimo priemones (pvz., kompensacines priemones), organizuoja naujų priemonių įsigijimą ar diegimą (pvz., prieigų teisių valdymo, įsilaužimų prevencijos, duomenų nutekinimo techninių priemonių ir kt.).

121. Ministerijos darbuotojai, atsakingi už TIS saugumo spragų šalinimą, negalėdami jose esančių saugumo spragų pašalinti per Kibernetinio saugumo užtikrinimo taisyklių 105 punkto lentelėje nustatytą terminą, turi apie tai informuoti IS saugos įgaliotinį bei su juo ir TIS, kuriuose yra

saugumo spraga, duomenų valdymo įgaliotiniais suderinti papildomą tokios spragos šalinimo terminą.

122. Visos TIS saugumo spragos, kurios įvertintos kaip itin reikšmingos TIS veiklai, turi būti pašalintos nedelsiant.

123. IS administratoriai, atsakingi už jiems paskirtų IS saugumo spragų šalinimą, organizuoja ir įgyvendina šių saugumo spragų šalinimo veiklas:

123.1. ištaiso techninės ar programinės įrangos klaidas ir atlieka reikiamas konfigūracijas, jei reikia, šiuo tikslu kreipiasi į paslaugų teikėjus ir koordinuoja paslaugų teikėjų atliekamus techninės ar programinės įrangos klaidų šalinimo ir nustatytų konfigūracijų keitimo veiklas, užtikrina jų įgyvendinimo kontrolę;

123.2. apriboja TIS, kuriuose yra esama ar žinoma saugumo spraga, pasiekiamumą;

123.3. atnaujina programinę įrangą, vadovaudamiesi Pokyčių valdymo tvarkos apraše nustatyta tvarka ir terminais;

123.4. paruošia ir su atitinkamos IS duomenų valdymo įgaliotiniais suderina konfigūracijų keitimo planą bei užtikrina jo įgyvendinimą;

123.5. inicijuoja reikiamų techninių priemonių įsigijimą, koordinuoja jų diegimą ir užtikrina diegimo kontrolę;

123.6. pagal poreikį atlieka kitas saugumo spragų šalinimo veiklas.

124. Kai dar nėra programinės įrangos atnaujinimo iš gamintojo ar taikomos priemonės visiškai nepašalina saugumo spragos, ar saugumo spragos švelninimo veiksmai turi įtaką kitiems ministerijos valdomiems tinklams ar IS, atlikus kibernetinio saugumo rizikos vertinimą, tokia IS gali būti naudojama su nepašalinta saugumo spraga tik saugos įgaliotinio ar kibernetinio saugumo vadovo sprendimu, tokį sprendimą suderinus su TIS, kuriuose yra saugumo spraga, duomenų valdymo įgaliotiniais.

125. Ministerijos darbuotojai, atsakingi už TIS saugumo spragų šalinimą, pašalinę saugumo spragą, turi ministerijos pagalbos tarnybos IS sukurti atitinkamus įrašus, o apie pašalintas kritinio ir aukšto rizikos lygio saugumo spragas papildomai nedelsdami informuoti saugos įgaliotinį.

126. Saugos įgaliotinis TIS saugumo spragų šalinimo eigos procesą turi tikrinti tokiu dažnumu:

126.1. kritinio rizikos lygio saugumo spragos šalinimo eigos procesą – 1 kartą per parą;

126.2. aukšto rizikos lygio saugumo spragos šalinimo eigos procesą – 1 kartą kas 3 paras;

126.3. vidutinio rizikos lygio saugumo spragos šalinimo eigos procesą – 1 kartą per savaitę;

126.4. žemo rizikos lygio saugumo spragos šalinimo eigos procesą – 1 kartą kas 3 mėnesius.

127. Ministerijos darbuotojai, atsakingi už IT turto valdymą, siekdami, kad ministerijos valdomi TIS būtų tinkamai apsaugoti nuo saugumo spragų, turi tinkamai įgyvendinti IT valdymo procesus (pakeitimų, konfigūracijų ir sąrankos valdymą, pataisymų valdymą, saugų programavimą ir kitus informacinių technologijų valdymo procesus). Pagal kompetenciją saugos įgaliotinis konsultuoja ministerijos darbuotojus, atsakingus už IT turto valdymą, šių procesų įgyvendinimo metu.

VII SKYRIUS
KIBERNETINIO SAUGUMO MOKYMŲ ORGANIZAVIMAS

128. Kibernetinio saugumo vadovas turi užtikrinti, kad ne rečiau kaip kartą per metus visi ministerijos darbuotojai išklausytų kibernetinio saugumo higienos praktikos mokymus.

129. Ministerijos darbuotojų kibernetinio saugumo mokymai planuojami struktūriniam padaliniui, atsakingam už personalo valdymą, parengiant ir finansų ministrui teikiant tvirtinti metinį

ministerijos darbuotojų mokymų planą. Jame turi būti numatyti bendrieji kibernetinio saugumo higienos praktikos mokymai visiems ministerijos darbuotojams, vykdomi gyvai ir (ar) nuotoliniu būdu, prisijungiant prie NKSC mokymų platformos ir išlaikant praktinių įgūdžių testą.

130. IS saugos įgaliotinis per 3 mėnesius nuo kibernetinio saugumo mokymų pradžios parengia, o kibernetinio saugumo vadovas patvirtina mokymų ataskaitą, kurioje turi būti nurodyta mokymų tema, dalyvių skaičius. Mokymų ataskaita saugoma ne mažiau kaip 3 metus nuo jos patvirtinimo datos.

131. Kibernetinio saugumo vadovas ir (arba) IS saugos įgaliotinis informuoja ministerijos darbuotojus apie kibernetinio saugumo aktualijas:

131.1. el. paštu siunčia saugumo pranešimus ar rekomendacijas;

131.2. aktualijas skelbia ministerijos intranete;

131.3. pristato informaciją reguliarių susirinkimų metu;

131.4. informacinę medžiagą skelbia ministerijos patalpose esančiose bendrose erdvėse.

132. Bent vieną kartą per metus ITD Kibernetinio saugumo skyriaus darbuotojai organizuoja ministerijos darbuotojų socialinės inžinerijos pratybas, kurių metu darbuotojai praktiškai supažindinami su kibernetinio saugumo grėsmėmis ir aktualijomis. Po šių pratybų rengiamos ataskaitos, su kuriomis supažindinami visi ministerijos darbuotojai.

133. IS valdytojas užtikrina tinkamą IS saugos įgaliotinio, IS administratorių, IS infrastruktūros administratorių, IS veiklos administratorių ir IS vidinių naudotojų kvalifikacijos tobulinimą, atsižvelgdamas į kibernetinio saugumo užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), IS saugos įgaliotinio, IS administratorių, IS infrastruktūros administratorių ir IS vidinių naudotojų poreikius.

134. SOC darbuotojai turi būti išklausę saugumo specialistams skirtą kursą NKSC mokymų platformoje ir išlaikę praktinių įgūdžių testą.

135. Finansų ministras ir ministerijos kancleris privalo ne rečiau kaip kartą per 2 metus NKSC vadovo nustatyta tvarka išklausyti kibernetinio saugumo mokymus ir užtikrinti ministerijos darbuotojų nuolatinį švietimą kibernetinio saugumo srityje.

_____

Finansų ministerijos tinklų ir
informacinių sistemų bei juose esančių
duomenų kibernetinio saugumo
užtikrinimo taisyklių
1 priedas

FINANSŲ MINISTERIJOS INFORMACINIŲ SISTEMŲ PRISKYRIMO VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ RŪŠIAI SĄRAŠAS

Eil. Nr.	**Informacinės sistemos pavadinimas**	**Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme nurodytų valstybės informacinių išteklių rūšis**	**Informacinės sistemos poveikio lygis**	**Informacinės sistemos priskyrimo valstybės informacinių išteklių rūšiai kriterijai**
1.	Valstybės biudžeto, apskaitos ir mokėjimų sistema (VBAMS)	Ypatingos svarbos	1	Vadovaujantis Valstybės informacinių išteklių svarbos nustatymo metodikos, patvirtintos Lietuvos Respublikos ekonomikos ir inovacijų ministro 2023 m. liepos 19 d. įsakymu Nr. 4-418 „Dėl Valstybės informacinių išteklių svarbos nustatymo metodikos patvirtinimo“, (toliau – Metodika) 8.5.1 papunkčiu
2.	Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinė sistema (VSAKIS)	Ypatingos svarbos	1	Vadovaujantis Metodikos 8.5.1 papunkčiu
3.	Europos Sąjungos struktūrinės paramos kompiuterinė informacinė valdymo ir priežiūros sistema (SFMIS)	Svarbi	2	Vadovaujantis Metodikos 8.5.2 papunkčiu
4.	Strateginio valdymo informacinė sistema (SVIS)	Vidutinės svarbos	3	Vadovaujantis Metodikos 8.5.3 papunkčiu
5.	Atvirųjų finansų informacinė sistema (AFIS)	Mažos svarbos	4	Vadovaujantis Metodikos 8.5.4 papunkčiu

_____

Finansų ministerijos tinklų ir informacinių sistemų bei juose esančių duomenų kibernetinio saugumo užtikrinimo taisyklių 2 priedas

(Asmens, prižiūrinčio Finansų ministerijos informacinę sistemą arba besinaudojančio ja, įsipareigojimo forma)

_____

(asmens, prižiūrinčio Finansų ministerijos informacinę sistemą arba besinaudojančio ja, vardas ir pavardė)

ASMENS, PRIŽIŪRINČIO FINANSŲ MINISTERIJOS INFORMACINĘ SISTEMĄ ARBA BESINAUDOJANČIO JA,
ĮSIPAREIGOJIMAS

20 m. _____ d.
Vilnius

Prižiūrėdamas (-a) Lietuvos Respublikos finansų ministerijos (toliau – ministerija)_____

_____

(informacinės sistemos pavadinimas)

informacinę sistemą (toliau – IS) arba besinaudodamas (-a) IS:

1. *suprantu, kad:*

1.1. savo darbe tvarkysiu duomenis, įskaitant asmens duomenis, kurie negali būti atskleisti ar perduoti neįgaliotiems asmenims ar institucijoms;

1.2. man draudžiama perduoti neįgaliotiems asmenims slaptažodžius ir kitus duomenis, leidžiančius programinėmis ir techninėmis priemonėmis sužinoti duomenis ar kitaip sudaryti sąlygas susipažinti su IS tvarkoma elektronine informacija;

1.3. man draudžiama perduoti neįgaliotiems asmenimis įstaigoje ar už jos ribų duomenis, dokumentus ir (arba) jų kopijas ar kitaip sudaryti sąlygas susipažinti su duomenimis, dokumentais, jų kopijomis;

1.4. visa informacija apie fizinius ir juridinius asmenis, išskyrus Lietuvos Respublikos mokesčių administravimo įstatymo 38 straipsnio 2 dalyje nurodytas išimtis, yra nevieša;

1.5. Mokesčių administravimo įstatymo 38 straipsnio 2 dalyje nurodytą informaciją tretiesiems asmenims gali atskleisti tik mokesčių administratorius;

1.6. netinkamas duomenų tvarkymas gali užtraukti atsakomybę Lietuvos Respublikos įstatymų, reglamentuojančių saugų duomenų tvarkymą, nustatyta tvarka;

2. *įsipareigoju:*

2.1. tvarkyti asmens duomenis vadovaudamasis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (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 asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais, reglamentuojančiais saugų asmens duomenų tvarkymą;

2.2. neatskleisti, neviešinti, neperduoti IS tvarkomų duomenų ir nesudaryti sąlygų sužinoti jų nė vienam asmeniui, kuris nėra įgaliotas naudotis šiais duomenimis tiek įstaigos viduje, tiek už jos ribų;

2.3. susipažinti su IS kibernetinės saugos dokumentais ir sutinku laikytis jų reikalavimų;

2.4. visus prieigai prie IS skirtus naudotojų vardus, slaptažodžius ir kitą IS duomenų saugą užtikrinančią informaciją, kuri man taps žinoma, saugoti ir naudoti IS duomenis įstatymų,

reglamentuojančių saugų duomenų tvarkymą, ir kitų teisės aktų nustatyta tvarka;

2.5. saugoti IS duomenų paslaptį, jei ji neskirta skelbti viešai (įsipareigojimas saugoti duomenų paslaptį galioja ir perėjus dirbti į kitas pareigas, ir nutraukus ar pasibaigus valstybės tarnybos, darbo ar sutartiniams santykiams);

2.6. pranešti apie suteiktų prieigos teisių panaikinimą, jei nėra poreikio naudotis atitinkama IS;

2.7. pranešti ministerijos saugos įgaliotiniui apie bet kokią įtartiną situaciją, galinčią kelti grėsmę IS duomenų saugumui;

3. *esu susipažinęs (-usi)* su:

3.1. Reglamentu (ES) 2016/679, Asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais, reglamentuojančiais asmens duomenų teisinę apsaugą;

3.2. TIS kibernetinio saugumo dokumentais, kurie skelbiami *https://finmin.lrv.lt/lt/paslaugos/ministerijos-is-saugos-dokumentai*:

3.2.1. Finansų ministerijos tinklų ir informacinių sistemų kibernetinio saugumo politikos aprašu, patvirtintu Lietuvos Respublikos finansų ministro 2026 m. balandžio d. įsakymu Nr. 1K- „Dėl kibernetinio saugumo Finansų ministerijoje“;

3.2.2. Finansų ministerijos informacinių sistemų prieigų valdymo tvarkos aprašu, patvirtintu Lietuvos Respublikos finansų ministro 2026 m. balandžio d. įsakymu Nr. 1K- „Dėl kibernetinio saugumo Finansų ministerijoje“;

4. *žinau, kad:*

4.1. už šio įsipareigojimo nesilaikymą, Reglamento (ES) 2016/679 ir Asmens duomenų teisinės apsaugos įstatymo pažeidimą pagal Lietuvos Respublikos įstatymus kyla drausminė, civilinė, administracinė arba baudžiamoji atsakomybė;

4.2. asmuo, patyręs žalą dėl neteisėto asmens duomenų tvarkymo arba kitų duomenų valdytojo ar duomenų tvarkytojo veiksmų ar neveikimo, turi teisę reikalauti atlyginti jam padarytą turtinę ar neturtinę žalą Reglamento (ES) 2016/679, Asmens duomenų teisinės apsaugos įstatymo ir kitų Lietuvos Respublikos teisės aktų nustatyta tvarka;

4.3. IS naudotojai, pažeidę šį įsipareigojimą ir kitų saugų duomenų tvarkymą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka;

4.4. šis įsipareigojimas galios visą mano darbo laiką šioje įstaigoje, perėjus dirbti į kitas pareigas ir nutraukus ar pasibaigus valstybės tarnybos, darbo ar sutartiniams santykiams.

_____ _____

(parašas) (vardas ir pavardė)

_____

Finansų ministerijos tinklų ir informacinių sistemų bei juose esančių duomenų kibernetinio saugumo užtikrinimo taisyklių 3 priedas

(Tinklų ir informacinių sistemų kompiuterinės įrangos gedimų registravimo žurnalo forma)

LIETUVOS RESPUBLIKOS FINANSŲ MINISTERIJA

TINKLŲ IR INFORMACINIŲ SISTEMŲ KOMPIUTERINĖS ĮRANGOS GEDIMŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Gedimo registravimo data ir laikas	Gedimo apibūdinimas / aprašymas	Gedimą užregistravo (vardas, pavardė, parašas)	Gedimo pašalinimo data ir laikas	Šalinant gedimą atlikti veiksmai / darbai	Gedimą pašalino (vardas, pavardė, parašas)
1.						
2.						
3.						

_____

Finansų ministerijos tinklų ir
informacinių sistemų bei juose esančių
duomenų kibernetinio saugumo
užtikrinimo taisyklių
4 priedas

(Finansų ministerijos duomenų centro patalpose apsilankiusių asmenų registravimo žurnalo forma)

LIETUVOS RESPUBLIKOS FINANSŲ MINISTERIJA

FINANSŲ MINISTERIJOS DUOMENŲ CENTRO PATALPOSE APSILANKIUSIŲ ASMENŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Įmonė / organizacija, vardas, pavardė	Atvykimo tikslas	Atvykimo data ir laikas	Išvykimo laikas ir parašas	Lydėjo (vardas, pavardė, parašas)
1.					
2.					
3.					

_____

Finansų ministerijos tinklų ir informacinių sistemų bei juose esančių duomenų kibernetinio saugumo užtikrinimo taisyklių 5 priedas

(Asmens, dalyvaujančio vykdant sutartį, įsipareigojimo forma)

_____

(paslaugų teikėjo įmonės kodas ir pavadinimas)

_____

(paslaugų teikėjo darbuotojo (eksperto) vardas ir pavardė)

ASMENS, DALYVAUJANČIO VYKDANT SUTARTĮ, ĮSIPAREIGOJIMAS

20____ m. _____d.
Vilnius

Dalyvaudamas (-a) vykdant Lietuvos Respublikos finansų ministerijos (toliau – ministerija) ir

_____

(paslaugų teikėjo pavadinimas)

sutartį _____

(sutarties sudarymo data, sutarties pavadinimas, Nr.)

_____,

1. *suprantu, kad:*

1.1. vykdant sutartį tvarkysiu duomenis, įskaitant asmens duomenis, kurie negali būti atskleisti ar perduoti neįgaliotiems asmenims ar institucijoms, įstaigoms;

1.2. man draudžiama perduoti neįgaliotiems asmenims slaptažodžius ir kitus duomenis, kurie man taps žinomi vykdant sutartį, kurie leistų programinėmis ir techninėmis priemonėmis sužinoti duomenis ar kitaip sudaryti sąlygas susipažinti su ministerijos informacinėje sistemoje (toliau – IS) tvarkomais duomenimis;

1.3. man draudžiama perduoti neįgaliotiems asmenimis duomenis, dokumentus ir (arba) jų kopijas ar kitaip sudaryti sąlygas susipažinti su duomenimis, dokumentais, jų kopijomis;

1.4. visa informacija apie fizinius ir juridinius asmenis, išskyrus Lietuvos Respublikos mokesčių administravimo įstatymo 38 straipsnio 2 dalyje nurodytas išimtis, yra nevieša;

1.5. Mokesčių administravimo įstatymo 38 straipsnio 2 dalyje nurodytą informaciją tretiesiems asmenims gali atskleisti tik mokesčių administratorius;

1.6. netinkamas duomenų tvarkymas gali užtraukti atsakomybę Lietuvos Respublikos įstatymų, reglamentuojančių saugų duomenų tvarkymą, nustatyta tvarka;

2. *įsipareigoju:*

2.1. tvarkyti asmens duomenis vadovaudamasis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (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 asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais, reglamentuojančiais saugų asmens duomenų tvarkymą;

2.2. neatskleisti, neviešinti, neperduoti IS tvarkomų duomenų ir nesudaryti sąlygų sužinoti jų nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija;

2.3. susipažinti su tinklų ir informacinių sistemų kibernetinės saugos dokumentais ir sutinku

laikytis jų reikalavimų;

2.4. visus prieigai prie IS skirtus naudotojų vardus, slaptažodžius ir kitą ministerijos duomenų saugą užtikrinančią informaciją, kuri man taps žinoma vykdant sutartį, saugoti ir naudoti įstatymų, reglamentuojančių saugų duomenų tvarkymą, ir kitų teisės aktų nustatyta tvarka;

2.5. saugoti patikėtų ar tapusių žinomų IS duomenų paslaptį, jei ji neskirta skelbti viešai (įsipareigojimas saugoti duomenų paslaptį galioja tiek šios sutarties vykdymo metu, tiek šiai sutarčiai pasibaigus, tiek pasibaigus mano darbo ar kitokiems santykiams su paslaugų teikėju);

2.6. teikdamas (-a) paslaugas pagal sutarties reikalavimus įgyvendinti tinkamas organizacines ir technines saugos priemones, skirtas IS duomenims nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo apsaugoti;

2.7. duomenis, programines ir technines priemones, suteikiančias galimybę naudotis IS duomenimis, bet kokia forma naudoti tik sutartyje nustatytoms užduotims vykdyti;

2.8. pranešti ministerijos saugos įgaliotiniui apie bet kokią įtartiną situaciją, galinčią kelti grėsmę IS duomenų saugumui;

3. *esu susipažinęs (-usi)* su:

3.1. Reglamentu (ES) 2016/679, Asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais, reglamentuojančiais asmens duomenų teisinę apsaugą;

3.2. TIS kibernetinį saugumą užtikrinančiais dokumentais, kurie skelbiami *https://finmin.lrv.lt/lt/paslaugos/ministerijos-is-saugos-dokumentai*:

3.2.1. Finansų ministerijos tinklų ir informacinių sistemų kibernetinio saugumo politikos aprašu, patvirtintu Lietuvos Respublikos finansų ministro 2026 m.balandžio d. įsakymu Nr. 1K- „Dėl kibernetinio saugumo Finansų ministerijoje“;

3.2.2. Finansų ministerijos informacinių sistemų prieigų valdymo tvarkos aprašu, patvirtintu Lietuvos Respublikos finansų ministro 2026 m. balandžio d. įsakymu Nr. 1K- „Dėl kibernetinio saugumo Finansų ministerijoje“;

4. *žinau, kad:*

4.1. už šio įsipareigojimo nesilaikymą, Reglamento (ES) 2016/679 ir Asmens duomenų teisinės apsaugos įstatymo pažeidimą pagal Lietuvos Respublikos įstatymus kyla drausminė, civilinė, administracinė arba baudžiamoji atsakomybė;

4.2. asmuo, patyręs žalą dėl neteisėto asmens duomenų tvarkymo arba kitų duomenų valdytojo ir (arba) duomenų tvarkytojo veiksmų ar neveikimo, turi teisę reikalauti atlyginti jam padarytą turtinę ar neturtinę žalą Reglamento (ES) 2016/679, Asmens duomenų teisinės apsaugos įstatymo ir kitų Lietuvos Respublikos teisės aktų nustatyta tvarka;

4.3. pažeidęs šį įsipareigojimą ir kitas duomenų tvarkymą reglamentuojančių teisės aktų nuostatas, atsakysiu įstatymų nustatyta tvarka;

4.4. šis įsipareigojimas galios tiek šios sutarties vykdymo metu, tiek šiai sutarčiai pasibaigus, tiek pasibaigus mano darbo ar kitokiems santykiams su paslaugų teikėju;

5. *patvirtinu*, kad nesu baustas (-a) už duomenų praradimą, atskleidimą, sunaikinimą ir kitokius neteisėtus veiksmus su duomenimis. Įsipareigoju raštu informuoti ministeriją, jeigu tokie atvejai išaiškėja sutarties vykdymo metu.

_____ _____

(parašas) (vardas ir pavardė)

Paslaugos teikėjo atstovas,
atsakingas už sutarties vykdymą _____ _____

(parašas) (vardas ir pavardė)

_____

Finansų ministerijos tinklų ir
informacinių sistemų bei juose esančių
duomenų kibernetinio saugumo
užtikrinimo taisyklių
6 priedas

(Prieigos prie Finansų ministerijos tinklų ir informacinių sistemų darbinės aplinkos tinklų ir informacinių sistemų priežiūros paslaugų teikėjui suteikimo ir (ar) panaikinimo registravimo žurnalo forma)

LIETUVOS RESPUBLIKOS FINANSŲ MINISTERIJA

PRIEIGOS PRIE FINANSŲ MINISTERIJOS TINKLŲ IR INFORMACINIŲ SISTEMŲ DARBINĖS APLINKOS TINKLŲ IR INFORMACINIŲ SISTEMŲ PRIEŽIŪROS PASLAUGŲ TEIKĖJUI SUTEIKIMO IR (AR) PANAIKINIMO REGISTRAVIMO ŽURNALAS

Eil. Nr.	Kam suteikta prieiga (vardas, pavardė, įstaiga)	Prieigos suteikimo tikslas (numatomi atlikti darbai)	Prieigos suteikimo data ir laikas	Prieigą suteikė (vardas, pavardė, parašas)	Prieigos panaikinimo data ir laikas	Prieigą panaikino (vardas, pavardė, parašas)
1.						
2.						
3.						

_____