Suvestinė redakcija nuo 2024-04-26

Įsakymas paskelbtas: TAR 2018-04-20, i. k. 2018-06345

Nauja redakcija nuo 2023-01-03:
Nr. 3D-789, 2022-12-09, paskelbta TAR 2022-12-09, i. k. 2022-25175

LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTRAS

ĮSAKYMAS
DĖL VALSTYBĖS ĮMONĖS ŽEMĖS ŪKIO DUOMENŲ CENTRO ADMINISTRUOJAMŲ INFORMACINIŲ SISTEMŲ IR REGISTRŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2018 m. balandžio 19 d. Nr. 3D-235
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 12, 19 ir 26 punktais bei Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2023 m. liepos 19 d. nutarimu Nr. 576 „Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo“, 4 ir 7 punktais:

Preambulės pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

1. T v i r t i n u Valstybės įmonės Žemės ūkio duomenų centro administruojamų informacinių sistemų ir registrų duomenų saugos nuostatus (pridedama).

2. P a v e d u :

2.1. valstybės įmonei Žemės ūkio duomenų centrui:

2.1.1. per 10 darbo dienų nuo šio įsakymo įsigaliojimo dienos paskirti administruojamų Lietuvos Respublikos žemės ūkio ir kaimo verslo registro, Lietuvos Respublikos ūkininkų ūkių registro, Lietuvos Respublikos traktorių, savaeigių ir žemės ūkio mašinų ir jų priekabų registro, Ūkinių gyvūnų registro, Lietuvos Respublikos pašarų ūkio subjektų registro, Žemdirbių mokymo ir konsultavimo informacinės sistemos, Paraiškų priėmimo informacinės sistemos, Lietuvos žemės ūkio ir maisto produktų rinkos informacinės sistemos, Paramos žemės ūkio veiklos subjektams apskaičiavimo informacinės sistemos, Pieno apskaitos informacinės sistemos, Ūkinių gyvūnų veislininkystės informacinės sistemos, Traktorininko pažymėjimų informacinės sistemos, Žemės ūkio veiklą vykdančių ūkio subjektų patikrinimo aktų informacinės sistemos, Žemės išteklių stebėsenos informacinės sistemos ir Žemės ūkio ir maisto produktų sertifikavimo informacinės sistemos saugos įgaliotinį ir administratorių (-ius);

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

2.1.2. paskirti kompetentingą asmenį ar padalinį, atsakingus už kibernetinio saugumo organizavimą ir užtikrinimą;

2.1.3. saugos įgaliotiniui pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai rizikos vertinimo ir atitikties vertinimo rezultatus Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka;

2.2. šio įsakymo vykdymą kontroliuoti žemės ūkio viceministrui pagal administravimo sritį.

Žemės ūkio ministras Bronius Markauskas

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2018-03-29 raštu Nr. IS-(4.2)6K-142

SUDERINTA
Valstybės įmonės Žemės ūkio informacijos ir
kaimo verslo centro
2018-03-28 raštu Nr. 1S-2148

PATVIRTINTA
Lietuvos Respublikos žemės ūkio ministro
2018 m. balandžio 19 d. įsakymu Nr. 3D-235
(Lietuvos Respublikos žemės ūkio ministro
2022 m. gruodžio 9 d. įsakymo Nr. 3D-789 redakcija)

VALSTYBĖS ĮMONĖS ŽEMĖS ŪKIO DUOMENŲ CENTRO ADMINISTRUOJAMŲ INFORMACINIŲ SISTEMŲ IR REGISTRŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybės įmonės Žemės ūkio duomenų centro (toliau – Centras) administruojamų informacinių sistemų ir registrų duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato Centro administruojamų informacinių sistemų ir registrų (toliau – IS / registrai) saugos politiką, organizacines, technines, programines, teisines ir kitas priemones, užtikrinančias saugų IS / registrų duomenų tvarkymą.

2. Saugos nuostatų reikalavimai taikomi administruojant Centro IS / registrus, nurodytus Centro administruojamų IS / registrų sąraše (priedas).

3. Centro administruojamų IS / registrų saugos politika įgyvendinama pagal Saugos nuostatus ir Lietuvos Respublikos žemės ūkio ministro įsakymu (ar įsakymais) tvirtinamus Centro administruojamų IS / registrų saugos politikos įgyvendinimo dokumentus (toliau – Saugos dokumentai):

3.1. Saugaus elektroninės informacijos tvarkymo taisykles;

3.2. Informacinės sistemos naudotojų administravimo taisykles;

3.3. Informacinės sistemos veiklos tęstinumo valdymo planą.

4. Saugos nuostatuose vartojamos sąvokos:

4.1. **elektroninė informacija** – duomenys, dokumentai ir informacija, tvarkomi Centro administruojamose IS / registruose;

4.2. **IS / registrų administratorius** – Centro darbuotojas, paskirtas prižiūrėti IS / registrus ir (ar) jų infrastruktūrą, užtikrinanti jų veikimą, elektroninės informacijos saugą (kibernetinį saugumą), ar kitas asmuo (asmenų grupė), kuriam (kuriai) Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos informacinių sistemų ir (ar) jų infrastruktūros priežiūros funkcijos;

4.3. **IS / registrų komponentai** – kompiuteriai, operacinės sistemos, duomenų bazės ir jų valdymo sistemos, taikomųjų programų sistemos, užkardos, įsilaužimų aptikimo ir prevencijos sistemos, elektroninės informacijos perdavimo tinklai, duomenų saugyklos, bylų serveriai ir kita

techninė ir programinė įranga, kurios pagrindu funkcionuoja informacinės sistemos ir užtikrinama jose tvarkomos elektroninės informacijos sauga (kibernetinis saugumas);

4.4. **IS / registrų naudotojų administratorius** – Centro paskirtas darbuotojas, administruojantis IS / registrų naudotojų prieigos teisių valdymą ir atliekantis kitas teisės aktų nustatytas funkcijas;

4.5. **saugos įgaliotinis** – Centro paskirtas darbuotojas, dirbantis pagal darbo sutartį, ar padalinys, koordinuojantis ir prižiūrintis elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimą IS / registruose;

4.6. **kibernetinio saugumo specialistas** – Centro paskirtas darbuotojas, dirbantis pagal darbo sutartį, atliekantis IS / registrų pažeidžiamų vietų nustatymo, saugumo reikalavimų atitikties nustatymo, stebėsenos ir reagavimo funkcijas;

4.7. **kibernetinio saugumo vadovas** – Centro paskirtas darbuotojas, dirbantis pagal darbo sutartį, ar padalinys, atsakingas už IS / registrų kibernetinio saugumo organizavimą ir užtikrinimą;

4.8. Kitos Saugos nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše ir Saugos dokumentų turinio gairių apraše, patvirtintuose Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas), ir kituose teisės aktuose bei ISO 27000 serijos standartuose.

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

5. IS / registrų tvarkomos elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo tikslai:

5.1. sudaryti sąlygas saugiai automatizuotu būdu tvarkyti IS / registrų elektroninę informaciją;

5.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

5.3. vykdyti elektroninės informacijos saugos (kibernetinių) incidentų prevenciją, reaguoti į elektroninės informacijos saugos (kibernetinius) incidentus ir juos operatyviai suvaldyti, atkuriant įprastą IS / registrų veiklą.

6. IS / registrų informacijos saugai (kibernetiniam saugumui) užtikrinti naudojamos organizacinės, techninės, programinės ir fizinės informacijos apsaugos priemonės.

7. IS / registrų elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetinės kryptys:

7.1. IS / registrų elektroninės informacijos konfidencialumo užtikrinimas;

7.2. IS / registrų elektroninės informacijos vientisumo užtikrinimas;

7.3. IS / registrų elektroninės informacijos prieinamumo užtikrinimas;

7.4. asmens duomenų apsauga;

7.5. IS / registrų veiklos tęstinumo užtikrinimas;

7.6. prieigos prie IS / registrų kontrolė;

7.7. IS / registrų rizikos valdymas;

7.8. IS / registrų naudotojų mokymas elektroninės informacijos saugos (kibernetinio saugumo) klausimais;

7.9. organizacinių, techninių, programinių, teisinių, informacijos sklaidos ir kitų priemonių, skirtų elektroninės informacijos saugai (kibernetiniam saugumui) užtikrinti, įgyvendinimas ir kontrolė.

8. Saugos nuostatai taikomi:

8.1. IS / registrų valdytojai – Lietuvos Respublikos žemės ūkio ministerijai (toliau – ŽŪM), Gedimino pr. 19, 01103 Vilnius;

8.2. IS / registrų tvarkytojui – Centrui, V. Kudirkos g. 18-1, 03105 Vilnius;

8.3. saugos įgaliotiniui;

8.4. kibernetinio saugumo vadovui;

8.5. kibernetinio saugumo specialistui;

8.6. IS / registrų naudotojams;

8.7. IS / registrų administratoriams (kompiuterinių tinklų administratoriui, tarnybinių stočių administratoriui ir duomenų bazių administratoriui);

8.8. IS / registrų naudotojų administratoriams.

9. ŽŪM funkcijos:

9.1. metodiškai vadovauti Centro veiklai kuriant ir diegiant IS / registrus, koordinuoti IS / registrų funkcionavimą;

9.2. pagal kompetenciją rengti ir priimti teisės aktus, užtikrinančius IS / registrų duomenų tvarkymo teisėtumą ir IS / registrų elektroninės informacijos saugą (kibernetinį saugumą), atlikti teisės aktų nuostatų laikymosi priežiūrą;

9.3. rengti IS / registrų biudžeto projektus;

9.4. koordinuoti Centro darbą, nustatyta tvarka atlikti veiklos priežiūrą;

9.5. atlikti IS / registrų elektroninės informacijos tvarkymo ir elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų laikymosi priežiūrą ir kontrolę;

9.6. nagrinėti Centro pasiūlymus dėl IS / registrų veiklos, elektroninės informacijos saugos (kibernetinio saugumo), juos apibendrinti ir priimti dėl IS / registrų tobulinimo;

9.7. priimti sprendimus dėl IS / registrų techninių ir programinių priemonių, būtinų IS / registrų elektroninės informacijos saugai (kibernetiniam saugumui) užtikrinti, įsigijimo, diegimo ir modernizavimo;

9.8. pavesti Centrui skirti IS / registrų saugos įgaliotinį, kibernetinio saugumo vadovą, IS / registrų administratorius ir IS / registrų naudotojų administratorius;

9.9. atlikti kitas Saugos nuostatuose, IS / registrų nuostatuose ir kituose teisės aktuose pavestas funkcijas.

10. Centro funkcijos:

10.1. užtikrinti nepertraukiamą IS / registrų veikimą (prieinamumą);

10.2. užtikrinti IS / registrų elektroninės informacijos saugą (kibernetinį saugumą) ir saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais (automatiniu būdu);

10.3. užtikrinti IS / registrų sąveiką su susijusiais registrais ir informacinėmis sistemomis;

10.4. užtikrinti IS / registrų duomenų atsarginių kopijų darymą;

10.5. pagal kompetenciją užtikrinti IS / registrų veiklos tęstinumą;

10.6. užtikrinti veiksmingą ir spartų IS / registrų pokyčių valdymo planavimą;

10.7. užtikrinti IS / registrų taikomajai programinei įrangai, tarnybinėms stotims ir juose esantiems duomenims funkcionuoti būtinos informacinių technologijų infrastruktūros (toliau – serverių sritis) saugą;

10.8. tvirtinti Centro rizikų tvarkymo priemonių įgyvendinimo planą, priimti sprendimus dėl IS / registrų rizikos vertinimo rezultatų;

10.9. prireikus tvirtinti IS / registrų informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

10.10. rengti ir saugoti serverių srities saugai užtikrinti būtiną dokumentaciją;

10.11. sudaryti IS / registrų duomenų gavimo ir teikimo sutartis ir užtikrinti duomenų gavimo ir teikimo saugą;

10.12. sudaryti galimybes duomenų teikėjams teikti duomenis elektroniniu būdu;

10.13. užtikrinti IS / registrų elektroninės informacijos saugą (kibernetinį saugumą);

10.14. skirti saugos įgaliotinį, kibernetinio saugumo vadovą, IS / registrų administratorius, IS / registrų naudotojų administratorius;

10.15. teikti ŽŪM pasiūlymus dėl IS / registrų elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo;

10.16. rengti ir įgyvendinti techninių ir programinių priemonių kūrimo ir plėtros planus, investicinius projektus;

10.17. ne rečiau kaip kartą per metus organizuoti kibernetinio saugumo dokumentų persvarstymą (peržiūrėjimą);

10.18. organizuoti IS / registrų naudotojams mokymus elektroninės informacijos saugos (kibernetinio saugumo) klausimais;

10.19. informuoti Nacionalinį kibernetinio saugumo centrą apie įvykusius kibernetinius incidentus ir taikytas šių incidentų valdymo Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, nustatyta tvarka;

10.20. teikti Valstybinei duomenų apsaugos inspekcijai informaciją apie kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių incidentų valdymo priemones;

10.21. teikti policijai ar kitoms ikiteisminį tyrimą atliekančioms Lietuvos institucijoms informaciją, reikalingą kibernetiniams incidentams, turintiems nusikalstamos veikos požymių, užkardyti ir tirti;

10.22. vykdyti kitas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Centro IS / registrų nuostatuose bei saugos dokumentuose nustatytas funkcijas.

11. Saugos įgaliotinio funkcijos ir atsakomybė:

11.1. teikti Centro vadovui pasiūlymus dėl:

11.1.1. IS / registrų administratorių, IS / registrų naudotojų administratorių paskyrimo ir reikalavimų jiems nustatymo;

11.1.2. Centro informacinių technologijų saugos atitikties vertinimo atlikimo;

11.1.3. Saugos dokumentų priėmimo, keitimo ir panaikinimo;

11.2. koordinuoti elektroninės informacijos saugos (kibernetinio saugumo) incidentų tyrimą ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos (kibernetinio saugumo) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetinio saugumo) incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos (kibernetinio saugumo) darbo grupės;

11.3. teikti kibernetinio saugumo vadovui, kibernetinio saugumo specialistui, IS / registrų administratoriams, IS / registrų naudotojų administratoriams ir IS / registrų naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Centro patvirtintos Informacijos saugumo politikos (toliau – Informacijos saugumo politika) įgyvendinimu;

11.4. organizuoti IS / registrų naudotojų supažindinimą su IS / registrų saugos dokumentais, užtikrinti supažindinimo įrodomumą;

11.5. koordinuoti IS / registrų saugos dokumentų reikalavimų vykdymą;

11.6. organizuoti IS / registrų rizikos ir informacinių technologijų saugos atitikties vertinimą;

11.7. organizuoti IS / registrų naudotojams mokymus elektroninės informacijos saugos (kibernetinio saugumo) klausimais;

11.8. atlikti kitas šiuose Saugos nuostatuose, kituose teisės aktuose nustatytas ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, saugos įgaliotiniui priskirtas funkcijas.

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

12. Kibernetinio saugumo specialistas atlieka kibernetinių atakų imitavimo veiksmus, IS / registrų pažeidžiamų vietų nustatymo, saugą užtikrinančių pagrindinių komponentų būklės, saugumo reikalavimų atitikties nustatymo ir stebėsenos, reagavimo į elektroninės informacijos saugos incidentus funkcijas.

13. Kibernetinio saugumo vadovas atlieka Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše ir kituose teisės aktuose nustatytas funkcijas. Kibernetinio saugumo vadovas ir saugos įgaliotinis gali būti tas pats asmuo.

14. Saugos įgaliotinis ir kibernetinio saugumo vadovas negali atlikti IS / registrų administratoriaus funkcijų.

15. Kompiuterinių tinklų administratorius atlieka šias funkcijas:

15.1. užtikrina kompiuterinių tinklų veikimą;

15.2. projektuoja kompiuterinius tinklus;

15.3. diegia, konfigūruoja ir prižiūri kompiuterinių tinklų aktyviąją įrangą;

15.4. užtikrina kompiuterinių tinklų saugumą (nustato pažeidžiamas vietas);

15.5. pagal kompetenciją reaguoja į elektroninės informacijos saugos (kibernetinio saugumo) incidentus ir juos valdo, atlieka įsilaužimų į IS / registrus aptikimo funkcijas;

15.6. administruoja ugniasienes, maršrutizatorius, komutatorius ir pagalbinę įrangą (nepertraukiamo maitinimo šaltinius, fizines linijas ir pan.).

16. Tarnybinių stočių administratorius atlieka šias funkcijas:

16.1. užtikrina tarnybinių stočių veikimą;

16.2. konfigūruoja tarnybinių stočių tinklo prieigą;

16.3. stebi ir analizuoja tarnybinių stočių veiklą;

16.4. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

16.5. diegia tarnybinių stočių programinės įrangos atnaujinimus;

16.6. pagal kompetenciją reaguoja į elektroninės informacijos saugos (kibernetinio saugumo) incidentus ir juos valdo, atlieka įsilaužimų į IS / registrus aptikimo funkcijas;

16.7. užtikrina tarnybinių stočių saugą.

17. Duomenų bazių administratorius atliekas šias funkcijas:

17.1. užtikrina duomenų bazių veikimą;

17.2. tvarko duomenų bazių programinę įrangą;

17.3. diegia duomenų bazių programinės įrangos atnaujinimus;

17.4. kuria ir atkuria atsargines elektroninės informacijos kopijas;

17.5. stebi duomenų bazes ir optimizuoja jų funkcionavimą;

17.6. pagal kompetenciją reaguoja į elektroninės informacijos saugos (kibernetinio saugumo) incidentus ir juos valdo, atlieka įsilaužimų į IS / registrus aptikimo funkcijas;

17.7. atlieka IS / registrų pažeidžiamų vietų nustatymo, saugumo reikalavimų atitikties nustatymo ir stebėsenos funkcijas.

18. IS / registrų administratoriai yra atsakingi už tinkamą kibernetinio saugumo dokumentuose nustatytų funkcijų vykdymą.

19. IS / registrų administratoriai privalo vykdyti visus saugos įgaliotinio ir kibernetinio saugumo vadovo nurodymus ir pavedimus dėl IS / registrų elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo, pagal kompetenciją reaguoti į elektroninės informacijos saugos (kibernetinio saugumo) incidentus ir nuolat teikti saugos įgaliotiniui ir kibernetinio saugumo vadovui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

20. Atlikdami IS / registrų sąrankos pakeitimus, IS / registrų administratoriai turi laikytis pokyčių valdymo tvarkos, nustatytos ŽŪM tvirtinamose Centro administruojamų informacinių sistemų ir registrų saugaus elektroninės informacijos tvarkymo taisyklėse.

21. IS / registrų administratoriai privalo patikrinti (peržiūrėti) IS / registrų sąranką ir IS / registrų būsenos rodiklius reguliariai – ne rečiau kaip kartą per metus ir (arba) po IS / registrų pokyčio.

22. IS / registrų administratoriai privalo atlikti kitas Saugos nuostatuose ir kituose saugos dokumentuose pavestas funkcijas.

23. IS / registrų administratoriai gali būti skiriami kelioms IS / registrams, posistemiams, funkciškai savarankiškoms sudedamosioms dalims ar tam tikroms IS / registrų administratoriaus funkcijoms atlikti.

24. IS / registrų naudotojų administratorius atlieka IS / registrų naudotojų teisių valdymo funkcijas (IS / registrų naudotojų duomenų administravimas, klasifikatorių tvarkymas, IS / registrų naudotojų veiksmų, registracijos žurnalų įrašų analizė ir kt.).

25. IS / registrų naudotojų administratoriaus funkcijos:

25.1. vykdyti prieigų prie IS / registrų suteikimą;

25.2. vykdyti IS / registrų teisių valdymą;

25.3. redaguoti IS / registrų naudotojų teises;

25.4. atlikti kitas Saugos nuostatuose ir kituose saugos dokumentuose pavestas funkcijas.

26. IS / registrų naudotojo funkcijos:

26.1. atsakyti už IS / registrų ir joje tvarkomų duomenų saugumą;

26.2. tvarkyti IS / registrų elektroninę informaciją;

26.3. neatskleisti, neperduoti tvarkomos IS / registrų elektroninės informacijos;

26.4. atlikti kitas Saugos nuostatų, IS / registrų nuostatų ir kitų teisės aktų nustatytas funkcijas.

27. Teisės aktai, kuriais vadovaujamasi tvarkant IS / registrų elektroninę informaciją ir užtikrinant jos saugą:

27.1. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (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);

27.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

27.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

27.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

27.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“;

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

27.6. 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“;

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

27.7. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

27.8. ISO 27000 serijos standartai, reglamentuojantys informacijos saugą;

27.9. kiti teisės aktai, reglamentuojantys IS / registrų elektroninės informacijos tvarkymą, elektroninės informacijos saugą (kibernetinį saugumą) bei ŽŪM ir Centro veiklą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

28. Centro administruojamose IS / registruose tvarkomos elektroninės informacijos svarbos rūšys nurodytos Saugos nuostatų priede.

Punkto pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

29. Centro administruojamose IS / registruose automatiniu būdu tvarkomi asmens duomenys priskiriami antrajam saugumo lygiui.

30. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, kasmet organizuoja / atlieka IS / registrų rizikos vertinimą. Kartu su IS / registrų rizikos vertinimu ir (arba) šių Saugos nuostatų 39 punkte ir jo papunkčiuose nurodytu informacinių technologijų saugos atitikties vertinimu turi būti atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos IS / registrų kibernetiniam saugumui, vertinimas.

31. Rizikos vertinimas atliekamas vertinant rizikos veiksnius, galinčius turėti įtakos IS / registrų elektroninės informacijos saugai (kibernetiniam saugumui), jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai:

31.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

31.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis IS / registrais elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymas, saugos pažeidimai, vagystės ir kita);

31.3. 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.

32. Pagrindinės nuostatos dėl rizikos veiksnių vertinimo:

32.1. IS / registrų rizikos vertinimą inicijuoja Centras;

32.2. IS / registrų rizika nustatoma periodinio rizikos vertinimo metu;

32.3. IS / registrų rizikos vertinimas atliekamas ne rečiau kaip kartą per metus;

32.4. saugos įgaliotinis yra atsakingas už IS / registrų rizikos vertinimo atlikimo organizavimą / atlikimą;

32.5. IS / registrų rizikos veiksniai vertinami taikant Centro patvirtintą Rizikos valdymo tvarkos aprašą.

33. IS / registrų rizikos vertinimas atliekamas vadovaujantis:

33.1. Vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“;

33.2. Informacijos saugumo politika;

33.3. Centro patvirtintu Rizikos valdymo tvarkos aprašu;

33.4. ISO/IEC 27001 ir kitais Lietuvos ir tarptautiniais standartais, reglamentuojančiais rizikos vertinimą.

34. Rizikos valdymo procesą sudaro rizikos vertinimo konteksto nustatymas, rizikos vertinimas (informacinių išteklių inventorizacija ir jų įtakos Centro veiklai vertinimas, rizikos analizė, rizikos įvertinimas), rizikos tvarkymas ir rizikos stebėsena, ir peržiūra.

35. IS / registrų rizikos vertinimo rezultatai išdėstomi elektroniniame Rizikų valdymo registre (saugomame excel formatu), kuris kartu su Rizikų tvarkymo planu (saugomu excel formatu) peržiūrimas, įvertinamas ir tvirtinamas kasmetinio Rizikos valdymo darbo grupės susitikimo metu.

36. Rizikų tvarkymo plane numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

37. IS / registrų saugos užtikrinimo priemonės parenkamos vadovaujantis:

37.1. Lietuvos Respublikos kibernetinio saugumo įstatymu;

37.2. *Neteko galios nuo 2024-04-26*

Papunkčio naikinimas:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

37.3. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu;

37.4. Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2023 m. liepos 19 d. nutarimu Nr. 576 „Dėl Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašo patvirtinimo“, nustatančiu būtinas priemones pagal informacinei sistemai priskirtą saugos rūšį;

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

37.5. Vidaus reikalų ministerijos išleista metodine priemone „Rizikos analizės vadovas“;

37.6. kitų elektroninės informacijos saugą reglamentuojančių Lietuvos Respublikos teisės aktų, nustatančių būtinas priemones pagal informacinei sistemai priskirtą kategoriją, reikalavimais;

37.7. ISO/IEC 27001 standarte išdėstytomis rekomendacijomis ir siūlymais.

38. Elektroninės informacijos saugos (kibernetinio saugumo) būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis IS / registrų elektroninės informacijos saugos (kibernetinio saugumo) priemonėmis, kurios pasirenkamos atsižvelgiant į Centro turimus išteklius, vadovaujantis šiais principais:

38.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

38.2. elektroninės informacijos saugos (kibernetinio saugumo) priemonės diegimo kaina turi būti proporcinga saugomos elektroninės informacijos vertei;

38.3. atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegtos prevencinės, detekcinės ir korekcinės elektroninės informacijos saugos (kibernetinio saugumo) priemonės.

39. Rizikos vertinimo ataskaitos ir rizikos tvarkymo plano kopijas saugos įgaliotinis ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – ARSIS) Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

Punkto pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

40. Siekiant užtikrinti saugos dokumentuose nustatytų elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų įgyvendinimo organizavimą ir kontrolę, turi būti organizuojamas IS / registrų informacinių technologijų saugos atitikties vertinimas:

40.1. IS / registrų saugos atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje, patvirtintoje Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, nustatyta tvarka. Atlikus informacinių technologijų saugos atitikties vertinimą, saugos įgaliotinis rengia ir teikia Centro generaliniam direktoriui informacinių technologijų saugos vertinimo ataskaitą. Atsižvelgdamas į Informacinių technologijų saugos atitikties vertinimo ataskaitą, saugos įgaliotinis prireikus parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina Centro generalinis direktorius;

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

40.2. IS / registrų informacinių technologijų saugos atitikties vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip. Pirmosios kategorijos IS / registrų informacinių technologijų saugos atitikties vertinimą ne rečiau kaip kartą per trejus metus turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai;

40.3. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas saugos įgaliotinis ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikia ARSIS Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka;

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

40.4. IS / registrų atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše nustatytų organizacinių ir techninių kibernetinio saugumo reikalavimų vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus;

40.5. IS / registrų informacinių technologijų saugos atitikties vertinimo metu turi būti atliekamas kibernetinių atakų imitavimas ir vykdomos kibernetinių incidentų imitavimo pratybos. Imituojant kibernetines atakas rekomenduojama vadovautis tarptautiniu mastu pripažintų organizacijų (pvz., EC-COUNCIL, ISACA, NIST ir kt.) rekomendacijomis ir gerąja praktika.

41. Kibernetinių atakų imitavimas atliekamas šiais etapais:

41.1. planavimo etapas. Kibernetinio saugumo vadovo parengiamas kibernetinių atakų imitavimo planas, kuriame apibrėžiami kibernetinių atakų imitavimo tikslai ir darbų apimtis, pateikiamas darbų grafikas, aprašomi planuojamų imituoti kibernetinių atakų tipai (išorinės ir (ar) vidinės), kibernetinių atakų imitavimo būdai (juodosios dėžės (angl. *Black Box*), baltosios dėžės (angl. *White Box*) ir (arba) pilkosios dėžės (angl. *Grey Box*)), galima neigiama įtaka veiklai, kibernetinių atakų imitavimo metodologija, programiniai ir (arba) techniniai įrankiai ir priemonės, nurodomi už plano vykdymą atsakingi asmenys ir jų kontaktai. Kibernetinių atakų imitavimo planas turi būti suderintas su centro generaliniu direktoriumi ir vykdomas tik gavus jo rašytinį pritarimą;

41.2. žvalgybos (angl. *Reconnaissance*) ir aptikimo (angl. *Discovery*) etapas. Surenkama informacija apie perimetrą, tinklo mazgus, tinklo mazguose veikiančių serverių ir kitų tinklo įrenginių operacines sistemas ir programinę įrangą, paslaugas (angl. *Services*), pažeidžiamumą, konfigūracijas ir kitą sėkmingai kibernetinei atakai įvykdyti reikalingą informaciją. Šiame etape turi būti teikiamos tarpinės ataskaitos apie vykdomas veiklas ir jos rezultatus;

41.3. kibernetinių atakų imitavimo etapas. Atliekami kibernetinių atakų imitavimo plane numatyti testai. Šiame etape turi būti teikiamos tarpinės ataskaitos apie vykdomas veiklas ir jos rezultatus;

41.4. ataskaitos parengimo etapas. Kibernetinių atakų imitavimo rezultatai turi būti išdėstomi Informacinių technologijų saugos vertinimo ataskaitoje. Kibernetinių atakų imitavimo plane numatyti testų rezultatai turi būti detalizuojami ataskaitoje ir lyginami su planuotaisiais. Kiekvienas aptiktas pažeidžiamumas turi būti detalizuojamas ir pateikiamos rekomendacijos jam pašalinti. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos įvertinimu. Jeigu nustatoma incidentų valdymo ir šalinimo, taip pat Centro nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinami veiklos tęstinumo planai.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

42. Centro organizaciniai ir techniniai reikalavimai formuojami remiantis „Nulinio pasitikėjimo“ (angl. *Zero-trust*) informacinių sistemų saugos modeliu.

43. Centro architektūra turi būti žinoma, aktuali ir dokumentuota įskaitant naudotojus, įrenginius, paslaugas ir duomenis.

44. Turi būti vykdoma išorinių ir vidinių grėsmių analizė, vertinamas naudotojų elgesys, sistemos komponentai ir jų pažeidžiamumai.

45. IS / registruose naudojamų svetainių saugos valdymo reikalavimai:

45.1. svetainės turi atitikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimus;

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

45.2. svetainių užkardos turi būti sukonfigūruotos taip, kad prie svetainių turinio valdymo sistemų (toliau – TVS) būtų galima jungtis tik iš vidinio Centro kompiuterinio tinklo arba nustatytų IP (angl. *Internet Protocol*) adresų;

45.3. turi būti pakeistos numatytos prisijungimo prie svetainių TVS ir administravimo skydų (angl. *Panel*) nuorodos (angl. *Default path*) ir slaptažodžiai;

45.4. turi būti užtikrinama, kad prie svetainių TVS ir administravimo skydų būtų galima jungtis tik naudojantis šifruotu ryšiu;

45.5. IS / registruose naudojamų svetainių sauga turi būti vertinama IS / registrų rizikos vertinimo ir (arba) informacinių technologijų saugos atitikties vertinimo, atliekamų saugos nuostatų II skyriuje nustatyta tvarka metu.

46. Programinės įrangos, skirtos IS / registrams apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

46.1. tarnybinėse stotyse ir vidinių IS / registrų naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo, stebėjimo realiu laiku priemonės;

46.2. IS / registrų komponentai be kenksmingos programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu rizikos vertinimo metu patvirtinama, kad šių komponentų rizika yra priimtina;

46.3. kenksmingos programinės įrangos aptikimo priemonės turi atsinaujinti automatiškai ne rečiau kaip kartą per 24 valandas. IS / registrų administratorius turi būti automatiškai informuojamas elektroniniu paštu apie tai, kuriems IS / registrų posistemiams, funkciškai savarankiškoms sudedamosioms dalims, vidinių IS / registrų naudotojų kompiuteriams ir kitiems IS / registrų komponentams yra pradelstas kenksmingos programinės įrangos aptikimo priemonių atsinaujinimo laikas, kenksmingos programinės įrangos aptikimo priemonės netinkamai funkcionuoja arba yra išjungtos.

47. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

47.1. IS / registrų tarnybinėse stotyse ir vidinių IS / registrų naudotojų kompiuteriuose turi būti naudojama tik legali programinė įranga;

47.2. vidinių IS / registrų naudotojų kompiuteriuose naudojama programinė įranga turi būti įtraukta į leistinos naudoti programinės įrangos sąrašą. Leistinos programinės įrangos sąrašą turi parengti, ne rečiau kaip kartą per metus peržiūrėti ir prireikus atnaujinti saugos įgaliotinis;

47.3. tarnybinių stočių ir vidinių IS / registrų naudotojų kompiuterių operacinės sistemos, kibernetiniam saugumui užtikrinti naudojamų priemonių ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai, klaidų pataisymai turi būti operatyviai išbandomi ir įdiegiami;

47.4. IS / registrų administratoriai reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius IS / registrų posistemiuose, funkciškai savarankiškose sudedamosiose dalyse, vidinių IS / registrų naudotojų kompiuteriuose. Apie įvertinimo rezultatus turi informuoti saugos įgaliotinį ir kibernetinio saugumo vadovą;

47.5. programinė įranga turi būti prižiūrima ir atnaujinama laikantis gamintojo reikalavimų ir rekomendacijų;

47.6. programinės įrangos diegimą, konfigūravimą, priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai – IS / registrų administratoriai arba tokias paslaugas teikiantys kvalifikuoti paslaugų teikėjai;

47.7. programinė įranga turi būti testuojama naudojant atskirą testavimo aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendraisiais reikalavimais asmens duomenų saugumo priemonėms;

47.8. IS / registrų programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų; 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.

48. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių ir kt.) pagrindinės naudojimo nuostatos:

48.1. IS / registrų naudotojų elektroninės informacijos perdavimo tinklo ir užkardų priežiūra vykdoma pagal Centro patvirtintą Kompiuterinio tinklo konfigūravimo ir stebėsenos tvarkos aprašą;

48.2. tinklo ir užkardų konfigūracija peržiūrima ne rečiau kaip kartą per metus. Peržiūrą inicijuoja saugos įgaliotinis, o ją vykdo IS / registrų administratorius;

48.3. kompiuterių tinklai turi būti atskirti nuo viešųjų elektroninių ryšių tinklų (interneto) naudojant užkardas, automatinę įsilaužimų aptikimo ir prevencijos įrangą, atkirtimo nuo paslaugos, dedikuoto atkirtimo nuo paslaugos įrangą;

48.4. kompiuterių tinklų perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešuose ryšių tinkluose naršančių vidinių IS / registrų naudotojų kompiuterinę įrangą nuo kenksmingo kodo. Visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

48.5. apsaugai nuo elektroninės informacijos nutekinimo turi būti naudojama duomenų srautų analizės ir kontrolės įranga;

48.6. turi būti naudojamos turinio filtravimo sistemos;

48.7. turi būti naudojamos taikomųjų programų kontrolės sistemos.

49. Leistinos IS / registrų naudotojų kompiuterių naudojimo ribos:

49.1. stacionarūs ir nešiojamieji IS / registrų naudotojų kompiuteriai privalo būti naudojami tik su tiesioginių pareigų atlikimu susijusiai veiklai atlikti. Iš kompiuterių, kurie perduodami remontui ar techninei priežiūrai, turi būti pašalinta visa IS / registrų konfidenciali ir apriboto naudojimo elektroninė informacija;

49.2. visiems IS / registrų naudotojų kompiuteriams privaloma naudoti papildomas saugos priemones, kuriomis patvirtinama IS / registrų naudotojo tapatybė ir šifruojami duomenys.

50. Metodai, kuriais galima užtikrinti saugų IS / registrų elektroninės informacijos teikimą ir (ar) gavimą:

50.1. IS / registrų duomenys perduodami automatiškai TCP/IP protokolu realiuoju laiku arba asinchroniniu režimu tik pagal IS / registrų nuostatuose ir duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

50.2. už duomenų teikimo ir gavimo sutartyse nurodomų saugos reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas saugos įgaliotinis;

50.3. IS / registrų duomenys perduodami šifruotais ryšio kanalais;

50.4. duomenims registruoti naudojamas saugus HTTPS protokolas;

50.5. duomenims perduoti naudojamas saugaus valstybinio duomenų perdavimo tinklas (SVDPT);

50.6. naudojamas virtualus privatus tinklas;

50.7. šifro raktų ilgiai, šifro raktų generavimo algoritmai, šifro raktų apsikeitimo protokolai, sertifikato parašo šifravimo algoritmai ir kiti šifravimo algoritmai nustatomi atsižvelgiant į Lietuvos ir tarptautinių organizacijų ir standartų rekomendacijas, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimus;

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

50.8. naudojamų šifravimo priemonių patikimumas vertinamas neeilinio arba kasmetinio IS / registrų rizikos vertinimo metu. Šifravimo priemonės turi būti operatyviai keičiamos nustačius saugumo spragų šifravimo algoritmuose.

51. Pagrindiniai atsarginių IS / registrų duomenų kopijų darymo ir atkūrimo reikalavimai:

51.1. atsarginių IS / registrų duomenų kopijų darymas ir atkūrimas turi būti atliekamas laikantis Lietuvos Respublikos teisės aktų reikalavimų;

51.2. atsarginės IS / registrų duomenų kopijos turi būti daromos periodiškai (visų duomenų kopija – vieną kartą per savaitę) pagal Centro patvirtintą Svarbiausių veiklos duomenų ir kitos informacijos atsarginių kopijų administravimo tvarkos aprašą;

51.3. atsarginių kopijų laikmenos yra pažymimos taip, kad jas būtų galima atpažinti;

51.4. IS / registrų duomenų atkūrimas iš atsarginių duomenų kopijų turi būti periodiškai išbandomas pagal Centro patvirtintą Svarbiausių veiklos duomenų ir kitos informacijos atsarginių kopijų administravimo tvarkos aprašą. Bandymų eiga ir rezultatai pateikiami saugos įgaliotiniui;

51.5. už atsarginių IS / registrų duomenų kopijų darymą ir atkūrimą, už IS / registrų taikomosios programinės įrangos (aplikacijų) kopijų inicijavimą atsakingas saugos įgaliotinis, o už vykdymą – IS / registrų administratorius;

51.6. atsarginės IS / registrų duomenų kopijos turi būti saugomos užrakintoje nedegioje spintoje, kitose patalpose arba kitame pastate, nei yra įrašymo įrenginys.

52. Centras, pirkdamas paslaugas, darbus ar įrangą, susijusius su informacinėmis sistemomis, jų projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo reikalavimams.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

53. Kvalifikacijos ir patirties reikalavimai IS / registrų naudotojams, IS / registrų administratoriams, IS / registrų naudotojų administratoriams, saugos įgaliotiniui ir kibernetinio saugumo vadovui:

53.1. IS / registrų administratorių, IS / registrų naudotojų administratorių, saugos įgaliotinio ir kibernetinio saugumo vadovo kvalifikacija turi atitikti bendruosius ir specialiuosius reikalavimus, nustatytus jų pareiginiuose nuostatuose;

53.2. IS / registrų naudotojai privalo turėti pagrindinių darbo kompiuteriu, taikomosiomis programomis įgūdžių, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, IS / registrų elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo saugoti jų paslaptį ir būti pasirašę Centro patvirtintą Konfidencialumo pasižadėjimą (toliau – Konfidencialumo pasižadėjimas). Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą;

53.3. IS / registrų naudotojai, pastebėję Informacijos saugumo politikos pažeidimų, nusikalstamos veikos požymių ar netinkamai veikiančių IS / registrų elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo priemonių, nedelsdami privalo apie tai pranešti Centrui;

53.4. saugos įgaliotinis, kibernetinio saugumo vadovas ir kibernetinio saugumo specialistas privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos (kibernetinio saugumo) srityje, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis,

reglamentuojančiomis elektroninės informacijos saugą (kibernetinį saugumą). Centras turi sudaryti sąlygas kelti saugos įgaliotinio ir kibernetinio saugumo vadovo kvalifikaciją;

Papunkčio pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

53.5. saugos įgaliotiniu, kibernetinio saugumo vadovu ir IS / registrų administratoriumi negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai;

53.6. IS / registrų administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti informacinių sistemų ir jose tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti IS / registrų komponentus (stebėti IS / registrų komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti informacinių sistemų komponentų nepertraukiamą funkcionavimą ir pan.). IS / registrų administratoriai turi būti susipažinę su Saugos dokumentais;

53.7. IS / registrų administratorius apie Saugos nuostatų 30 punkte ir jo papunkčiuose nurodytus rizikos veiksnius informuoja saugos įgaliotinį. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeidžiančią IS / registrų elektroninę informaciją (jos konfidencialumą, vientisumą ar prieinamumą), saugos įgaliotinis apie tai turi pranešti Centro generaliniam direktoriui ir, jeigu reikia, kompetentingoms institucijoms;

53.8. IS / registrų naudotojų administratorius turi būti gerai susipažinęs su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais, reglamentuojančiais asmens duomenų saugą, žinoti visus sutartinius įsipareigojimus ir teisės aktus, susijusius su IS / registrų naudotojų administravimu;

53.9. IS / registrų naudotojų administratorius turi žinoti IS / registrų vaidmenis ir jų suteikimo principus.

54. IS / registrų naudotojų ir IS / registrų administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

54.1. IS / registrų naudotojams turi būti organizuojami mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais, įvairiais būdais primenama apie elektroninės

informacijos saugos (kibernetinio saugumo) problemas (pvz., svarbios informacijos priminimai elektroniniu paštu, informacijos skelbimas Centro intranete, lankstinukai – atmintinės ir pan.);

54.2. mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), IS / registrų naudotojų ar IS / registrų administratorių poreikius;

54.3. mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.). Mokymus gali vykdyti registro saugos įgaliotinis ar kitas Centro darbuotojas, išmanantis elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, arba elektroninės informacijos saugos (kibernetinio saugumo) mokymų paslaugų teikėjas;

54.4. mokymai IS / registrų naudotojams elektroninės informacijos saugos ir kibernetinio saugumo klausimais, įvairiais būdais primenant apie saugumo problemas (pvz., pranešimai elektroniniu paštu, naujų darbuotojų instruktavimas ir pan.), turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Mokymai IS / registrų administratoriams turi būti organizuojami pagal poreikį. Už mokymų organizavimą atsakingas saugos įgaliotinis.

55. Apie saugos reikalavimų ir saugaus darbo rekomendacijų atnaujinimą naudotojai informuojami reguliariai skelbiant aktualią informaciją Centro intranete, esant būtinybei, informuojami tiesiogiai elektroniniu paštu arba tikslinėms naudotojų grupėms rengiant papildomus mokymus.

V SKYRIUS
IS / REGISTRŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

56. Už IS / registrų naudotojų supažindinimą su saugos dokumentais ar jų santraukomis bei teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, įrodomumą ir atsakomybę už jų reikalavimų nesilaikymą, yra atsakingas saugos įgaliotinis.

57. IS / registrų naudotojų supažindinimo su saugos dokumentais ar jų santraukomis būdai turi būti pasirenkami atsižvelgiant į IS / registrų specifiką (pvz., IS / registrų naudotojų buvimo vietą, organizacinių ar techninių priemonių, leidžiančių identifikuoti su saugos dokumentais ar jų santraukomis susipažinusį asmenį ir užtikrinančių supažindinimo procedūros įrodomąją (teisinę) galią, panaudojimo galimybes ir pan.). IS / registrų naudotojai su saugos dokumentais ar jų

santraukomis turi būti supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą.

58. Pakartotinai su saugos dokumentais ar jų santraukomis IS / registrų naudotojai supažindinami tik iš esmės pasikeitus IS / registrams arba elektroninės informacijos saugą (kibernetinį saugumą) reglamentuojantiems teisės aktams.

59. Tvarkyti IS / registrų elektroninę informaciją gali tik tie asmenys, kurie yra susipažinę su saugos dokumentais ir įsipareigoję laikytis jų reikalavimų (pasirašę Konfidencialumo pasižadėjimą).

60. IS / registrų naudotojai atsako už IS / registrų ir juose tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją.

61. IS / registrų naudotojai, IS / registrų administratoriai, IS / registrų naudotojų administratoriai, saugos įgaliotinis, kibernetinio saugumo vadovas ir kibernetinio saugumo specialistas, pažeidę Saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

62. Informacijos saugumo politikos santrauka, Išorinių naudotojų administravimo taisyklės ir Saugos dokumentai yra viešai skelbiami Centro interneto svetainėje ir yra privalomi visiems IS / registrų naudotojams, dirbantiems su IS / registrais.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

63. Saugos dokumentai privalomi ŽŪM, Centro darbuotojams ir IS / registrų naudotojams, kurie tvarko IS / registrų elektroninę informaciją.

64. Saugos dokumentai turi būti derinami su Nacionaliniu kibernetinio saugumo centru prie Lietuvos Respublikos krašto apsaugos ministerijos (toliau – NKSC), išskyrus atvejus, kai keičiant minėtus dokumentus atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos ir kibernetinio saugumo politikos nekeičiantys pakeitimai arba taisoma teisės technika. NKSC turi būti pateiktos keičiamų saugos dokumentų kopijos.

65. Centras saugos dokumentus turi persvarstyti (peržiūrėti) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos vertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminių organizacinių, sisteminių ar kitų ŽŪM ar Centro pokyčių.

66. Saugos dokumentų ir kitos su IS / registrų elektroninės informacijos sauga (kibernetiniu saugumu) susijusios dokumentacijos priežiūrą ar keitimą inicijuoja Centras.

67. Asmenys, pažeidę Saugos nuostatus, atsako teisės aktų nustatyta tvarka.

Valstybės įmonės Žemės ūkio duomenų centro administruojamų informacinių sistemų ir registrų duomenų saugos nuostatų priedas

VALSTYBĖS ĮMONĖS ŽEMĖS ŪKIO DUOMENŲ CENTRO ADMINISTRUOJAMŲ INFORMACINIŲ SISTEMŲ IR REGISTRŲ SĄRAŠAS

Eil. Nr.	**Registro / valstybės informacinės sistemos pavadinimas**	**Registro / valstybės informacinės sistemos rūšis, kuriai priskiriami valstybės informacinį išteklių sudarantys duomenys ir informacinė sistema, kurioje jie tvarkomi**
1.	Ūkinių gyvūnų registras	ypatingos svarbos (1)
2.	Paraiškų priėmimo informacinė sistema	svarbi (2)
3.	Lietuvos žemės ūkio ir maisto produktų rinkos informacinė sistema	svarbi (2)
4.	Lietuvos Respublikos žemės ūkio ir kaimo verslo registras	svarbi (2)
5.	Lietuvos Respublikos ūkininkų ūkių registras	svarbi (2)
6.	Lietuvos Respublikos traktorių, savaeigių ir žemės ūkio mašinų ir jų priekabų registras	svarbi (2)
7.	Ūkinių gyvūnų veislininkystės informacinė sistema	Svarbi (2)
8.	Traktorininko pažymėjimų informacinė sistema	Svarbi (2)
9.	Lietuvos Respublikos pašarų ūkio subjektų registras	vidutinės svarbos (3)
10.	Žemdirbių mokymo ir konsultavimo informacinė sistema	vidutinės svarbos (3)
11.	Paramos žemės ūkio veiklos subjektams apskaičiavimo informacinė sistema	vidutinės svarbos (3)
12.	Pieno apskaitos informacinė sistema	vidutinės svarbos (3)
13.	Žemės ūkio ir maisto produktų sertifikavimo informacinė sistema	vidutinės svarbos (3)
14.	Žemės ūkio veiklą vykdančių ūkio subjektų patikrinimo aktų informacinė sistema	vidutinės svarbos (3)

15.	Žemės išteklių stebėsenos informacinė sistema	mažai svarbi (4)

Priedo pakeitimai:
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584

Pakeitimai:

1.
Lietuvos Respublikos žemės ūkio ministerija, Įsakymas
Nr. 3D-748, 2020-10-29, paskelbta TAR 2020-10-29, i. k. 2020-22522
Dėl žemės ūkio ministro 2018 m. balandžio 19 d. įsakymo Nr. 3D-235 „Dėl valstybės įmonės Žemės ūkio informacijos ir kaimo verslo centro administruojamų informacinių sistemų ir registrų duomenų saugos nuostatų patvirtinimo“ pakeitimo

2.
Lietuvos Respublikos žemės ūkio ministerija, Įsakymas
Nr. 3D-789, 2022-12-09, paskelbta TAR 2022-12-09, i. k. 2022-25175
Dėl žemės ūkio ministro 2018 m. balandžio 19 d. įsakymo Nr. 3D-235 „Dėl Valstybės įmonės žemės ūkio informacijos ir kaimo verslo centro administruojamų informacinių sistemų ir registrų duomenų saugos nuostatų patvirtinimo“ pakeitimo

3.
Lietuvos Respublikos žemės ūkio ministerija, Įsakymas
Nr. 3D-340, 2024-04-25, paskelbta TAR 2024-04-25, i. k. 2024-07584
Dėl žemės ūkio ministro 2018 m. balandžio 19 d. įsakymo Nr. 3D-235 „Dėl Valstybės įmonės Žemės ūkio duomenų centro administruojamų informacinių sistemų ir registrų duomenų saugos nuostatų patvirtinimo“ pakeitimo