ŽUVININKYSTĖS TARNYBOS
PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS
DIREKTORIUS

ĮSAKYMAS
DĖL ŽUVININKYSTĖS TARNYBOS PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS KIBERNETINIO SAUGUMO POLITIKOS IR JOS ĮGYVENDINIMO DOKUMENTŲ PATVIRTINIMO

2026 m. vasario 9 d. Nr. V1-27
Klaipėda

Vadovaudamasis Lietuvos Respublikos kibernetinio saugumo įstatymo 14 straipsniu ir Kibernetinio saugumo reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“:

1. Tvirtinu:

1.1. Žuvininkystės tarnybos informacinių sistemų ir naudotojų administravimo taisykles (pridedama);

1.2. Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarką (pridedama);

1.3. Kriptografijos ir šifravimo naudojimo tvarką (pridedama);

1.4. Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, tvarką (pridedama);

1.5. Tinklų ir informacinių sistemų kibernetinio saugumo politiką (pridedama);

1.6. Fizinės apsaugos tvarką (pridedama);

1.7. Tiekimo grandinės saugumo valdymo tvarką (pridedama).

2. Nustatau, kad šis įsakymas įsigalioja nuo jo pasirašymo dienos.

Direktorius Tomas Kazlauskas

SUDERINTA
Lietuvos Respublikos žemės ūkio
ministerijos 2026-02-02
raštu Nr. 2D-286

PATVIRTINTA
Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
direktoriaus 2026 m. vasario 9 d.
įsakymu Nr. V1-27

ŽUVININKYSTĖS TARNYBOS PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS INFORMACINIŲ SISTEMŲ IR NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Žuvininkystės tarnyba) informacinių sistemų naudotojų administravimo taisyklės (toliau – Administravimo taisyklės) nustato Žuvininkystės tarnybos informacinių sistemų (toliau – Informacinės sistemos) naudotojų ir Informacinės sistemos administratoriaus įgaliojimus, teises ir pareigas bei saugaus duomenų ir informacijos teikimo Informacinės sistemos paslaugų gavėjams kontrolės tvarką.

2. Administravimo taisyklės parengtos vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatymu, Kibernetinio saugumo reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

3. Administravimo taisyklėse vartojamos sąvokos:

3.1. Informacinės sistemos **valdytoja** – Lietuvos Respublikos žemės ūkio ministerija.

3.2. Informacinės sistemos **tvarkytoja** – Žuvininkystės tarnyba prie Lietuvos Respublikos žemės ūkio ministerijos.

3.3. Informacinės sistemos **administratorius** (toliau – IS administratorius) – Žuvininkystės tarnybos darbuotojas, kuris yra atsakingas už naujų tinklų ir informacinių paskyrų sukūrimą, sustabdymą ar panaikinimą bei prieigų prie Žuvininkystės tarnybos tinklų ir informacinių sistemų suteikimą, keitimą, sustabdymą ar panaikinimą pagal Prieigos užsakovo pateiktą prašymą ir IT padalinio ar tinklų ir informacinių sistemų savininko nurodymus.

3.4. Informacinės sistemos **saugos įgaliotinis –** Informacinės sistemos tvarkytojos direktoriaus įsakymu paskirtas asmuo, atsakingas už kibernetinių incidentų valdymą, informavimą apie kibernetinius incidentus ypatingos svarbos informacinėse infrastruktūrose bei saugos politikos įgyvendinimą.

3.5. Informacinės sistemos naudotojas – Informacinės sistemos tvarkytojos valstybės tarnautojai arba darbuotojai, dirbantys pagal darbo sutartis (toliau – darbuotojai), arba kitas asmuo,

pagal kompetenciją naudojantis ir (ar) tvarkantis Informacinės sistemos elektroninę informaciją Informacinės sistemos veiklą reglamentuojančių teisės aktų nustatyta tvarka.

3.6. **Standartinis naudotojas**, turintis standartines teises prisijungti ir naudotis Žuvininkystės tarnybos tinklų ir informacine sistema, bet negalintis atlikti jokių sisteminių ar kitų tinklų ir informacinių sistemų pokyčių, konfigūracijų ar programinės įrangos diegimų;

3.7. **Privilegijuotas naudotojas**, turintis didesnes teises nei standartinis naudotojas, leidžiančias atlikti kai kurias tinklų ir informacinių sistemų administravimo funkcijas (privilegijuotais naudotojais dažniausiai yra organizacijos ar tiekėjo tinklų ir informacinių sistemų palaikymo funkcijas vykdantys darbuotojai, kurie turi papildomas teises, pvz. teisę prisijungti prie serverių, aptarnauti duomenų bazes ir pan.);

3.8. Informacinės sistemos **paslaugų gavėjai** – fiziniai ir juridiniai asmenys, naudojantys Informacinės sistemos duomenis.

3.9. **Kibernetinio saugumo vadovas** – kaip apibrėžta Žuvininkystės tarnybos tinklų ir informacinių sistemų kibernetinio saugumo politikoje;

3.10. Informacinių technologijų pagalbos tarnyba (angl. *Service desk*) (toliau – IT pagalbos tarnyba) – Žuvininkystės tarnybos valdoma informacinė sistema, kurios pagalba valdomi tinklų ir informacinių sistemų kreipiniai ir problemos, įskaitant prašymus suteikti, pakeisti, sustabdyti arba panaikinti paskyrą ir prieigos teises prie Žuvininkystės tarnybos tinklų ir informacinių sistemų. Nesant IT pagalbos tarnybos, prašymai suteikti, pakeisti, sustabdyti arba panaikinti paskyrą ir prieigos teises prie Žuvininkystės tarnybos tinklų ir informacinių sistemų gali būti pateikiami tik elektroniniu paštu už tinklų ir informacinių sistemų priežiūrą ir palaikymą atsakingiems tinklų ir informacinių sistemų administratoriams;

3.11. **Paskyra** – unikalus identifikatorius, suteikiantis naudotojui ar techninei sistemai prieigą prie tinklų ir informacinių sistemų;

3.12. **Paskyrų valdymas** – tinklų ir informacinių sistemų naudotojų paskyrų sukūrimas, keitimas, sustabdymas ar naikinimas ir kontrolės užtikrinimas;

3.13. **Prieiga** – galimybė naudotis tinklų ir informacinėmis sistemomis, atsižvelgiant į suteiktas teises (teisių rinkinį);

3.14. **Prieigos užsakovas** – Žuvininkystės tarnybos darbuotojas arba jo vadovas (arba už sutartį su trečiąja šalimi atsakingas Žuvininkystės tarnybos darbuotojas) IT administratoriui teikiantis prašymą suteikti, pakeisti, sustabdyti arba panaikinti paskyrą ir prieigos teises prie organizacijos tinklų ir informacinių sistemų;

3.15. **Prieigų valdymas** – tinklų ir informacinių sistemų naudotojams prieigos teisių (teisių rinkinių) prie Žuvininkystės tarnybos tinklų ir informacinių sistemų suteikimas, keitimas, sustabdymas ar naikinimas ir kontrolės užtikrinimas;

3.16. **Sisteminė paskyra** – tai techninė paskyra, kuri naudojama tinklų ir informacinėje sistemoje, aplikacijos ar automatizuotų procesų veikimui užtikrinti.

3.17. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

3.18. Kitos Administravimo taisyklėse vartojamos sąvokos atitinka Administravimo taisyklių 2 punkte nurodytuose teisės aktuose arba Žuvininkystės tarnybos tinklų ir informacinių sistemų kibernetinio saugumo politikoje apibrėžtas sąvokas.

4. Administravimo taisyklės taikomos visiems Informacinės sistemos naudotojams, Informacinės sistemos administratoriui, Informacinės sistemos saugos įgaliotiniui, kurių prieigos prie Informacinės sistemos duomenų teisės paremtos Informacinės sistemos duomenų saugumo, stabilumo, operatyvumo principais.

5. Informacinės sistemos naudotojams prieiga prie Informacinės sistemos duomenų suteikiama vadovaujantis šiais principais:

5.1. Būtina žinoti (angl. *Need to know*) – standartiniams ir privilegijuotiems naudotojams turėtų būti suteikta prieiga tik prie tų Žuvininkystės tarnybos tvarkomų duomenų, kurie jiems reikalingi darbo funkcijoms atlikti ar sutartiniams įsipareigojimams įgyvendinti;

5.2. Mažiausios privilegijos (angl. *Least privilege*) – naudotojams suteikiamos mažiausios prieigos teisės prie Žuvininkystės tarnybos tinklų ir informacinių sistemų, kurios jiems reikalingi darbo funkcijoms atlikti ar sutartiniams įsipareigojimams įgyvendinti, bet ne daugiau;

5.3. Pareigų atskyrimas (angl. *Segregation of duties*) – Žuvininkystės tarnyboje turi būti sukurtos procedūros ir organizacinė struktūra, neleidžiančios vienam naudotojui kontroliuoti visų pagrindinių tinklų ir informacinių sistemų veiklos aspektų ir atlikti neleistinus veiksmus ar neteisėtai pasiekti organizacijos tinklų ir informacinių sistemų ir juose esančių duomenų.

5.4. Informacinės sistemos naudotojams prieiga turi būti suteikiama tik prie tų Informacinės sistemos duomenų ir tokia apimtimi, kiek reikia Informacinės sistemos naudotojo pareigybės aprašyme nurodytoms funkcijoms atlikti;

5.5. Informacinės sistemos duomenis gali keisti (sukurti, papildyti ar panaikinti) tik tokią teisę turintys Informacinės sistemos naudotojai;

5.6. prieiga prie Informacinės sistemos duomenų ir teisė ją keisti suteikiama tik atlikus Informacinės sistemos naudotojo atpažinimą.

5.7. Žuvininkystės tarnyba privalo įgyvendinti Kibernetinio saugumo įstatymą ir Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 3 d.

nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, numatytus techninius prieigos valdymo ir tapatumo nustatymo reikalavimus, kurie pateikti šios Tvarkos 1 priede. (žr. šios Tvarkos 1 priedą).

II SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ IR INFORMACINĖS SISTEMOS ADMINISTRATORIAUS ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. Kibernetinio saugumo vadovo funkcijos ir atsakomybės:

6.1. kontroliuoja, kad organizacijoje būtų pilna apimtimi įgyvendinti šios Tvarkos 1 priede numatyti Techniniai prieigos valdymo ir tapatumo nustatymo reikalavimai;

6.2. kontroliuoja, kad naudotojų paskyrų ir prieigos prie TIS valdymo procesai būtų įgyvendinami pagal šios Tvarkos reikalavimus;

6.3. rengia ir esant poreikiui koreguoja paskyrų ir prieigų matricą;

6.4. vertina periodinių prieigų valdymo auditų rezultatus;

6.5. bent kartą per metus arba kai organizacijoje atsiranda esminiai pokyčiai, kurie turi įtakos šiai Tvarkai, peržiūri ir atnaujina šią Tvarką.

7. Saugos įgaliotinio funkcijos ir atsakomybės:

7.1. užtikrina, kad organizacijoje būtų pilna apimtimi įgyvendinti šios Tvarkos 1 priede numatyti Techniniai prieigos valdymo ir tapatumo nustatymo reikalavimai;

7.2. užtikrina, kad naudotojų paskyrų ir prieigos prie Žuvininkystės tarnybos TIS valdymo procesai būtų įgyvendinami pagal šios Tvarkos reikalavimus;

7.3. teikia privalomus nurodymus naudotojams ir IS administratoriams, siekiant užtikrinti tinkamą paskyrų ir prieigų valdymą.

8. Prieigos užsakovo funkcijos ir atsakomybės:

8.1. teikia prašymus naudotojams sukurti, pakeisti, sustabdyti ir panaikinti paskyras, vadovaudamasis paskyrų ir prieigos teisių valdymo principais;

8.2. teikia prašymus naudotojams suteikti, pakeisti, sustabdyti ar panaikinti prieigas prie TIS, vadovaudamasis paskyrų ir prieigos teisių valdymo principais;

8.3. užtikrina, kad IS administratorius laiku gautų prašymą ir, kad IS administratoriai naudotojams laiku sukurtų, sustabdytų ar panaikintų paskyras bei laiku suteiktų, pakeistų, sustabdytų ar panaikintų jiems prieigas prie TIS.

9. Informacinės sistemos naudotojai turi teisę:

9.1. naudotis tik tomis Informacinės sistemos funkcijomis bei Informacinės sistemos duomenimis, prie kurių prieigą jiems suteikė Informacinės sistemos administratorius;

9.2. gauti informaciją apie jų naudojamų Informacinės sistemos duomenų apsaugos lygį bei taikomas apsaugos priemones, teikti siūlymus dėl papildomų apsaugos priemonių;

9.3. kreiptis į Informacinės sistemos administratorių ar Informacinės sistemos saugos įgaliotinį dėl neveikiančių ar netinkamai veikiančių Informacinių sistemų;

9.4. Informacinės sistemos naudotojai turi teisę atlikti kitus veiksmus, numatytus Informacinės sistemos saugos politikos įgyvendinamuosiuose teisės aktuose.

10. Informacinės sistemos naudotojai privalo:

10.1. naudoti Informacinės sistemos duomenis tik tarnybinėms arba darbo funkcijoms atlikti;

10.2. nedelsiant pranešti Informacinės sistemos administratoriui ir Informacinės sistemos saugos įgaliotiniui apie Informacinės sistemos saugos politikos įgyvendinamųjų teisės aktų pažeidimus, veiksmus, turinčius nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų ir informacijos saugos užtikrinimo priemones, apie pastebėtus galimus asmens duomenų saugumo pažeidimus;

10.3. užtikrinti jų naudojamų Informacinės sistemos duomenų konfidencialumą bei vientisumą, savo veiksmais netrikdyti Informacinės sistemos duomenų prieinamumo;

10.4. baigus darbą ar pasitraukiant iš darbo vietos, imtis priemonių, kad su Informacinės sistemos duomenimis negalėtų susipažinti pašaliniai asmenys: atsijungti nuo Informacinės sistemos, įjungti ekrano užsklandą su slaptažodžiu, dokumentus ar jų kopijas darbo vietoje padėti į pašaliniams asmenims neprieinamą vietą;

10.5. susipažinti ir laikytis Informacinės sistemos saugos politiką įgyvendinančių teisės aktų ir šių Administravimo taisyklių reikalavimų;

10.6. pranešti Informacinės sistemos administratoriui apie slaptažodžio užblokavimą ar užmiršimą;

10.7. Informacinės sistemos naudotojai privalo vykdyti kitas pareigas, nustatytas Informacinės sistemos saugos politikos įgyvendinamuosiuose teisės aktuose.

11. Informacinės sistemos naudotojui draudžiama:

11.1. leisti prisijungti prie Informacinės sistemos ne Informacinės sistemos naudotojui ar kitais nei Administravimo taisyklėse nurodytais būdais;

11.2. be priežiūros palikti įrenginius, kuriais jungiamasi prie Informacinės sistemos, neužrakintu ekranu;

11.3. platinti Informacinėje sistemoje esančią informaciją, išskyrus viešo turinio informaciją;

11.4. Informacinės sistemos naudotojams negali būti suteikiamos Informacinės sistemos administratoriaus teisės.

12. Informacinės sistemos administratorius turi teisę:

12.1. matyti visų Informacinės sistemos naudotojų atpažinties ir suteiktų teisių duomenis;

12.2. matyti Informacinės sistemos naudotojų su Informacinės sistemos duomenimis atliktus veiksmus;

12.3. atlikti užklausas Informacinėje sistemoje pagal pasirinktus paieškos kriterijus;

12.4. fiziškai prieiti prie techninės ir sisteminės programinės įrangos;

12.5. vykdyti Informacinės sistemos techninės priežiūros funkcijas.

13. Informacinės sistemos administratorius privalo:

13.1. registruoti naujus Informacinės sistemos naudotojus;

13.2. tvarkyti esamų Informacinės sistemos naudotojų duomenis;

13.3. periodiškai tikrinti, ar yra Informacinės sistemos administratoriaus nepatvirtintų paskyrų;

13.4. reguliariai tikrinti, ar yra Informacinės sistemos naudotojų nepatvirtintų paskyrų; apie nepatvirtintas Informacinės sistemos naudotojų paskyras pranešti Informacinės sistemos saugos įgaliotiniui;

13.5. konsultuoti Informacinės sistemos naudotojus apie Informacinės sistemos veikimą ir kitais su susijusiais klausimais;

13.6. Informacinės sistemos priežiūros funkcijas atlikti naudojant atskirą paskyrą, kuri negali būti naudojama įprastoms Informacinės sistemos naudotojo funkcijoms atlikti;

13.7. pagal kompetenciją užtikrinti nepertraukiamą Informacinės sistemos techninės ir sisteminės programinės įrangos veikimą;

13.8. dalyvauti vertinant Informacinės sistemos atlikti rizikos veiksnius, rengiant Informacinės sistemos rizikos veiksnių įvertinimo ataskaitą, rizikos veiksnių įvertinimo ir rizikos veiksnių valdymo priemonių planą;

13.9. atlikti Informacinės sistemos taikomų saugumo reikalavimų atitikties vertinimą.

14. Informacinės sistemos administratoriui draudžiama:

14.1. suteikti ne Informacinės sistemos naudotojams prieigos teises prie Informacinės sistemos duomenų, išskyrus viešo turinio informaciją.

15. Informacinės sistemos administratoriaus slaptažodis, kuriuo jungiamasi prie Informacinės sistemos, turi atitikti specialiuosius reikalavimus (t. y. slaptažodžio ilgis, naudojami simboliai).

16. Informacinės sistemos administratoriaus, Informacinės sistemos saugos įgaliotinio funkcijos reglamentuotos Informacinės sistemos saugos nuostatuose ir kituose Informacinės sistemos saugos politikos įgyvendinamuosiuose teisės aktuose.

17. Informacinės sistemos administratorius turi prieigos prie Informacinės sistemos duomenų teisę (elektroninės informacijos skaitymas, kūrimas, atnaujinimas, naikinimas, Informacinės sistemos naudotojų informacijos, prieigos teisių redagavimas ir kt.).

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO INFORMACINĖS SISTEMOS NAUDOTOJAMS KONTROLĖS TVARKA

18. Informacinės sistemos administratorius yra atsakinga už Informacinės sistemos naudotojų registravimą, išregistravimą, prieigos prie Informacinės sistemos tarnybinių stočių ir Informacinės sistemos teisių suteikimą ir panaikinimą.

19. Informacinės sistemos naudotojams registruojantis Informacinėje sistemoje, suteikiamas unikalus prisijungimo prie Informacinės sistemos vardas ir atsitiktiniu būdu sugeneruotas slaptažodis su galimybe jį pasikeisti.

20. Informacinės sistemos paslaugų gavėjams informacija teikiama Informacinių sistemų duomenų saugos nuostatuose nustatyta tvarka.

21. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Informacinės sistemos saugos įgaliotinio sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo ir tik tuo atveju, nėra techninių galimybių Informacinės sistemos naudotojui perduoti slaptažodžio šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

22. Informacinės sistemos naudotojai, kuriems suteikta teisė prisijungti prie Informacinės sistemos tarnybinių stočių, prisijungti gali tik su Informacinės sistemos administratoriaus suteiktais unikaliais vardais ir slaptažodžiais.

23. Informacinės sistemos dalys, patvirtinančios Informacinės sistemos naudotojo tapatumą, turi drausti automatiškai išsaugoti slaptažodžius.

24. Informacinės sistemos naudotojų prisijungimo prie Informacinės sistemos vardai ir slaptažodžiai saugomi atitinkamos Informacinės sistemos duomenų bazėje.

25. Prieigą prie duomenų bazės turi tik Informacinės sistemos administratorius. Duomenys duomenų bazėje šifruojami.

26. Slaptažodį Informacinės sistemos naudotojai, prisijungę prie Informacinės sistemos, turi teisę pasikeisti savarankiškai.

27. Informacinės sistemos naudotojo slaptažodžiui yra keliami šie reikalavimai:

27.1. slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija (t. y. gimimo data, šeimos narių vardai ir pan.);

27.2. slaptažodis turi būti iš netrumpesnės kaip 12 simbolių kombinacijos, sudarytos iš didžiųjų ir mažųjų raidžių, skaitmenų ir specialiųjų simbolių;

27.3. keičiant slaptažodį neleidžiama pasirinkti slaptažodžio iš buvusių 10 paskutinių slaptažodžių;

27.4. slaptažodis turi būti keičiamas ne rečiau kaip kas 3 (tris) mėnesius;

27.5. Informacinės sistemos naudotojas, pirmą kartą gavęs Informacinės sistemos administratoriaus suteiktą vardą ir slaptažodį, turi prisijungti prie Informacinės sistemos ir nedelsdamas slaptažodį pakeisti;

27.6. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius – 10 kartų. Informacinės sistemos naudotojui 10 kartų neteisingai įvedus slaptažodį, Informacinė sistema užrakina ir Informacinės sistemos naudotojui 30 minučių neleidžiama prisijungti;

27.7. Informacinės sistemos naudotojas privalo saugoti slaptažodį ir jo neatskleisti;

27.8. Informacinės sistemos naudotojas, įtaręs, kad kiti asmenys sužinojo slaptažodį, privalo nedelsdamas jį pakeisti.

28. Laikotarpiu, kai Informacinės sistemos naudotojas nevykdo funkcijų, susijusiu su darbu Informacinėje sistemoje, teisė dirbti su atitinkama Informacinės sistemos elektronine informacija jam yra sustabdoma.

29. Pasibaigus darbo santykiams, Informacinės sistemos naudotojui panaikinama Informacinės sistemos naudotojo paskyra.

30. Pasibaigus darbo santykiams, Informacinės sistemos administratoriaus teisė dirbti su Informacine sistema turi būti sustabdoma ir panaikinama Informacinės sistemos administratoriaus paskyra.

31. Leistinas nuotolinio Informacinės sistemos naudotojų prisijungimo prie Informacinės sistemos būdas yra virtualaus kompiuterių tinklo (angl. *Virtual Private Network*) paslauga.

III SKYRIUS
PASKYRŲ IR PRIEIGŲ VALDYMAS

32. Užtikrinant paskyrų ir prieigų valdymą turi būti pilnai įgyvendinti šios Tvarkos 1 priede numatyti Techniniai prieigos valdymo ir tapatumo nustatymo reikalavimai, susiję su paskyrų ir prieigų valdymu, taip pat šioje Tvarkoje papildomai nustatyti paskyrų ir prieigų valdymo reikalavimai.

33. Naujos paskyros sukuriamos ir prieigos prie TIS suteikiamos vadovaujantis šiuo procesu:

33.1. Nauja TIS naudotojo paskyra sukuriama priėmus į darbą naują darbuotoją arba esamą darbuotoją perkėlus į kitas pareigas (kurio darbo funkcijoms atlikti reikalinga sukurti paskyrą ir prieigos teises) arba su trečiąja šalimi (pvz. su TIS priežiūros ir vystymo paslaugas teikiančiu tiekėju) sudarius paslaugos teikimo sutartį (jei suteikiama paslauga negali būti įgyvendinta be paskyros ir prieigos prie TIS sukūrimo ir suteikimo);

33.2. Esant bent vienai iš aukščiau numatytų aplinkybių, Prieigos užsakovas elektroniniu paštu arba per IT pagalbos tarnybą turi pateikti prašymą TIS naudotojui sukurti, pakeisti, sustabdyti

ar panaikinti paskyrą ar suteikti, pakeisti, sustabdyti ar panaikinti prieigas prie TIS (toliau – Prašymas), jame nurodydamas:

33.2.1. darbuotojo (trečiosios šalies darbuotojo) vardą, pavardę, padalinį ir pareigas;

33.2.2. naujos paskyros sukūrimo priežastį (darbuotojo priėmimas, perkėlimas, atleidimas, ar kt.);

33.2.3. paskyros tipą;

33.2.4. reikalingų suteikti prieigų prie TIS teisių sąrašą (teisių rinkinį);

33.2.5. paskyros ir (ar) prieigos apribojimus, jei tokie yra;

33.2.6. paskyros aktyvavimo datą (naujai sukurta paskyra gali būti aktyvuojama ne anksčiau kaip pirmą darbuotojo darbo dieną. Trečiosios šalies darbuotojo paskyra aktyvuojama ne anksčiau, kai pradeda galioti pasirašyta sutartis. Išimtis gali būti taikoma tais atvejais, jei sudaromoje sutartyje nurodomos kitos datos).

33.3. Prieigos užsakovas Prašymus turi teikti vadovaudamasis paskyrų ir prieigos teisių valdymo principais.

33.4. IS administratorius, gavęs Prašymą, turi sukurti naują naudotojo paskyrą ir jam suteikti prieigas prie TIS, vadovaudamasis Prašyme pateikta informacija ir jame nustatytais terminais.

33.5. IS administratorius sukurdamas paskyrą turi užtikrinti, kad būtų įgyvendintos priemonės TIS naudotojo tapatybei nustatyti.

33.6. Jei Prašyme yra numatyta sukurti paskyrą ir suteikti prieigas privilegijuotam naudotojui ar sisteminei paskyrai, tokį prašymą papildomai turi tvirtinti paskirtas atsakingas darbuotojas.

33.7. Jeigu Prašyme yra numatyta sukurti paskyrą IS administratoriui ir jam suteikti prieigas prie TIS, tokį prašymą papildomai turi tvirtinti saugos įgaliotinis.

33.8. Darbuotojams, vykdantiems specifines, su TIS administravimu susijusias funkcijas (pvz. vykdantiems TIS priežiūrą ir vystymą, standartiniams naudotojams suteikiantys prieigas ir pan.), kartu su privilegijuota ir (ar) IS administratorius paskyra turi būti sukurta ir standartinio naudotojo paskyra ir jai suteiktos prieigos prie TIS, kasdienėms funkcijos vykdyti.

33.9. Draudžiama privilegijuotiems naudotojams ir IS administratoriams jų funkcijoms įgyvendinti sukurtas paskyras ir (ar) joms suteiktas prieigas prie TIS naudoti kasdienėms funkcijos vykdyti (kuomet šie darbai/funkcijos nereikalauja privilegijuotų prieigos teisių).

34. Galiojančios paskyros ir joms suteiktų prieigų keitimas yra įgyvendinamas tokia pačia tvarka kaip ir naujos paskyros sukūrimas ir prieigų suteikimas. Atsiradus poreikiui pakeisti paskyrą ir (ar) prieigas (pvz. pasikeičia darbuotojo funkcijos arba su TIS priežiūros ir plėtojimo paslaugas teikiančiu tiekėju keičiama sutartis), Prieigos užsakovas, teikdamas Prašymą papildomai turi nurodyti, ar naudojama paskyra turi būti palikta ar panaikinta, ar naudotojui jau suteiktos prieigos turi būti paliktos ar panaikintos, bei nurodyti terminą nuo kada turi būti įgyvendintas pakeitimas.

IV SKYRIUS
PASKYRŲ IR PRIEIGOS TEISIŲ PERŽIŪRA IR ATITIKTIES REIKALAVIMAI

35. Naudotojų paskyros ir prieigos prie TIS turi būti peržiūrimos periodiškai, ne rečiau kaip kartą per metus, siekiant užtikrinti, kad visų naudotojų paskyros ir prieigos teisės būtų sustabdytos ar panaikintos, kai paskyros ir (ar) teisių poreikis pasibaigia. Už paskyrų ir prieigos teisių peržiūrą atsakingas paskirtas IS administratorius ir (ar) paslaugų teikėjo atsakingas darbuotojas (jei paskyras ir (ar) prieigas valdo trečioji šalis sutarties pagrindu).

36. IS administratorius, atlikęs paskyrų ir prieigos teisių peržiūrą, informaciją apie tai fiksuoja numatytuose dokumentuose.

37. IS administratorius, trečiosios šalies atstovas (jei paskyras ir (ar) prieigas valdo trečioji šalis) sutarties pagrindu nustatę, kad paskyros ir prieigos yra valdomos ne pagal šią Tvarką turi nedelsiant ištaisyti neatitikimus ir apie tai informuoti saugos įgaliotinį.

VI SKYRIUS
SLAPTAŽODŽIŲ VALDYMO REIKALAVMAI

38. IS administratorius, užtikrindamas slaptažodžių valdymą, turi įgyvendinti tokius TIS naudotojų slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimus:

38.1. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai);

38.2. slaptažodis negali būti sudarytas iš pasikartojančių arba nuoseklių simbolių (pvz., „aaaaaaaaaaaa“ arba „0123456789“) ar įprastos klaviatūros sekos (pvz., „Qwerty“);

38.3. sudarant naudotojų ir (ar) IS administratorių slaptažodžius, jie turi atitikti šios Tvarkos 1 priede numatytus reikalavimus, keliamus slaptažodžiams.

39. Unikalų prisijungimo vardą ir pirminį slaptažodį darbuotojui ar trečiųjų šalių paslaugų teikėjui suteikia IS administratorius sukūręs paskyrą ir (ar) prieigas.

40. Prisijungimo vardą ir slaptažodį IS administratorius naudotojui tiesiogiai perduoda konfidencialiai žodžiu arba kitomis saugiomis priemonėmis. IS administratorius naudotojui laikiną slaptažodį gali perduoti atviru tekstu, tačiau atskirai nuo prisijungimo vardo, tik jeigu naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

41. Naudotojų ir IS administratorių nuotolinės prieigos prie TIS turi būti apsaugotos naudojant šifravimą ar virtualųjį privatų tinklą (angl. *Virtual private network*, *VPN*).

42. Naudotojams, jungiantis prie kritinių, o IS administratoriams jungiantis prie visų paskyrų ir (ar) TIS turi būti naudojamos kelių veiksnių autentifikavimo (angl. *Multifactor Authentication*, *MFA*) priemonės.

43. Reikalavimai slaptažodžių saugojimui:

43.1. visi slaptažodžiai laikomi konfidencialia informacija ir negali būti atskleisti ar pasidalinti su niekuo įskaitant, bet neapsiribojant, kitu darbuotoju, tiesioginiu vadovu, Žuvininkystės tarnybos direktoriumi, trečiąja šalimi;

43.2. slaptažodžiai negali būti saugomi atviru tekstu ar užšifruojami nepatikimais algoritmais, išskyrus laikinuosius slaptažodžius, kurie išduodami pirmam naudotojo prisijungimui;

43.3. visi naudotojai yra atsakingi už savo prisijungimo duomenų slaptumą;

43.4. jei naudotojas įtaria, jog jo slaptažodis buvo atskleistas, jis apie tai privalo nedelsiant pranešti IS administratoriui ir saugos įgaliotiniui bei nedelsiant pasikeisti savo slaptažodį;

43.5. už slaptažodžių saugojimą, reguliarią peržiūrą ir prieigos kontrolės užtikrinimą yra atsakingas saugos įgaliotinis. Už slaptažodžių valdymo proceso kontrolės įgyvendinimą atsakingas kibernetinio saugumo vadovas.

44. Sisteminės paskyros slaptažodžiai turi būti unikalūs ir skirti tik konkrečiai paskyrai, kuriai taikomi papildomi šios Tvarkos 1 priede numatyti slaptažodžių reikalavimai.

45. Sisteminėms paskyroms bei TIS techninėje ir programinėje įrangoje draudžiama naudoti numatytuosius (angl. *default*) gamintojo slaptažodžius.

46. Darbuotojui draudžiama:

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

46.2. slaptažodžius atskleisti kitiems asmenims ir įvardinti telefoninio pokalbio metu;

46.3. nešifruotus slaptažodžius laikyti bet kur organizacijos patalpose;

46.4. slaptažodžius saugoti elektronine forma bendruose TIS, jei jie yra nešifruoti.

47. IS administratorių slaptažodžiai prie visų TIS gali būti saugomi centralizuotai, naudojant automatizuotą slaptažodžių valdymo sprendimą.

47.1. Rekomenduojama, kad naudotojai slaptažodžius saugotų šifruotoje saugykloje (angl. *password vault*).

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

48. Visi organizacijos darbuotojai ir trečiosios šalys, turintys paskyras ir prieigą prie TIS privalo laikytis šios Tvarkos.

49. Saugos įgaliotinis užtikrina, o kibernetinio saugumo vadovas kontroliuoja, kad naudotojų paskyrų valdymo bei prieigos prie TIS valdymo procesai būtų įgyvendinami pagal šios Tvarkos reikalavimus.

50. Ši Tvarka turi būti peržiūrima ir atnaujinama bent kartą per metus arba kai atsiranda esminiai pokyčiai, kurie turi įtakos šiai Tvarkai. Už šios Tvarkos peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas.

51. Informacinės sistemos naudotojai, Informacinės sistemos administratorius ir Informacinės sistemos saugos įgaliotinis, pažeidę šių Administravimo taisyklių ir kitų saugos politikos įgyvendinamųjų teisės aktų nuostatas, atsako teisės aktuose nustatyta tvarka.

_____

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKOS DOKUMENTO PERŽIŪRA

Dokumento versija	Patvirtinimo data ir Nr.	Dokumento savininkas	Pagrindinės korekcijos
v1.0	2025-06-06 Nr. XXX-I23-130	Kibernetinio saugumo vadovas	Naujai tvirtinama tvarka
V1.1	2025-06-06 Nr. XXX-I23-130	Kibernetinio saugumo vadovas	Taisyklės papildytos nuostatomis atsižvelgiant į kibernetinio saugumo įstatymą.

Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
Prieigų valdymo tvarkos
1 priedas

TECHNINIAI PRIEIGOS VALDYMO IR TAPATUMO NUSTATYMO REIKALAVIMAI

Nr.	Reikalavimo aprašymas[1]	Esminiams	Svarbiems
1.	Tinklų ir informacinių sistemų (toliau – TIS) administratoriaus funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms naudotojo funkcijoms atlikti.	x	x
2.	Naudotojams negali būti suteikiamos IS administratoriaus teisės.	x	x
3.	Kiekvienas naudotojas turi būti unikaliai atpažįstamas.	x	x
4.	Naudotojas ir IS administratorius turi patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksnių tapatumo nustatymo priemonės).	x	x
5.	Naudotojo teisė dirbti su konkrečia TIS turi būti sustabdoma, kai naudotojas nesinaudoja TIS ilgiau kaip 3 mėnesius.	x	x
6.	IS administratoriaus teisė dirbti su TIS turi būti sustabdoma, kai administratorius nesinaudoja TIS ilgiau kaip 2 mėnesius.	x	x
7.	Kai naudotojas ar IS administratorius nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų naudotojo ar IS administratoriaus kvalifikacinių reikalavimų, taip pat pasibaigia jo darbo (tarnybos) santykiai, jis praranda patikimumą, jo teisė naudotis TIS turi būti panaikinta nedelsiant, bet ne vėliau kaip per organizacijos nustatytą terminą.	x	x
8.	Nereikalingos ar nenaudojamos TIS paskyros turi būti blokuojamos nedelsiant, bet ne vėliau kaip per organizacijos nustatytą terminą ir ištrinamos praėjus žurnalinių įrašų saugojimo terminui (ne trumpiau kaip 90 kalendorinių dienų).	x	x
9.	Baigus darbą arba pasitraukiant iš darbo vietos, turi būti atsijungiama nuo tinklų ir informacinių sistemų, įjungiama ekrano užsklanda su slaptažodžiu.	x	x
10.	TIS neatliekant jokių veiksmų, darbo stotis turi užsirakinti (ne ilgiau nei po 15 minučių), kad toliau naudotis tinklų ir informacine sistema būtų galima tik pakartotinai patvirtinus savo tapatybę.	x	x
11.	TIS dalys, tarp jų ir svetainės ir naršyklės, patvirtinančios naudotojo tapatumą, turi drausti išsaugoti slaptažodžius,	x	x

[1] Kibernetinio saugumo subjektams taikomi techniniai reikalavimai, nustatyti Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

Nr.	Reikalavimo aprašymas[1]	Esminiams	Svarbiems
	išskyrus specializuotą slaptažodžių tvarkymo programinę įrangą.		
12.	Slaptažodis turi būti sudarytas iš didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų simbolių.	x	x
13.	Turi būti nustatytas maksimalus leistinas naudotojų mėginimų prisijungti prie TIS skaičius – ne daugiau negu 5 kartai iš eilės. Po numatyto bandymų skaičiaus prisijungti prie TIS, paskyra turi užsiblokuoti. Atblokuoti gali tik įgalioti asmenys.	x	x
14.	Papildomi naudotojo slaptažodžių reikalavimai:		
14.1.	slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius;	x	x
14.2.	slaptažodį turi sudaryti ne mažiau kaip 10 simbolių;	x	x
14.3.	keičiamo slaptažodžio neturi būti leidžiama sudaryti iš buvusių 6 paskutinių slaptažodžių;	x	x
14.4.	pirmąkart jungiantis prie TIS, turi būti reikalaujama, kad naudotojas pakeistų slaptažodį;	x	x
14.5.	naudotojas turi turėti galimybę bet kuriuo metu pasikeisti slaptažodį.	x	x
15.	Papildomi IS administratorių slaptažodžių reikalavimai:		
15.1.	slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius;	x	x
15.2.	slaptažodį turi sudaryti ne mažiau kaip 15 simbolių;	x	x
15.3.	keičiant slaptažodį, neturi būti leidžiama naudoti slaptažodžio iš buvusių 8 paskutinių slaptažodžių.	x	x
16.	Turi būti vykdoma IS administratorių paskyrų kontrolė:		
16.1.	reguliariai, ne rečiau kaip kartą per metus, tikrinama, ar administratoriaus paskyros atitinka šiame skyriuje nustatytus reikalavimus, ir pranešama įgaliotam atsakingam asmeniui apie administratorių paskyras, kurios neatitinka šiame skirsnyje nustatytų reikalavimų;		x
16.2	naudojamos IS administratorių paskyrų kontrolės priemonės, kurios periodiškai tikrina administratoriaus paskyras. Apie IS administratoriaus paskyras, kurios neatitinka šiame skirsnyje nustatytų reikalavimų, turi būti pranešama įgaliotam asmeniui.	x	
17.	Vykdoma naudotojų paskyrų kontrolė:		
17.1.	naudojamos naudotojų paskyrų kontrolės priemonės, kurios periodiškai tikrina naudotojų paskyras. Apie naudotojų paskyras, kurios neatitinka šiame skirsnyje nustatytų reikalavimų, turi būti pranešama įgaliotam asmeniui;		x
17.2.	lokalios naudotojų ir IS administratorių paskyros turi atitikti reikalavimus, nurodytus šiame skirsnyje.	x	

Nr.	Reikalavimo aprašymas[1]	Esminiams	Svarbiems
18.	Papildomi atpažinties, tapatumo patvirtinimo ir naudojimosi kontrolės reikalavimai (Organizacijos pavadinimo trumpinys) svetainėms, pasiekiamoms iš viešųjų elektroninių ryšių tinklų):		
18.1.	programiniame kode draudžiama išsaugoti duomenis (vardą, slaptažodį, aplikacijų programavimo sąsajas (angl. *Application programming interface*) raktus / ženklus (angl. *Token*) ir kt.), kuriuos atskleidus gali būti pasinaudota prieiga prie įrenginių, resursų, paskyrų ar valdiklių.	x	x

PATVIRTINTA
Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos direktoriaus 2026 m. vasario 9 d. įsakymu Nr. V1-27

KIBERNETINIO SAUGUMO REIKALAVIMŲ VEIKSMINGUMO VERTINIMO TVARKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarka (toliau – Tvarka) reglamentuoja Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Žuvininkystės tarnyba) kibernetinio saugumo reikalavimų, nustatytų Lietuvos Respublikos kibernetinio saugumo įstatyme ir Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas), įgyvendinimo stebėjimą, matavimą, analizę ir įvertinimą.

2. Tvarka taikoma visoms Žuvininkystės tarnybos valdomoms tinklų ir informacinėms sistemoms, kibernetinio saugumo valdymo procesams bei taikomoms kibernetinio saugumo organizacinėms ir techninėms priemonėms, skirtoms mažinti kibernetinio saugumo riziką ir užtikrinti kibernetinio saugumo reikalavimų įgyvendinimą.

3. Tvarkoje naudojamos sąvokos:

3.1. **Atitikties vertinimas** – kibernetinio saugumo reikalavimų atitikties Kibernetinio saugumo įstatymo ir Kibernetinio saugumo reikalavimų aprašo bei Žuvininkystės tarnybos patvirtintiems kibernetinio saugumo politikos dokumentuose nustatytiems reikalavimams vertinimas, atliekamas vadovaujantis Kibernetinio saugumo reikalavimų aprašo VIII skyriaus reikalavimais;

3.2. **Kibernetinio saugumo vadovas** – Žuvininkystės tarnybos darbuotojas atsakingas už kibernetinio saugumo subjekto atitikties Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

3.3. **Kontrolės priemonės** – techniniai, organizaciniai ir procedūriniai veiksmai, skirti mažinti informacijos saugumo riziką ir užtikrinti kibernetinio saugumo reikalavimų įgyvendinimą ir užtikrinimą;

3.4. **Rodiklis** – matavimo vienetas, naudojamas kibernetinio saugumo reikalavimų įgyvendinimo veiksmingumui ir tikslų pasiekimui vertinti;

3.5. **Stebėsenos planas** – šios Tvarkos pagrindu parengtas ir Žuvininkystės tarnybos direktoriaus patvirtintas Kibernetinio saugumo reikalavimų įgyvendinimo ir užtikrinimo stebėsenos planas;

3.6. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

4. Žuvininkystės tarnyba turi užtikrinti reikiamus išteklius kibernetinio saugumo reikalavimų įgyvendinimo veiksmingumo stebėsenos ir vertinimo veikloms vykdyti.

II SKYRIUS
KIBERNETINIŲ SAUGUMO REIKALAVIMŲ ĮGYVENDINIMO STEBĖSENA, MATAVIMAS, ANALIZĖ IR VERTINIMAS

5. Kibernetinio saugumo reikalavimų stebėsenai, matavimui, analizei ir įvertinimui užtikrinti yra rengiamas Žuvininkystės tarnybos Stebėsenos planas. Stebėsenos planą kibernetinio saugumo vadovas turi parengti ir Žuvininkystės tarnybos direktoriui pateikti tvirtinti per 3 (tris) mėnesius nuo šios Tvarkos patvirtinimo dienos.

6. Kibernetinio saugumo vadovas Stebėsenos planą rengia atsižvelgdamas į:

6.1. kibernetinio saugumo rizikos vertinimo rezultatus;

6.2. kibernetinio saugumo reikalavimų atitikties Kibernetinio saugumo įstatymo ir atitikties vertinimo rezultatus;

6.3. kibernetinio saugumo audito, atliekamo vadovaujantis Kibernetinio saugumo įstatymo 14 straipsnio 8 dalies nuostatomis, rezultatus;

6.4. kibernetinio saugumo reikalavimų pasiekimo būklę;

6.5. organizacijos kibernetinių incidentų pobūdį ir skaičių;

6.6. trečiųjų šalių paslaugų teikėjams iškeltus kibernetinio saugumo reikalavimus;

6.7. organizacijos veiklos procesų pasikeitimus.

7. Stebėsenos plane turi būti:

7.1. Identifikuotos stebimos kibernetinio saugumo reikalavimų valdymo priemonės;

7.2. nurodomi kokie stebėsenos, matavimo, analizės ir vertinimo metodai pasitelkiami stebėjimui;

7.3. nurodoma kokiu periodiškumu turi būti atliekama nustatytų metodų stebėsena ir matavimai;

7.4. už veiksmingumo vertinimo stebėjimą ir matavimą atsakingas darbuotojas arba padalinys;

7.5. veiksmingumo vertinimo rezultatų analizės periodiškumas;

7.6. taikomų kibernetinių saugumo priemonių gerinimo poreikis ir siūlomos priemonės, atsižvelgiant į vertinimo rezultatus;

8. Kibernetinio saugumo vadovas Stebėsenos planą peržiūrį ir, jei reikia, atnaujina ne rečiau kaip kartą per metus.

9. Organizacijos darbuotojas, atsakingas už Stebėsenos plane numatytų rodiklių stebėjimą, informaciją apie rodiklių būklę suveda į Stebėsenos planą jame numatytais terminais.

10. Kibernetinio saugumo vadovas kartą į ketvirtį rengia ir Žuvininkystės tarnybos direktoriaus peržiūrai teikia tarpinę Stebėsenos plano rodiklių pasiekimų ataskaitą, o metų pabaigoje – metinę Stebėsenos plano rodiklių pasiekimų ataskaitą.

11. Kibernetinio saugumo vadovas, įvertinęs, kad stebimas kibernetinio saugumo reikalavimų rodiklis neatitinka nustatytų reikšmių, turi nustatyti neatitikties priežastį ir pagerinti neatitikčių šalinimo planą.

12. Stebėsenos plano duomenys vertinami atsižvelgiant į įstaigos rizikos vertinimą, bei incidentus.

13. Remiantis Stebėsenos plano rezultatais gali būti peržiūrimas organizacijos rizikos valdymo priemonių planas ir, esant poreikiui, koreguojami jame įvardintų konkrečių priemonių įgyvendinimo prioritetai arba papildoma naujomis kontrolės priemonėmis.

III SKYRIUS
ATITIKTIES VERTINIMAS

14. Kibernetinio saugumo vadovas ne rečiau kaip kartą į metus organizuoja atitikties vertinimą, tam pasitelkdamas saugos įgaliotinį. Atitikties vertinimui gali būti pasitelkiamos trečiosios šalys.

15. Saugos įgaliotinis, atlikęs atitikties vertinimą, Kibernetinio saugumo informacinės sistemos (toliau – KSIS) savideklaracijos klausimyno pagrindu turi parengti ir kibernetinio saugumo vadovui pateikti atitikties vertinimo ataskaitą ir atitikties vertinimo metu identifikuotų neatitikčių šalinimo planą, kuriame turi būti nurodyti už neatitikčių šalinimo veiksmus atsakingi darbuotojai ir (ar) padaliniai, šalinimui reikalingi ištekliai ir nustatyti šalinimo veiksmų įgyvendinimo terminai (toliau – neatitikčių šalinimo planas). Kibernetinio saugumo vadovas atitikties vertinimo ataskaitą ir atitikties vertinimo metu identifikuotų neatitikčių šalinimo planą teikia tvirtinti Žuvininkystės tarnybos direktoriui vidaus teisės aktų nustatyta tvarka. Iki bus įgyvendinti neatitikčių šalinimo plane numatyti veiksmai, organizacija, pagal galimybes, turi taikyti kompensacines priemones.

16. Esminio kibernetinio saugumo subjekto kibernetinio saugumo vadovas po atitikties vertinimo turi ne rečiau kaip kartą per metus pateikti atitikties vertinimo rezultatus, KSIS

užpildydamas Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) klausimyną.

17. Kibernetinio saugumo vadovas, vadovaudamasis Kibernetinio saugumo įstatymo 14 straipsnio 8 punkto nuostatomis, ne rečiau kaip kartą per 3 metus turi organizuoti organizacijos kibernetinio saugumo audito atlikimą. Kibernetinio saugumo auditas turi būti atliktas pagal NKSC tvirtinamą kibernetinio saugumo auditų atlikimo metodiką. Kibernetinio saugumo auditą turi atlikti nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų saugumo atitikties auditoriai, audito įmonės ar kitos institucijos, NKSC vadovo nustatyta tvarka mokymus išklausę ir kvalifikacinius žinių ir praktinių įgūdžių patikrinimo egzaminą išlaikę asmenys, kurie atitinka NKSC kibernetinio saugumo auditų atlikimo metodikoje nustatytus nepriklausomumo, nešališkumo ir nepriekaištingos reputacijos reikalavimus (toliau kartu – Auditoriai). Auditoriams negali būti pavedama vertinti TIS, kurias valdo ir (ar) tvarko subjektas, kuriame dirba auditorius, kibernetinio saugumo valdymo.

18. Atlikus kibernetinio saugumo auditą, Auditorius turi parengti ir kibernetinio saugumo vadovui pateikti kibernetinio saugumo audito ataskaitą, su kuria kibernetinio saugumo vadovas turi supažindinti Žuvininkystės tarnybos direktorių, kitų suinteresuotų padalinių vadovus ir kitas suinteresuotas šalis. Kibernetinio saugumo vadovas per 10 darbo dienų nuo kibernetinio saugumo audito ataskaitos pateikimo dienos turi parengti ir Žuvininkystės tarnybos direktoriui teikti tvirtinti kibernetinio saugumo audito metu identifikuotų neatitikčių (jei nustatyta) šalinimo planą, kuriame turi būti nurodyti už šalinimo veiksmus atsakingi darbuotojai ir (ar) padaliniai, šalinimui reikalingi ištekliai ir nustatyti šalinimo veiksmų įgyvendinimo terminai.

19. Kibernetinio saugumo vadovas atitikties vertinimų ir kibernetinio saugumo auditų ataskaitas bei identifikuotų neatitikčių (jei nustatyta) šalinimo planus turi saugoti ne mažiau kaip 3 metus nuo Žuvininkystės tarnybos direktoriaus patvirtinimo ir jų parengimo dienos.

20. NKSC, atlikdamas Žuvininkystės tarnybos patikrinimą, turi teisę pareikalauti Žuvininkystės tarnybos pateikti atliktų kibernetinio saugumo audito, atitikties vertinimo ataskaitos, atitikties vertinimo metu nustatytų neatitikčių šalinimo plano, rizikų vertinimo ataskaitos ir rizikų valdymo plano kopijas. Kibernetinio saugumo vadovas šiuos dokumentus turi pateikti į KSIS ne vėliau kaip per 5 darbo dienas nuo NKSC prašymo gavimo dienos.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

21. Ši Tvarka turi būti peržiūrima ir atnaujinama bent kartą per metus arba kai atsiranda esminiai pokyčiai Žuvininkystės tarnyboje, kurie turi įtakos šiai Tvarkai. Už šios Tvarkos peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas.

22. Visi su kibernetinio saugumo reikalavimų stebėsena susiję įrodymai turi būti saugomi užtikrinant jų konfidencialumą, vientisumą ir prieinamumą tik organizacijos įgaliotiems darbuotojams, kurie dalyvauja kibernetinio saugumo reikalavimų stebėsenos, matavimo, analizės ir įvertinimo procese.

23. Organizacijos darbuotojai, dalyvaujantys kibernetinio saugumo reikalavimų stebėsenos, matavimo, analizės ir įvertinimo procese, privalo laikytis šios Tvarkos reikalavimų.

_____

KIBERNETINIO SAUGUMO REIKALAVIMŲ VEIKSMINGUMO VERTINIMO TVARKOS PERŽIŪRA

Dokumento versija	Patvirtinimo data ir Nr.	Dokumento savininkas	Pagrindinės korekcijos
v1.0	2025-06-06 Nr. XXX-I23-130	Kibernetinio saugumo vadovas	Naujai tvirtinama tvarka

PATVIRTINTA
Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos direktoriaus 2026 m. vasario 9 d. įsakymu Nr. V1-27

KRIPTOGRAFIJOS IR ŠIFRAVIMO NAUDOJIMO TVARKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kriptografijos ir šifravimo naudojimo tvarka (toliau – Tvarka) reglamentuoja Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Žuvininkystės tarnyba) kriptografinių raktų naudojimo tikslus ir saugų jų valdymą.

2. Tvarkoje naudojamos sąvokos:

2.1. **Asimetrinis šifravimas** – šifravimo metodas, kuriame naudojama tarpusavyje susietų kriptografinių raktų pora: viešasis kriptografijos raktas ir privatusis kriptografijos raktas. Viešasis raktas naudojamas elektroninei informacijai šifruoti arba parašo autentifikavimui, o privatusis raktas – informacijai iššifruoti arba skaitmeniniam parašui kurti. Šių raktų tarpusavio ryšys užtikrina, kad informacija liktų saugi ir būtų tinkamai autentifikuota;

2.2. **Ilgalaikė saugykla** – tai fizinė arba programinė laikmena, debesijos paslauga ar raktų valdymo įrenginys, skirtas kriptografinių raktų ar kitos jautrios informacijos saugojimui ilgesnį laiką;

2.3. **Kriptografijos kontrolės priemonės** – tai techninės ir organizacinės priemonės, naudojamos duomenų šifravimui, apsaugai nuo neteisėtos prieigos ir informacijos konfidencialumo, vientisumo bei autentiškumo užtikrinimui;

2.4. **Kriptografinis raktas** – elektroninės informacijos šifravimui ir (arba) dešifravimui naudojama papildoma informacija;

2.5. **MAC adresas** (angl. *Media Access Control address*) – tai unikalus identifikatorius, priskiriamas tinklo įrenginio tinklo sąsajai, pvz., kompiuterio, maršrutizatoriaus, išmaniojo telefono ar spausdintuvo tinklo plokštei);

2.6. **Privatusis raktas** (angl. *Private Key*) – konfidencialus kriptografijos raktas, naudojamas elektroninei informacijai iššifruoti, kuri užšifruota viešuoju kriptografijos raktu;

2.7. **Ryšio šifravimas** – duomenų šifravimas duomenų perdavimo metu, užtikrinant jų konfidencialumą ir vientisumą. Tam naudojamų įrankių pavyzdžiai: TLS (angl. *Transport Layer Security*) protokolas, VPN (angl. *Virtual Private Network*), RDP (angl. *Remote Desktop Protocol*) ir kt.;

2.8. **Simetrinis šifravimas** – šifravimo metodas, kuriame tam pačiam kriptografijos raktui tenka dvejopa funkcija – tiek elektroninės informacijos šifravimo, tiek iššifravimo;

2.9. **Šifravimas** – kriptografinis elektroninės informacijos formos pakeitimas iš paprastos į specifinę, iš kurios elektroninę informaciją pakeisti į pradinę formą galima tik turint atitinkamą kriptografijos raktą;

2.10. **Šifravimo algoritmas** – matematinis procesas, naudojamas duomenims šifruoti ir iššifruoti, atitinkantis tarptautinius saugumo standartus, pvz.: AES (angl. *Advanced Encryption Standard*), RSA (angl. *Rivest–Shamir–Adleman*), ECC (angl. *Elliptic Curve Cryptography*), SHA-3 (angl. *Secure Hash Algorithm v3*);

2.11. **Viešasis raktas** (angl. *Public Key*) – laisvai prieinamas ir platinamas kriptografijos raktas, naudojamas elektroninei informacijai, siunčiamai viešojo kriptografijos rakto savininkui, šifruoti;

2.12. **Viešojo rakto infrastruktūra** (angl. *Public Key Infrastructure, PKI*) – tai standartizuotų technologinių ir organizacinių priemonių visuma, leidžianti saugiai valdyti viešuosius raktus ir jų pagrindu išduodamus skaitmeninius sertifikatus. Viešojo rakto infrastruktūra apima raktų generavimą, sertifikatų išdavimą, paskirstymą, naudojimą, galiojimo nutraukimą (atšaukimą) ir audito vykdymą. Viešojo rakto infrastruktūros pagrindiniai komponentai yra sertifikavimo centrai (angl. *Certificate Authority, CA*), registravimo institucijos (angl. *Registration Authority, RA*), sertifikatų paskirstymo priemonės, atšaukimo informacijos mechanizmai pvz., CRL (angl. *Certificate Revocation List*), OCSP (angl. *Online Certificate Status Protocol*) ir pasitikėjimo politikos.

3. Už šios Tvarkos tinkamą vykdymą atsakingas Žuvininkystės tarnybos kibernetinio saugumo vadovas.

II SKYRIUS
KRIPTOGRAFINIŲ RAKTŲ NAUDOJIMO TIKSLAI

4. Kriptografijos kontrolės priemonės gali būti naudojamos siekiant šių kibernetinio saugumo tikslų:

4.1. Konfidencialumo (angl. *Confidentiality*) – tiek saugomos, tiek perduodamos informacijos apsaugai, naudojant informacijos šifravimą;

4.2. Vientisumo ir (arba) autentiškumo (angl. *Integrity and/or Authenticity*) – saugomos arba perduodamos informacijos patikrai, naudojant skaitmeninius parašus ar pranešimų autentiškumo patvirtinimo kodus;

4.3. Negalėjimo išsižadėti (angl. *Non-repudiation*) – įvykusio arba neįvykusio veiksmo ar įvykio įrodymui, naudojant kriptografinius metodus;

4.4. Tapatybės patvirtinimo (angl. *Authentication*) – naudotojų ir kitų tinklų ir informacinių sistemų (toliau – TIS) subjektų, prašančių prieigos prie TIS ar vykdančių operacijas su jos ištekliais, tapatybės patvirtinimui naudojant kriptografines priemones;

4.5. Prieinamumo (angl. *Availability*) – informacijos ir paslaugų prieigos užtikrinimui, pvz., naudojant kriptografines apsaugos priemones nuo paslaugos trikdymo ar neleistino išteklių naudojimo.

5. Kriptografijos kontrolės priemonės gali būti naudojamos įvairiems tikslams, atsižvelgiant į duomenų būseną ir saugumo funkciją:

5.1. Duomenų apsaugai perdavimo metu (angl. *Data in transit*):

5.1.1. informacijos šifravimui tarp naudotojų ar TIS per komunikacijos kanalus (pvz., TLS, VPN, RDP);

5.1.2. informacijos perdavimui mobiliaisiais įrenginiais arba kitais ryšio kanalais.

5.2. Duomenų apsaugai saugojimo metu (angl. *Data at rest*):

5.2.1. pilnam disko šifravimui (pvz., *BitLocker, VeraCrypt*);

5.2.2. nešiojamųjų ir stacionariųjų laikmenų šifravimui;

5.2.3. atsarginių kopijų šifravimui;

5.2.4. duomenų bazių šifravimui.

5.3. Duomenų apsaugai apdorojimo metu (angl. *Data in use*):

5.3.1. tarnybinės stoties tapatybės patvirtinimui šifruotų seansų metu (pvz., naudojant TLS sertifikatus);

5.3.2. kriptografinėms priemonėms, naudojamoms realaus laiko autentifikacijai ar pasirašymui.

5.4. Tapatybės patvirtinimui ir prieigos kontrolei (angl. *Identity & access control*):

5.4.1. el. parašui ir el. pašto pasirašymui;

5.4.2. naudotojų ar įrenginių autentifikacijai (pvz., viešojo rakto pagrindu);

5.4.3. aktyvios tinklo įrangos autorizavimui kompiuteriniame tinkle.

5.5. Kitais atvejais, kai būtina užtikrinti informacijos konfidencialumą, vientisumą, prieinamumą ar autentiškumą.

III SKYRIUS
KRIPTOGRAFINIŲ RAKTŲ VALDYMAS

6. Kriptografinių raktų gyvavimo ciklą sudaro šios fazės:

6.1. Generavimas – tai procesas, kurio metu sukuriamas unikalus raktas, naudojamas duomenų šifravimui ir iššifravimui. Raktas kuriamas naudojant kriptografinius algoritmus ir atsitiktinių skaičių generatorius.

6.2. Paskirstymas – saugus rakto perdavimas tiems, kam jis reikalingas, kad būtų galima naudoti šifravimui ar iššifravimui.

6.3. Saugojimas – rakto laikymas apsaugotoje aplinkoje, kad būtų išvengta neteisėtos

prieigos.

6.4. Naudojimas – aktyvus rakto naudojimas šifravimo, iššifravimo, skaitmeninio pasirašymo ar autentifikavimo procesams.

6.5. Atnaujinimas – periodinis seno rakto pakeitimas nauju, siekiant sumažinti kompromitacijos riziką.

6.6. Deaktyvavimas (arba atšaukimas) – rakto galiojimo pabaiga arba sąmoningas jo galiojimo nutraukimas.

6.7. Sunaikinimas – veiksmas, kuriuo raktas negrįžtamai pašalinamas taip, kad jo nebūtų įmanoma atkurti. Tai užtikrina, kad raktas nebus panaudotas neteisėtai.

7. Simetriniai raktai (angl. *symmetric keys*) naudojami šifravimo procesuose, kuriuose tiek šifravimui, tiek iššifravimui naudojamas tas pats raktas. Taikomi šiose srityse:

7.1. Saugyklose ir atsarginėse kopijose esančių duomenų šifravimui (pvz., atsarginių kopijų apsaugai);

7.2. Galinių įrenginių duomenų laikmenų šifravimui;

7.3. Duomenų bazių eilučių/stulpelių šifravimui;

7.4. Failų lygmens (angl. *file-level*) šifravimui dokumentų valdymo sistemose;

7.5. Tinklo ryšio duomenų šifravimui;

7.6. Debesijos paslaugose esančių duomenų šifravimui, kai naudojamas paslaugos teikėjo arba kliento valdomas raktas;

7.7. Mobiliojo ryšio įrenginių šifravimui (jei taikomas mobiliųjų įrenginių valdymo sprendimas (angl. *Mobile Device Management, MDM*));

7.8. Virtualių mašinų ir konteinerių šifravimui (diskų ar konteinerių saugojimui).

8. Asimetriniai raktai (angl. *asymmetric keys*) naudojami poromis – viešasis raktas šifravimui ar parašo tikrinimui, o privatusis – iššifravimui ar parašo generavimui. Jie taikomi šiose srityse:

8.1. skaitmeninio parašo generavimui ir tikrinimui, siekiant užtikrinti autentiškumą, vientisumą ir neišsižadėjimą;

8.2. naudotojų, įrenginių ir TIS autentifikavimui;

8.3. viešojo rakto infrastruktūroje (angl. *Public Key Infrastructure, PKI*) raktų mainams, sertifikatų pasirašymui;

8.4. el. pašto turinio ir priedų šifravimui;

8.5. partnerių ar teikėjų raktų importui, kai naudojamas viešasis raktas duomenims perduoti saugiai.

9. Kriptografiniai raktai naudojami:

9.1. šifravimo pagalba užtikrinti duomenų konfidencialumą;

9.2. kriptografinės maišos (angl. *hash*) ir skaitmeninio parašo funkcijomis užtikrinti duomenų vientisumą;

9.3. MAC adreso ir skaitmeninio parašo pagalba nustatyti naudotojo, patvirtinančio savo tapatybę, tapatumą;

9.4. skaitmeninio parašo pagalba užtikrinti atliktų veiksmų neišsižadėjimą.

10. Už kriptografinių raktų valdymą organizacijoje atsakingi IT administratoriai.

11. Praradus kriptografinį raktą arba įtariant, kad jį naudoja pašaliniai asmenys, IT administratorius turi nedelsiant informuoti kibernetinio saugumo vadovą.

12. Tarnybinės stoties tapatybės užtikrinimui, duomenų šifravimui tarp tarnybinės stoties ir kliento kompiuterio naudojami TLS sertifikatai.

13. Techniniai reikalavimai kriptografinėms priemonėms pateikiami šios Tvarkos 1 priede.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

14. Ši Tvarka turi būti peržiūrima ir atnaujinama bent kartą per metus arba kai atsiranda esminiai pokyčiai Žuvininkystės tarnyboje, kurie turi įtakos šiai Tvarkai. Už šios Tvarkos peržiūrėjimą ir atnaujinimą yra atsakingas Kibernetinio saugumo vadovas.

_____

KRIPTOGRAFIJOS IR ŠIFRAVIMO NAUDOJIMO TVARKOS PERŽIŪRA

Dokumento versija	Patvirtinimo data ir Nr.	Dokumento savininkas	Pagrindinės korekcijos
v1.0	2025-06-06 Nr. XXX-I23-130	Kibernetinio saugumo vadovas	Naujai tvirtinama tvarka

Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
Kriptografijos ir šifravimo naudojimo
tvarkos
1 priedas

TECHNINIAI KRIPTOGRAFIJOS IR ŠIFRAVIMO NAUDOJIMO REIKALAVIMAI

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams[1]	Esminiams	Svarbiems
1.	Viešaisiais elektroninių ryšių tinklais perduodamos kibernetinio saugumo subjektui jautrios informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą ar virtualųjį privatų tinklą (angl. *Virtual private network,* VPN).	x	x
2.	Belaidis ryšys turi būti šifruojamas pagal gerąją saugumo praktiką rekomenduojamu šifravimo ilgio raktu. Naudoti visuotinai saugiais pripažįstamus raktus ir protokolų versijas. Belaidės prieigos stotelėje turi būti pakeisti standartiniai gamintojo raktai.	x	x
3.	Duomenys, perduodami tarp mobiliojo įrenginio ir TIS, turi būti šifruojami taikant virtualaus privataus tinklo (VPN) technologiją su TLS / SSL sertifikatu arba naudojama privataus prieigos taško (angl. *Access Point Name*, APN) per mobiliojo ryšio operatorių technologija, taikant perduodamų duomenų šifravimą sraute su TLS / SSL sertifikatu, kai VPN technologija nėra palaikoma mobiliųjų įrenginių.	x	x
4.	Mobiliųjų įrenginių laikmenose ir išorinėse kompiuterinėse laikmenose laikomi TIS duomenys turi būti šifruojami.	x	x
5	Turi būti įgyvendinti svetainės kriptografijos reikalavimai:		
5.1.	turi būti naudojami oficialiai pripažinti saugus ilgio raktai;	x	x
5.2.	atliekant svetainės administravimo darbus, ryšys turi būti šifruojamas;	x	x
5.3.	šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų;	x	x
5.4.	turi būti naudojamas TLS standartas (1.3 versija arba naujesnė);	x	
5.5.	svetainės kriptografinės funkcijos turi būti įdiegtos serverio, kuriame yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. *Hardware security module*);	x	x
5.6.	visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. *fail securely*).	x	
6.	Duomenys atsarginėse kopijose turi būti užšifruoti (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų informacijai neteisėtai atkurti.	x	x
7.	Turi būti saugomi ir stebimi audito įrašai, susiję su kriptografinių raktų valdymo veikla (generavimas, sunaikinimas, archyvavimas, naudotojų veiksmai).	x	x

[1] Kibernetinio saugumo subjektams taikomi techniniai reikalavimai pagal Kibernetinio saugumo reikalavimų aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, nurodyti 4 lentelėje.

PATVIRTINTA
Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos direktoriaus 2026 m. vasario 9 d. įsakymu Nr. V1-27

TINKLŲ IR INFORMACINIŲ SISTEMŲ ĮSIGIJIMO, PLĖTOJIMO IR PRIEŽIŪROS SAUGUMO, ĮSKAITANT SPRAGŲ VALDYMĄ IR ATSKLEIDIMĄ, TVARKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, tvarka (toliau – Tvarka) reglamentuoja Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Žuvininkystės tarnyba) tinklų ir informacinių sistemų (toliau – TIS) įsigijimo, plėtojimo ir priežiūros viso TIS gyvavimo ciklo metu, TIS pokyčių ir pataisų valdymo, TIS saugumo spragų valdymo ir atskleidimo, taip pat Žuvininkystės tarnybos taikomų techninių reikalavimų, numatytų šios Tvarkos 1 priede, užtikrinimo planavimo, organizavimo, vykdymo ir įgyvendinimo kontrolės proceso eigą, atsakingų padalinių ir darbuotojų funkcijas ir atsakomybes, siekiant, kad organizacija tinkamai valdytų TIS įsigijimą, plėtojimą ir priežiūrą bei TIS pokyčius ir pataisas, atskleistų ir šalintų TIS esamas ir (ar) žinomas saugumo spragas, taip pat tinkamai įgyvendintų joms keliamus techninius reikalavimus.

2. Šioje Tvarkoje vartojamos sąvokos:

2.1. **Kibernetinio saugumo vadovas –** Žuvininkystės tarnybos darbuotojas atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

2.2. **Pokyčio iniciatorius** – Žuvininkystės tarnybos darbuotojas, inicijavęs tinklų ir informacinių sistemų pokytį;

2.3. **Pokyčio vykdytojas** – Žuvininkystės tarnybos darbuotojas ar paslaugų teikėjo įgaliotas asmuo, įgyvendinantis tinklų ir informacinių sistemų pokytį;

2.4. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

2.5. **Tinklų ir informacinių sistemų programinės įrangos atnaujinimas** (angl. *release*) **–** TIS programinės įrangos gamintojo paskelbta informacija apie tinklų ir informacinių sistemų programinės įrangos atnaujinimą ar atnaujinimų rinkinį;

2.6. **Tinklų ir informacinių sistemų programinės įrangos pataisa** (toliau **–** Pataisa) (angl. *patch*) – TIS programinės įrangos atnaujinimas ar atnaujinimų rinkinys, skirtas patobulinti tinklų ir informacinių sistemų programinę įrangą, ištaisyti jos veikimo sutrikimus ir (ar) programiniame kode esančias klaidas ir (ar) saugumo spragas;

2.7. **Tinklų ir informacinių sistemų kūrimas** – TIS diegimo, konfigūravimo, programavimo darbų ir licencijų (jei taikoma) įsigijimas;

2.8. **Tinklų ir informacinių sistemų likvidavimas** – procesas, kuris inicijuojamas panaikinus veiklos funkciją (funkcijas), kuriai vykdyti buvo sukurta TIS;

2.9. **Tinklų ir informacinių sistemų pokytis –** TIS techninės ar programinės įrangos ar programinio kodo pakeitimas, siekiant patobulinti tinklų ir informacinių sistemų funkcionalumą ar pašalinti saugumo spragą;

2.10. **Tinklų ir informacinių sistemų priežiūra** – pokyčiai TIS, nereikalaujantys arba reikalaujantis minimalių programavimo/konfigūravimo darbų;

2.11. **Tinklų ir informacinių sistemų saugumas** – TIS pajėgumas tam tikru patikimumo lygiu išlikti atspariems bet kokiam įvykiui, galinčiam sukelti pavojų saugomų, perduodamų ar tvarkomų duomenų arba per tas tinklų ir informacines sistemas teikiamų arba gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui;

2.12. **Tinklų ir informacinių sistemų saugumo vertinimas** (toliau – Saugumo vertinimas) – Žuvininkystės tarnybos padalinio ar jo darbuotojo arba trečiosios šalies atliekamas tinklų ir informacinių sistemų saugumo vertinimas ar automatizuotas skenavimas, naudojant automatizuotus skenavimo įrankius (toliau – VMS įrankis) (angl. *Vulnerability management scanner*) ar programinio kodo saugumo vertinimas (angl. *a Code security review*) ar kitų saugumo spragų nustatymo būdų (pvz. įsilaužimų testavimą) įgyvendinimą, kurio tikslas įvertinti, ar TIS neturi esamų ar žinomų saugumo spragų;

2.13. **Tinklų ir informacinių sistemų skenavimas** – tai TIS saugumo spragų nustatymo ir vertinimo būdas, kuomet Žuvininkystės tarnybos darbuotojai ir (ar) trečiosios šalys, naudodamos VMS ir kitus įrankius atlieka TIS, įskaitant, tačiau neapsiribojant valdomų ir tvarkomų TIS programinės įrangos, programinio kodo, kompiuterizuotų darbo ir gamybos vietų ir kitos įrangos, skenavimais, siekiant nustatyti, ar nėra esamų ar žinomų saugumo spragų;

2.14. **Tinklų ir informacinės sistemos spraga –** TIS trūkumas, įskaitant informacinių ir ryšių technologijų produktų arba informacinių ir ryšių technologijų paslaugų trūkumus, dėl kurio gali įvykti kibernetinis incidentas ar kuriuo gali būti pasinaudota kibernetinei grėsmei kelti;

2.15. **Tinklų ir informacinės sistemos spragų atskleidimas** (toliau – Spragų atskleidimas) – Žuvininkystės tarnybos darbuotojų ir (ar) trečiųjų šalių atliekami veiksmai (pvz. TIS skenavimai,

informacijos surinkimas ar gavimas iš įvairų šaltinių ir pan.), norint surasti ir nustatyti esamas ar žinomas TIS saugumo spragas;

2.16. **Tinklų ir informacinės sistemos spragų šalinimas** (toliau – Spragų šalinimas) Žuvininkystės tarnybos darbuotojų ir (ar) trečiųjų šalių atliekami veiksmai TIS (pvz., programinės įrangos atnaujinimai, konfigūracijų keitimai, pasiekiamumo ribojamai, atitinkamų techninių priemonių įsigijimas ir diegimas bei kiti veiksmai), siekiant tinkamai pašalinti TIS nustatytas ir įvertintas esamas ar žinomas spragas (angl. *exploiting of known vulnerabilities*);

2.17. **Tinklų ir informacinės sistemos spragų valdymas** (toliau – Spragų valdymas) **–** spragų atskleidimas, jų vertinimas ir šalinimas;

2.18. **Tinklų ir informacinės sistemos spragų vertinimas** (toliau – Spragų vertinimas) – Žuvininkystės tarnybos darbuotojų ir (ar) trečiųjų šalių atliekami veiksmai, siekiant įvertinti nustatytas esamas ar žinomas spragas, t. y. įvertinti jų keliamą riziką esamoje aplinkoje, pašalinti netikras ar neteisingai identifikuotas spragas (angl. *false positive*) ir pagal TIS spragų vertinimo klasifikatorių priskirti juos prie atitinkamų rizikos lygių;

2.19. **Tinklų ir informacinių sistemų spragų vertinimo klasifikatorius** (angl. *the Common Vulnerability Scoring System Base Score)* (toliau – CVSS) – organizacijos FIRST (angl. *Forum of Incident Response and Security Teams*) parengtas ir tarptautiniu mastu pripažintas techninis standartas, skirtas tinklų ir informacinių sistemų saugumo spragoms įvertinti (aktuali versija https://www.first.org/cvss/v4-0/).

3. Kitos šioje Tvarkoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Lietuvos Respublikos kibernetinio saugumo įstatyme bei tarptautinių standartų ISO 27000 ir ISO 20000 grupėse.

4. Tvarka taikoma visoms Žuvininkystės tarnybos valdomoms TIS, numatytoms Turto valdymo tvarkoje.

II SKYRIUS
ATSAKINGŲ PADALINIŲ IR DARBUOTOJŲ FUNKCIJOS IR ATSAKOMYBĖS

5. Kibernetinio saugumo vadovas atsako už:

5.1. šios Tvarkos koordinavimą ir įgyvendinimo kontrolę;

5.2. kibernetinio saugumo reikalavimų nustatymo ir įgyvendinimo kontrolę TIS kūrimo, įsigijimo, priežiūros ir plėtros metu;

5.3. kibernetinio saugumo reikalavimų įgyvendinimo užtikrinimo kontrolę TIS pokyčių ir pataisų valdymo procesuose;

5.4. TIS saugumo vertinimo inicijavimą, koordinavimą ir įgyvendinimo kontrolę;

5.5. TIS saugumo vertinimo įgyvendinimo plano (toliau – Spragų nustatymo planas) tvirtinimą;

5.6. TIS kritinės ir aukštos rizikos lygio saugumo spragos šalinimo koordinavimą ir įgyvendinimo kontrolę;

5.7. techninių reikalavimų, taikomų organizacijoje, įgyvendinimo kontrolę;

5.8. šios Tvarkos periodinę peržiūrą ir atnaujinimą.

6. Saugos įgaliotinis atsako už:

6.1. kibernetinio saugumo reikalavimų nustatymą TIS kūrimo, įsigijimo, priežiūros ir plėtros metu bei šių reikalavimų įgyvendinimo organizavimą;

6.2. kibernetinio saugumo reikalavimų įgyvendinimo TIS pokyčių ir pataisų valdymo procesuose užtikrinimą;

6.3. Spragų nustatymo plano parengimą ir jo suderinimą su kibernetinio saugumo vadovu;

6.4. saugumo spragų atskleidimo organizavimą;

6.5. saugumo vertinimų pagal Spragų nustatymo planą organizavimą bei Kibernetinio saugumo įstatyme ir jo įgyvendinimą reglamentuojančiuose teisės aktuose nustatyta tvarka ir periodiškumu (ne rečiau kaip kas 6 mėnesius) visų TIS saugumo spragų skenavimų organizavimą;

6.6. TIS saugumo vertinimo užduočių tiekėjams parengimą;

6.7. TIS saugumo vertinimo ataskaitų iš paslaugų tiekėjų gavimą ir jų suderinimą;

6.8. spragų, apie kurias informacija gauta pagal Kibernetinio saugumo įstatymo 25 straipsnį, tyrimo organizavimą ir informacijos teikimą;

6.9. atskleistų saugumo spragų įvertinimą pagal CVSS klasifikatorių, esant poreikiui informacijos saugumo rizikos vertinimo atlikimą;

6.10. TIS saugumo spragų registravimą šioje Tvarkoje numatytomis priemonėmis ir šios informacijos atnaujinimą;

6.11. TIS kritinės ir aukštos rizikos lygio saugumo spragos šalinimo inicijavimą;

6.12. TIS vidutinės ir žemos rizikos lygio saugumo spragų šalinimo plano parengimą, pavedimą organizacijos atsakingiems padaliniams ir darbuotojams pašalinti jas šioje Tvarkoje nustatyta tvarka ir terminais bei jų šalinimo koordinavimą ir įgyvendinimo kontrolę;

6.13. TIS saugumo spragų šalinimo eigos įgyvendinimo kontrolę šioje Tvarkoje nustatyta tvarka ir dažnumu;

6.14. techninių reikalavimų, taikomų organizacijoje, įgyvendinimo organizavimą ir koordinavimą;

6.15. konsultacijų, susijusių su TIS saugumo vertinimais ar saugumo spragų atskleidimu, jų įvertinimu ir šalinimu bei pagalbos teikimą kitiems saugumo spragų valdyme dalyvaujantiems organizacijos padaliniams ir jų darbuotojams.

7. IS administratorius atsako už:

7.1. TIS kūrimo, priežiūros ir plėtros organizavimą ir įgyvendinimą bei tokių paslaugų įsigijimo iš tiekėjų inicijavimą;

7.2. informacijos apie planuojamą saugumo vertinimo pateikimą saugos įgaliotiniui;

7.3. kitos informacijos, susijusios su TIS, kurio atžvilgiu turi būti atliktas saugumo vertinimas, pateikimą saugos įgaliotiniui, TIS savininkui, kitiems organizacijos darbuotojams ir paslaugų tiekėjams;

7.4. informacijos apie TIS programinės įrangos (toliau – PĮ) gamintojų paskelbtus TIS PĮ atnaujinimus surinkimą;

7.5. informacijos apie TIS PĮ gamintojo paskelbtą TIS PĮ atnaujinimą pateikimą organizacijos atsakingiems darbuotojams;

8. IT padalinio vadovas atsako už:

8.1. kibernetinio saugumo reikalavimų įgyvendinimą TIS kūrimo, įsigijimo, priežiūros ir plėtros metu;

8.2. kibernetinio saugumo reikalavimų įgyvendinimą TIS eksploatavimo ir priežiūros metu;

8.3. kibernetinio saugumo reikalavimų įgyvendinimą TIS likvidavimo metu;

8.4. TIS pokyčių ir pataisų valdymo organizavimą ir įgyvendinimą;

8.5. saugumo spragų šalinimo organizavimą ir įgyvendinimą šioje Tvarkoje nustatyta tvarka ir terminais, nebent saugos įgaliotinis savo pavedimu saugumo spragų šalinimo veiksmus paveda atlikti kitam organizacijos padaliniui ar jo darbuotojui ar paslaugų tiekėjui;

8.6. TIS PĮ atnaujinimo organizavimą ir įgyvendinimą šioje Tvarkoje nustatyta tvarka ir terminais;

8.7. savalaikį saugos įgaliotinio bei TIS savininko informavimą apie pašalintą saugumo spragą šioje Tvarkoje nustatyta tvarka ir terminais.

9. TIS savininkas atsako už:

9.1. TIS įsigijimo inicijavimą ir planavimą;

9.2. TIS įsigijimo rezultatų įvertinimą;

9.3. sprendimo dėl TIS likvidavimo priėmimą;

9.4. sprendimo dėl TIS pokyčių įgyvendinimo bei pokyčio įgyvendinimo plano patvirtinimo, priėmimą;

9.5. pokyčių rezultatų įvertinimą.

10. Pokyčio iniciatorius atsako už:

10.1. reikiamų duomenų, susijusių su inicijuojamu pokyčiu, teikimą pokyčių valdymo proceso dalyviams, vertina pokyčio rezultatų atitiktį planuotiems rezultatams;

10.2. galutinių pokyčio rezultatų įvertinimą ir patvirtinimą;

10.3. TIS pokyčių planavimo eigos fiksavimą šioje Tvarkoje numatytomis priemonėms;

11. Pokyčio vykdytojas atsako už:

11.1. pokyčio įgyvendinimą ir įgyvendinimo eigos kontrolę šioje Tvarkoje nustatyta tvarka ir terminais;

11.2. TIS naudotojų ir kitų suinteresuotų asmenų informavimą apie pokyčius, kurių įgyvendinimo metu galimi TIS darbo sutrikimai, šioje Tvarkoje nustatyta tvarka ir terminais;

11.3. pokyčio iniciatoriaus, TIS savininko saugos įgaliotinio informavimą apie pokyčių eigą ir rezultatus šioje Tvarkoje nustatyta tvarka ir terminais;

11.4. TIS funkcinių, greitaveikos, apkrovos, skenavimo ir kitų testavimų įgyvendinimą arba inicijavimą ir įgyvendinimo kontrolę;

11.5. testinės aplinkos sukūrimą pagal šioje Tvarkoje nustatytus reikalavimus;

11.6. pokyčio ištestavimo testinėje aplinkoje įgyvendinimą arba inicijavimą ir įgyvendinimo kontrolę;

11.7. TIS pokyčių įgyvendinimo eigos fiksavimą šioje Tvarkoje numatytomis priemonėms.

12. Organizacijos padalinių vadovai ir darbuotojai yra atsakingi už kibernetinio saugumo vadovo ir (ar) saugos įgaliotinio pavedimų, susijusių su šioje Tvarkoje numatytų techninių reikalavimų, taikomų Žuvininkystės tarnyboje, vykdymu, saugumo spragų valdymu ir atskleidimu, įgyvendinimą, taip pat kitų organizacijos padalinių ar darbuotojų pavedimus, susijusius su TIS pokyčių ir pataisų valdymu.

III SKYRIUS
TINKLŲ IR INFORMACINIŲ SISTEMŲ ĮSIGIJIMAS, PLĖTOJIMAS IR PRIEŽIŪRA

13. Šios tvarkos nuostatos yra taikomos visų organizacijos valdomų TIS įsigijimui, plėtojimui ir priežiūrai bei likvidavimui viso TIS gyvavimo ciklo metu. Jei organizacija valdo valstybės informacinę sistemą, jai papildomai taikomi Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo ir jo įgyvendinimą reglamentuojančių teisės aktų reikalavimai.

14. TIS gyvavimo ciklas – TIS būsenos pokyčių nuo jos sukūrimo iki veikimo pabaigos visuma.

15. TIS gyvavimo ciklo stadijos:

15.1. TIS įsigijimas;

15.2. TIS eksploatavimas;

15.3. TIS plėtojimas;

15.4. TIS likvidavimas.

16. Prieš atliekant TIS įsigijimą, organizacijos atsakingi darbuotojai turi įvertinti veiklos poreikius, teisės aktų reikalavimus, kibernetinio saugumo reikalavimus. Pasirengimo įsigyti TIS turi būti parengti TIS techniniai reikalavimai, kibernetinio saugumo reikalavimai ir įsigijimo sąlygos.

17. Rengiant įsigyjamos TIS techninius reikalavimus, jie specifikuojami techninėje

specifikacijoje ar užduotyje (toliau – Specifikacija). Specifikacijoje turi būti numatyti atliktų reikalavimų analizės rezultatai, numatyti TIS funkcionalumai, duomenų srautai ir integracijų poreikiai, nustatyti funkciniai ir nefunkciniai reikalavimai, įskaitant kibernetinio saugumo reikalavimai. Specifikacijoje turi būti įtraukti privalomi apsaugos nuo kenkimo programinės įrangos (virusų, šnipinėjimo programų), filtravimo, pašto apsaugos, tinklo saugumo ir kiti kibernetinio saugumo reikalavimai.

18. Rengiant Specifikaciją joje turi būti numatyti kibernetinio saugumo reikalavimai (pateikiamas pavyzdinis sąrašas):

18.1. saugiam programavimui, jei TIS yra kuriama;

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

18.3. kompiuterių tinklo filtravimo įrangai (saugasienių, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kita);

18.4. duomenų perdavimo tinklo saugumui;

18.5. kitoms priemonėms, naudojamoms kibernetiniam saugumui užtikrinti;

18.6. kiti kibernetinio saugumo reikalavimai, kurie organizacijos manymu, yra būtini, kad būtų įsigyta saugi TIS, jos programinė ar techninė įranga.

19. Perkant TIS ar jos kūrimo paslaugas, tiekėjams turi būti keliami kvalifikaciniai reikalavimai, numatyti Tiekimo grandinės saugumo valdymo tvarkoje.

20. TIS įsigijimo metu:

20.1. įsigyjamos TIS kūrimo paslaugos, kurios pilnai turi pilnai tenkinti Specifikacijoje numatytus reikalavimus saugiam programavimui;

20.2. įsigyjama TIS programinė ar techninė įranga, kuri turi pilnai tenkinti tokiai įrangai Specifikacijoje numatytus kibernetinio saugumo reikalavimus;

20.3. atliekami TIS programinės ar techninės įrangos diegimo ir konfigūravimo darbai, kuri turi pilnai tenkinti tokioms paslaugoms Specifikacijoje numatytus kibernetinio saugumo reikalavimus;

20.4. atliekami TIS programinės ar techninės įrangos testavimo testinėje aplinkoje veiklos. 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 bandomąją eksploatavimą;

20.5. atliekami TIS programinės ar techninės įrangos diegimo į gamybinę aplinką veiklos. PĮ į gamybinę aplinką gali diegti tik organizacijos įgalioti darbuotojai ir (ar) trečiosios šalys;

20.6. atliekamas TIS programinės ar techninės įrangos bandomoji eksploatacija, kurios metu yra vertinamas TIS programinės ar techninės įrangos funkcionalumas;

20.7. vykdomi TIS naudotojų mokymai;

20.8. rengiama TIS tinkamumo eksploatuoti ir kita dokumentacija.

21. TIS įsigijimas laikomas baigtu, kai organizacijos veiklos padaliniai ir atsakingi darbuotojai patvirtina, kad TIS įsigijimas ir diegimas sėkmingai baigtas ir TIS yra saugi (pilnai atitinka Specifikacijoje numatytus kibernetinio saugumo reikalavimus) ir tinkama naudoti gamybinėje aplinkoje.

22. TIS eksploatavimo metu gamybinėje aplinkoje atliekama nuolatinė TIS veikimo stebėsena, reguliariai atnaujinami filtrai, atliekami saugumo vertinimai ir rizikų analizė. Vykdomas TIS pokyčių valdymas pagal šios Tvarkos nuostatas. Organizacijoje leidžiama naudoti tik organizacijos direktoriaus patvirtintą PĮ, jos sąrašas peržiūrimas ne rečiau kaip kartą per metus.

23. TIS eksploatavimo metu organizacijos atsakingi padaliniai, darbuotojai ir (ar) trečiosios šalys, teikiančios TIS priežiūros paslaugas, turi užtikrinti nuolatinę TIS priežiūrą, savalaikį reagavimą į TIS sutrikimus ar neveikimą bei savalaikį TIS sutrikimų ar neveikimo bei PĮ klaidų šalinimą.

24. TIS eksploatavimo etapo metu periodiškai vykdomi TIS skenavimai.

25. TIS plėtojimo darbai atliekami pagal šioje Tvarkoje apibrėžtą TIS pokyčių valdymo procesą.

26. Likvidavimas inicijuojamas panaikinus veiklos funkciją (-as) ar atsiradus kitoms priežastims, dėl ko TIS tampa nebereikalinga. TIS likvidavimo metu turi būti užtikrintas saugus juose esančių duomenų perkėlimas ar naikinimas.

27. TIS likvidavimo etapo metu:

27.1. informuojami duomenų teikėjai ir duomenų gavėjai;

27.2. organizacijos interneto svetainėje paskelbiama informacija, kuri toliau nebus apdorojama, atnaujinama, teikiama ar skelbiama;

27.3. TIS sukaupti duomenys perduodami kitoms organizacijos TIS arba sunaikinami;

27.4. techninės priemonės perduodamos naudoti kitoms organizacijos TIS arba likviduojamos.

28. Jeigu organizacija pati atlieka visas ar dalį TIS programavimo veiklų, atliekant šioje Tvarkoje nurodytus TIS programinio kodo kūrimo, konfigūravimo ar plėtojimo darbus, turi būti taikomi saugaus programavimo principai, siekiant užtikrinti, kad PĮ būtų parašyta saugiai, taip sumažinant galimų PĮ saugumo spragų skaičių. Saugaus programavimo principai taip pat turi būti taikomi ir trečiųjų šalių programinės įrangos komponentams ir atvirojo kodo programinei įrangai.

29. Atliekant TIS programinio kodo kūrimo, konfigūravimo ar plėtojimo darbus turi būti atsižvelgiama į:

29.1. saugaus programavimo praktikų ir metodų naudojimą;

29.2. programinio kodo dokumentavimą ir programavimo defektų, kurie gali leisti

pasinaudoti saugumo spragoms, pašalinimą;

29.3. draudimą naudoti nesaugius projektavimo metodus (pavyzdžiui, naudoti įkoduotus slaptažodžius);

29.4. prieš patvirtinant programinės įrangos parengimą naudoti, turi būti įvertinti jos saugumo vertinimo rezultatai ir atlikta dažniausiai pasitaikančių programavimo klaidų analizė ir įsitikinta, kad programinė įranga yra tinkama eksploatuoti.

30. Patvirtinus TIS programinio kodo parengimą naudoti turi būti užtikrinta nuolatinė TIS programinio kodo peržiūra ir priežiūra:

30.1. atnaujinimai turi būti saugiai įdiegiami laikantis šios Tvarkos reikalavimų;

30.2. visos saugumo vertinimo metu nustatytos saugumo spragos turi būti sutvarkytos ir pašalintos;

30.3. programinio kodo klaidos turi būti registruojamos, o registracijos žurnalai turi būti reguliariai peržiūrimi, kad prireikus būtų galima pakoreguoti programinį kodą;

30.4. pirminis programinis kodas turi būti apsaugotas nuo neleistinos prieigos ir modifikavimo.

31. TIS gyvavimo ciklo metu užtikrinant TIS įsigijimą, kūrimą, priežiūrą, plėtrą ir likvidavimą turi būti vadovaujamasi Lietuvos Respublikos teisės aktų reikalavimais, tarptautiniais standartais (pvz., standartų ISO/IEC 27001, ISO/IEC 20000 grupėmis) bei gerosiomis pasaulinėmis praktikomis. Už visų etapų įgyvendinimą turi būti paskirti organizacijos atsakingi darbuotojai, į atitinkamus etapus įtrauktas kibernetinio saugumo vadovas ar saugos įgaliotinis.

32. Organizacijos atsakingi darbuotojai su paslaugų tiekėjais sudarydami TIS įsigijimo, plėtojimo ir priežiūros paslaugų teikimo sutartis, turi vadovautis Tiekimo grandinės saugumo valdymo tvarka.

IV SKYRIUS
TINKLŲ IR INFORMACINIŲ SISTEMŲ POKYČIŲ VALDYMAS

33. TIS pokyčių (toliau – pokytis) gyvavimo ciklo etapai:

33.1. Pokyčio planavimas, kuris apima pokyčio identifikavimą, jo inicijavimą, įvertinimą ir patvirtinimą;

33.2. pokyčio įgyvendinimas;

33.3. įgyvendinto pokyčio peržiūra;

33.4. pokyčio uždarymas.

34. Pokyčio planavimas ir įgyvendinimas organizuojamas atsižvelgiant į pokyčių kategorijas:

34.1. **Standartinis pokytis** (angl. *Standard change*) – pokytis, kuriam galima taikyti standartines procedūras, nes jam atlikti būtini veiksmai yra žinomi, jie nekelia rizikos kokybiškam TIS paslaugų teikimui arba TIS infrastruktūros veikimui ir nereikalauja papildomų lėšų.

34.2. **Skubus pokytis** (angl. *Emergency change*) – pokytis, skirtas aukščiausio prioriteto TIS sutrikimams arba problemoms šalinti ir reikalauja ypatingos įvertinimo, patvirtinimo ir atlikimo skubos, taip pat TIS avariniai pokyčiai (pvz., veiklos atkūrimas likviduojant kibernetinio saugumo incidento ar kitų ekstremaliųjų situacijų padarinius).

34.3. **Plėtros pokytis** (angl. *Normal change*) – pokytis, kuriuo yra kuriamos arba modernizuojamos TIS paslaugos ir su tuo susiję pokyčio atlikimo veiksmai nėra visiškai aiškūs, o pokyčio atlikimas yra susijęs su tam tikra rizika TIS paslaugų teikimui arba visos TIS infrastruktūros veikimui.

35. Pokyčiai pagal pokyčio rizikos, skubumo, poveikio ir reikiamų išteklių kriterijus klasifikuojami į aukšto sudėtingumo, vidutinio sudėtingumo ir žemo sudėtingumo.

36. Žemo sudėtingumo pokyčių valdymas nereikalauja tvirtinimo, jie gali būti registruojami ir įgyvendinami.

37. Aukšto ir vidutinio sudėtingumo pokyčiai turi būti planuojami ir įgyvendinami žemiau šioje Tvarkoje nustatyta tvarka.

38. Pokyčiai identifikuojami analizuojant TIS veiklos poreikius, kuriuos formuoja socialiniai, teisiniai, ekonominiai, technologiniai aspektai ir tendencijos, esama TIS būklė (pvz. netinkama konfigūracija, esamos ar žinomos spragos, neatitiktis teisės aktų ir standartų reikalavimams, pasikartojančios TIS veikimo klaidos ir pan.), taip pat TIS naudotojų ir administratorių poreikiai.

39. Pokyčius inicijuoja pokyčio iniciatorius. TIS naudotojai gali TIS savininkui ar saugos įgaliotiniui teikti pasiūlymus dėl reikalingų pokyčių.

40. Pokyčių inicijavimo pagrindai:

40.1. TIS ar jos infrastruktūros tobulinimas;

40.2. TIS plėtra ar modernizavimas;

40.3. elektroninių paslaugų fiziniams ir juridiniams asmenims teikimo tobulinimas ar plėtra;

40.4. TIS tobulinimas ar plėtra atsižvelgiant į TIS naudotojų ir IS administratorių poreikius;

40.5. kibernetinio saugumo rizikos įvertinimo metu nustatytos rizikos;

40.6. atitikties Kibernetinio saugumo įstatymo ir jo įgyvendinimą reglamentuojančių teisės aktų ir Tinklų ir informacinių sistemų kibernetinio saugumo politikos ir jos įgyvendinimą reglamentuojančių vidaus teisės aktų reikalavimams vertinimo metu nustatytos neatitiktys;

40.7. TIS konfigūracijos klaidos;

40.8. kibernetinio saugumo incidentai;

40.9. nustatytos esamos ar žinomos TIS spragos.

41. Pokyčio iniciatorius standartinius pokyčius ir plėtros pokyčius turi suderinti su TIS savininkais ir kibernetinio saugumo vadovu ar saugos įgaliotiniu, bei su jais suderinti pokyčio įgyvendinimo grafiką. Pokyčio iniciatorius skubius pokyčius su organizacijos TIS savininkais turi suderinti tik esant tokiai galimybei. Pokyčio iniciatorius skubius pokyčius visais atvejais turi suderinti su kibernetinio saugumo vadovu.

42. Pokyčiai, galintys sutrikdyti ar sustabdyti organizacijos veiklą, papildomai turi būti suderinti su organizacijos direktoriumi ar jo įgaliotu asmeniu.

43. Pokyčio iniciatoriui pokyčius aukščiau nustatyta tvarka suderinus su organizacijos atsakingais darbuotojais, juos perduoda pokyčių vykdytojui.

44. Pokyčio vykdytojas, prieš pradėdamas įgyvendinti pokytį, turi informuoti TIS naudotojus ir kitus suinteresuotus asmenis apie pokyčius, kurių įgyvendinimo metu galimi TIS darbo sutrikimai. Apie pokyčius turi būti informuojama pokyčius įgyvendinančio subjekto interneto svetainėje, TIS taikomosiose programose ar kitomis priemonėmis (pvz., raštu, elektroniniu paštu ir pan.) ne vėliau kaip prieš 3 (tris) darbo dienas iki planuojamo pokyčio įgyvendinimo pradžios. Šio punkto nuostatų gali būti nesilaikoma, jeigu įgyvendinami skubūs pokyčiai.

45. Pokyčio vykdytojas pokytį įgyvendina pagal su TIS savininkais ir kibernetinio saugumo vadovu ar saugos įgaliotiniu suderintą pokyčio įgyvendinimo grafiką, juos nuolat informuodamas apie pokyčio eigą ir tarpinius bei galutinius rezultatus. Pokyčio vykdytojas pokyčio metu kontroliuoja pokyčio įgyvendinimo eigą: svarsto pokyčių valdymo proceso dalyvių pasiūlymus, koordinuoja pokytyje dalyvaujančių dalyvių veiksmus, teikia pasiūlymus TIS savininkams, kibernetinio saugumo vadovui ar saugos įgaliotiniui, pagal poreikį –organizacijos direktoriui.

46. Įgyvendinto pokyčio peržiūros metu gali būti atliekami TIS funkciniai, greitaveikos, apkrovos, skenavimo ir kiti testavimai.

47. Pokyčiai, galintys sutrikdyti ar sustabdyti TIS darbą, daryti neigiamą įtaką informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti testavimui skirtoje aplinkoje, atliekant TIS saugumo vertinimus. Pokyčiai darbinėje aplinkoje gali būti vykdomi šioje Tvarkoje numatytu būdu tik išimtiniais atvejais, kai dėl techninių, programinių ar kitų priežasčių (pvz., veiklos atkūrimas ir kitos ekstremalios situacijos ir pan.) pokyčių nėra galimybės patikrinti testavimui skirtoje TIS aplinkoje ir tik gavus kibernetinio saugumo vadovo leidimą.

48. TIS testavimo aplinkoje neturi būti konfidencialių ir asmens duomenų. TIS testavimo aplinka turi būti atskirta nuo TIS darbinės aplinkos.

49. TIS savininkui nustačius, kad pokyčių testavimo testavimui skirtoje aplinkoje rezultatas atitinka laukiamus rezultatus, pokyčiai gali būti atliekami darbinėje TIS aplinkoje.

50. Įgyvendinus pokytį, pokyčio vykdytojas turi parengti ir (ar) atnaujinti TIS

dokumentaciją (pvz. tinklo schemas, TIS struktūrą, duomenų mainų schemas ir pan.).

51. Įgyvendinus pokytį, pokyčio uždarymo metu, pokyčio iniciatorius ir pokyčio vykdytojas turi patikrinti (peržiūrėti) TIS konfigūraciją ir TIS būsenos rodiklius, palyginti ir pagal kompetenciją įvertinti, ar pokytis atitinka planuojamus rezultatus. Sudėtingiems ir specifinių pokyčių rezultatams įvertinti gali būti pasitelkti ir kiti organizacijos ar trečiosios šalies (paslaugų teikėjo) kompetentingi specialistai.

52. Pokyčių valdymo proceso dalyviai pokyčių planavimo ir įgyvendinimo eigą fiksuoja pokyčių valdymo registruose.

53. Už TIS saugumo vertinimo inicijavimą, kai yra atliekamas standartinis pokytis ir plėtros pokytis, yra atsakingas pokyčio iniciatorius, skubaus pokyčio atveju – kibernetinio saugumo vadovas ar saugos įgaliotinis.

V SKYRIUS
TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO SPRAGŲ VALDYMAS IR ATSKLEIDIMAS

54. Spragų valdymo objektai yra Turto valdymo tvarkoje nurodytų TIS elementai, esantys:

54.1. fiziniuose (įskaitant telkinius, angl. *cluster*) ir virtualiuose serveriuose (toliau – Serveriai), esančiuose organizacijos patalpose arba trečiųjų šalių (toliau – paslaugų teikėjas) duomenų centre;

54.2. trečiųjų šalių debesijos infrastruktūroje (*angl. Infrastructure as a Service – IaaS*), kai tokias paslaugas užsako organizacija;

54.3. kompiuterizuotų darbo vietų (toliau – KDV) techninėje įrangoje, kurią valdo organizacija;

54.4. aplikacijose (angl. *Applications*), kurias valdo ir (ar) prižiūri organizacija;

54.5. duomenų bazėse, kurias valdo ir (ar) prižiūri organizacija;

54.6. tinklo techninėje įrangoje, kurias valdo ir (ar) prižiūri organizacija;

54.7. įrenginiuose esančių valdiklių ir daviklių (daiktų interneto valdiklių ir daviklių (angl. *Internet of Things*, *IoT*), kuriuos valdo organizacija.

55. Organizacija, atlikusi esminius valdomų ir tvarkomų TIS techninės ar programinės įrangos, programinio kodo, KDV ir gamybos vietų ir kitos įrangos pakeitimus (pvz. TIS architektūros ar infrastruktūros keitimus, naujų TIS modulių diegimą ar ženklų TIS esamų modulių funkcionalumo keitimą, visų kompiuterizuotų darbo ar gamybos vietų operacinės įrangos diegimą ir pan.), perkeliant juos į gamybinę aplinką, savarankiškai ar su trečiųjų šalių pagalba, turi nustatyti, įvertinti ir pašalinti TIS esamas ar žinomas saugumo spragas, t. y. atlikti TIS saugumo vertinimą ir, esant poreikiui, atlikti kibernetinio saugumo rizikos vertinimą vadovaujantis Tinklų ir informacinių sistemų rizikos vertinimo tvarka.

56. Organizacijos TIS saugumo vertinimai turi būti atlikti kartu su TIS funkcionalumų, apkrovos ir (ar) kitais vertinimais ar atlikti iš karto po jų.

57. Draudžiama organizacijoje atlikus TIS esminius pakeitimus, valdomas TIS ir jų dalis (pvz., valdomą ir tvarkomą TIS techninę ir programinę įrangą, programinį kodą, kompiuterizuotas darbo ir gamybos vietas ir kitą įrangą) diegti į gamybinę aplinką, prieš tai neatlikus jų saugumo vertinimo ar kibernetinio saugumo rizikos vertinimo.

58. Draudžiama (organizacijos valdomas TIS (pvz., valdomų ir tvarkomų TIS techninę ir programinę įrangą, programinį kodą, tinklo įrangą, kompiuterizuotas darbo ir gamybos vietas ir kitą įrangą)) diegti į gamybinę aplinką, jei yra nustatytos ar žinomos kritinio ir didelės rizikos lygio saugumo spragos.

59. TIS, KDV ir gamybos vietų skenavimai ar kitų saugumo spragų nustatymo būdų (pvz. įsilaužimų testavimų) įgyvendinimas turi būti periodinis, o visų TIS spragų skenavimas, vadovaujantis Kibernetinio saugumo įstatymo ir jį įgyvendinančių teisės aktų reikalavimais, atlikti ne rečiau kaip kas 6 mėnesius. Kartu su TIS saugumo vertinimu, tai pat turi būti atliktas ir elektroninio pašto saugumo vertinimas.

60. Saugos įgaliotinis turi parengti ir su kibernetinio saugumo vadovu suderinti Spragų nustatymo planą. Spragų nustatymo plano pagrindu saugos įgaliotinis turi organizuoti saugumo vertinimus, esant poreikiui, tam pasitelkti paslaugų tiekėjus, organizuojant tokių paslaugų įsigijimus.

61. Už saugumo vertinimo įgyvendinimą yra atsakingas organizacijos darbuotojas, kuriam kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis paveda atlikti saugumo vertinimą arba trečioji šalis, su kuria organizacija yra sudariusi paslaugų teikimo sutartį ir kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis paveda jai atlikti saugumo vertinimą.

62. Organizacijos valdomose TIS esamos ir žinomos saugumo spragos gali būti nustatomi iš organizacijos valdomų TIS techninės ar programinės įrangos gamintojų, informacijos ir kibernetinio saugumo forumų ar kitų šaltinių (pvz., Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos paviešinus atitinkamą informaciją) gaunant (surenkant) informaciją apie žinomas tokios TIS techninės ar programinės įrangos saugumo spragas.

63. TIS saugumo vertinimai gali būti atliekami naudojant VMS įrankius 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* išleistą ir atnaujinamą saugumo spragų vertinimo (aktualios versijos) metodiką (toliau – OWASP metodika).

64. 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 saugos įgaliotiniu.

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

65.1. įsibrovimo iš interneto, išorės perimetro, žiniatinklio, interneto svetainių, mobiliųjų aplikacijų saugumo vertinimas (toliau – Išorinio tinklo saugumo vertinimas);

65.2. vidinio ir gamybinio (pvz., SCADA) tinklo bei vidiniame tinkle esančios techninės ir programinės įrangos ir IT paslaugų saugumo įvertinimas (toliau – Vidinio tinklo saugumo vertinimas);

65.3. KDV ir gamybos vietų saugumo vertinimas;

65.4. pagal poreikį, programinio kodo saugumo vertinimas.

66. Skenavimo metu, naudojant VMS įrankius, yra automatizuotai skanuojamos TIS, nustatomos saugumo esamos spragos, įvertinami, ar jos nėra netikros ir (ar) neteisingai identifikuotos (angl. *false positive*) ir pagal CVSS klasifikatorių spragos yra priskiriamos atitinkamam rizikos lygiui.

67. Įsilaužimų testavimas vykdomas papildomai su VMS įrankiais ir rankiniu būdu, tikrinant galimybes išnaudoti surastas saugumo spragas bei nustatant jų įtaką TIS.

68. Išorinio tinklo saugumo vertinimas turi apimti bent:

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

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

68.3. perimetro tinklo mazguose veikiančių operacinių sistemų nustatymą ir atitinkamų, šiai dienai žinomų saugumo spragų patikrinimą;

68.4. perimetro tinklo mazguose veikiančių tarnybų nustatymą ir atitinkamų, šiai dienai žinomų saugumo spragų patikrinimą bei konfigūracijos analizę (pavyzdžiui, papildomos informacijos apie audituojamas sistemas surinkimą per klaidų, sisteminius pranešimus, servisų programinę realizaciją);

68.5. nustačius spragas, gali būti atliekamas įsilaužimo testas;

68.6. jei aptinkama iš interneto pasiekiamų tarnybų, reikalaujančių vartotojo autentifikavimo, tuomet atliekamas išorinės paslaugos slaptažodžių auditas. Tikrinama, ar naudojami patikimi slaptažodžiai, ar įmanoma juos atspėti arba parinkti, taip pat ar įmanoma atspėti naudotojus;

68.7. vertinamos antivirusinės sistemos galimybės susidoroti su žalingu kodu;

68.8. vertinamas tinklo mazgų atsparumas paslaugos trikdymo DoS (angl. *Denial of Service*) atakoms.

69. Vidinio tinklo saugumo vertinimas turi apimti bent:

69.1. aktyvios tinklo įrangos konfigūracijos tikrinimą;

69.2. tarnybinių stočių saugumo patikrinimą;

69.3. KDV saugumo patikrinimą;

69.4. duomenų bazių valdymo sistemų patikrinimą;

69.5. svarbių slaptažodžių auditą. Tikrinama ar naudojami patikimi slaptažodžiai, ar įmanoma juos atspėti arba parinkti.

70. TIS programinės įrangos saugumo įvertinimas turi apimti ne mažiau kaip:

70.1. naudojamų technologijų identifikavimą (pavyzdžiui, platforma, programavimo įrankiai ir priemonės);

70.2. paslaugų konfigūracijos patikrinimą (pavyzdžiui, darbinės direktorijos pakeitimas, naudotojų teisių padidinimas, informacijos atskleidimas per klaidų pranešimus ir pan.);

70.3. saugumo spragų paiešką (pavyzdžiui, duomenų tikrinimas (angl. *Input Validation*), struktūruotos užklausų kalbos injekcijos (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;

70.4. komunikacijų tarp skirtingų TIS elementų saugumo įvertinimą;

70.5. trūkumų ieškojimą tomis teisėmis ir sąlygomis, kuriomis dirba organizacijos darbuotojai ir/ar trečiųjų šalių atstovai;

70.6. tikrinant tinklapių prieigą ir tinklo paslaugas (angl. *web service*) rankiniu turi būti įvertinta bent:

70.6.1. įvairios injekcijos (struktūruotos užklausų kalbos SQL, kompiuterinės žymėjimo kalbos XML, protokolo LDAP, dinaminės interpretuojamos programavimo kalbos PHP, komandų ir t.t.);

70.6.2. autorizacijos ir sesijos valdymo saugumas, perėmimo galimybės;

70.6.3. perduodamų/priimamų duomenų perėmimo galimybės ir manipuliavimas jais;

70.6.4. naudotojų teisės.

71. Atliekant KDV saugumo vertinimą turi būti įvertinta ne mažiau kaip 5 (penkios) organizacijos IS administratorių KDV, ne mažiau kaip 5 (penkios) skirtingų tipų TIS naudotojų KDV ir ne mažiau kaip 5 (penkios) skirtingų tipų gamybos darbo vietų.

72. 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*).

73. Informacija apie TIS spragą taip pat gali būti gauta iš išorės (pvz., pagal atsakingo atskleidimo principą) ir naudojama kaip tinkamas šaltinis, jei jos gavimo būdas pilnai atitinka Kibernetinio saugumo įstatymo 25 straipsnyje nustatytus reikalavimus.

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

75. Organizacijoje atsakingas darbuotojas ar paslaugų teikėjas, atlikęs organizacijos TIS saugumo vertinimą turi parengti TIS saugumo vertinimo ataskaitą (toliau – Ataskaita), kurioje turi detaliai aprašyti nustatytas saugumo spragas, pateikiant jų aptikimą patvirtinančius įrodymus, jų išnaudojimo galimybes ir rizikos lygį pagal CVSS klasifikatorių, kuris pateiktas Tvarkos 1 lentelėje „Saugumo spragų vertinimo balai ir šalinimo laikai pagal CVSS klasifikatorių“.

76. Ataskaitoje prie kiekvienos saugumo spragos taip pat privaloma pateikti nustatytų saugumo spragų pašalinimo išsamias rekomendacijas.

77. Saugos įgaliotinis su Ataskaita supažindina saugumo vertinimą inicijavusį darbuotoją ir TIS, kuriuose nustatytos saugumo spragos, savininkus.

78. Saugos įgaliotinis, TIS saugumo vertinimo metu nustatytas saugumo spragas turi šalinti toliau šioje Tvarkoje aprašyta pataisų valdymo tvarka duodamas pavedimus atsakingiems darbuotojams atlikti šioje Tvarkoje numatytų saugumo spragų šalinimo veiklas.

79. Saugos įgaliotinis, atsakingiems darbuotojams duodamas pavedimus pašalinti nustatytas saugumo turi nurodyti jų įgyvendinimo datą, vadovaudamiesi toliau šioje Tvarkoje aprašyta pataisų valdymo įgyvendinimo terminais ir saugumo spragų šalinimo terminais.

80. Saugos įgaliotinis, duodamas pavedimus, atitinkamai įvertina TIS saugumo spragos galimą įtaką kitoms organizacijos valdomoms TIS, esant poreikiui, inicijuoja arba pats atlieka jų informacijos saugumo rizikos vertinimą.

81. Darbuotojai, atsakingi už saugumo spragų šalinimą, organizuoja ir įgyvendina organizacijos TIS saugumo spragų šalinimą vadovaudamiesi toliau šioje Tvarkoje aprašyta pataisų valdymo įgyvendinimo terminais ir saugumo spragų šalinimo terminais.

82. Jei TIS saugumo spragų šalinimo priemonių nėra, tokiu atveju 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.).

83. Darbuotojai, atsakingi už TIS saugumo spragų šalinimą nustatytas TIS saugumo spragas turi pašalinti per laiką, numatytą šios Tvarkos 1 lentelėje.

1 lentelė. TIS saugumo spragų vertinimo balai pagal CVSS klasifikatorių ir jų šalinimo laikai.

Saugumo spragos rizikos lygis	**CVSS balas nuo iki**	**Įtaka**	**Maksimalus saugumo spragos šalinimo laikas nuo jos nustatymo momento**
Kritinis *(angl. critical)*	10.0 – 9.0	Neigiamai paveikiama visos organizacijos ir visų jos klientų veikla.	5 kalendorinės dienos
Aukštas *(angl. high)*	8.9 – 7.0	Neigiamai paveikiama visos organizacijos ir kelių jos klientų veikla.	15 kalendorinių dienų

Vidutinis *(angl. medium)*	6.9 – 4.0	Neigiamai paveikiami visi vidiniai organizacijos procesai ir (ar) visi vidiniai darbuotojai.	30 kalendorinių dienų
Žemas *(angl. low)*	3.9 – 0.1	Neigiamai paveikiami keli vidiniai organizacijos procesai ir (ar) keli vidiniai darbuotojai.	365 kalendorinės dienos

84. Darbuotojai, atsakingi už TIS saugumo spragų šalinimą, negalėdami TIS saugumo spragas pašalinti per šios Tvarkos 1 lentelėje nustatytą terminą, turi apie tai informuoti saugos įgaliotinį bei su juo ir TIS, kuriame yra saugumo spraga, savininku suderinti papildomą tokios spragos šalinimo terminą.

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

86. Darbuotojai, atsakingi už TIS saugumo spragų šalinimą, organizuoja ir įgyvendina tokių TIS saugumo spragų šalinimo veiklas:

86.1. ištaiso techninės ar programinės įrangos klaidas ir atlieka reikiamas konfigūracijas, jei reikia šiam tikslui kreipiasi į paslaugų tiekėjus. Tokiu atveju, koordinuoja paslaugų teikėjų atliekamus techninės ar programinės įrangos klaidų šalinimo ir nustatytų keitimo veiklas, užtikrina jų įgyvendinimo kontrolę;

86.2. apriboja TIS, kuriame yra esama ar žinoma saugumo spraga, pasiekiamumą;

86.3. atnaujina PĮ vadovaudamiesi Pataisų valdymo tvarkoje nustatyta tvarka ir terminais;

86.4. paruošia ir su TIS savininku suderina konfigūracijų keitimo planą bei užtikrina jo įgyvendinimą;

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

86.6. pagal poreikį atlieka kitas saugumo spragų šalinimo veiklas.

87. Tais atvejais, kai dar nėra programinės įrangos atnaujinimo iš gamintojo ar taikomos priemonės visiškai nepašalina saugumo spragos, ar saugumo spragos švelninimo veiksmai turi įtaką kitoms organizacijos valdomoms TIS, atlikus kibernetinio saugumo rizikos vertinimą, tokia TIS gali būti naudojamas su nepašalinta saugumo spraga tik saugos įgaliotinio sprendimu, tokį sprendimą suderinus su TIS, kuriame yra saugumo spraga, savininku.

88. Darbuotojai, atsakingi už TIS saugumo spragų šalinimą, pašalinę saugumo spragą, turi organizacijos IT pagalbos tarnyboje atlikti atitinkamus įrašus, o apie pašalintus kritines ir didelės rizikos saugumo spragas papildomai nedelsiant, informuoti saugos įgaliotinį.

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

89.1. kritinės rizikos saugumo spragos šalinimo eigos procesą – kartą į parą;

89.2. didelės rizikos saugumo spragos šalinimo eigos procesą – kartą kas 2 paras;

89.3. vidutinės rizikos saugumo spragos šalinimo eigos procesą – kartą į 2 savaites.

89.4. žemos rizikos saugumo spragos šalinimo eigos procesą – kartą į 1 mėnesį.

90. Darbuotojai, atsakingi už IT turto valdymą, siekdami, kad organizacijos valdomos TIS būtų tinkamai apsaugoti nuo saugumo spragų, turi tinkamai įgyvendinti IT valdymo procesus (pakeitimų, konfigūracijų ir sąrankos valdymą, pataisymų valdymą, saugų programavimą ir kitus IT valdymo procesus). Pagal kompetenciją saugos įgaliotinis konsultuoja darbuotojus, atsakingus už IT turto valdymą, šių procesų įgyvendinimo metu.

91. Šioje Tvarkoje numatytas TIS saugumo spragų valdymo ir atskleidimo procesas turi būti suderintas su Kibernetinių incidentų valdymo plano nuostatomis.

VI SKYRIUS
TINKLŲ IR INFORMACINIŲ SISTEMŲ PATAISŲ VALDYMAS

92. IS administratorius turi periodiškai turimomis priemonėmis tikrinti informaciją apie TIS PĮ gamintojų paskelbtus TIS PĮ atnaujinimus.

93. IS administratorius nustatęs, kad TIS PĮ gamintojas paskelbė TIS PĮ atnaujinimą, kuris šalina kritinę ar aukštos rizikos saugumo spragą, apie tai turi informuoti saugos įgaliotinį ir už TIS PĮ atnaujinimą atsakingo padalinio vadovą, darbuotoją ir (ar) paslaugų tiekėją.

94. Už TIS PĮ atnaujinimą atsakingo padalinio vadovas ar darbuotojas nuo informacijos gavimo momento turi nedelsiant inicijuoti TIS PĮ atnaujinimą pagal skubų pokyčio valdymo būdą ir užtikrinti, kad ši TIS PĮ būtų atnaujinta šioje Tvarkoje numatytais terminais. Už TIS PĮ atnaujinimą atsakingo padalinio vadovas ar darbuotojas apie atliktą TIS PĮ atnaujinimą, kuriuo buvo pašalinta kritinė ar aukšto rizikos lygio saugumo spraga turi nedelsiant informuoti saugos įgaliotinį.

95. Saugos įgaliotinis turi imtis veiksmų, siekiant įsitikinti, kad su TIS PĮ atnaujinimu yra tinkamai pašalinta kritinė ar aukšto rizikos lygio saugumo spraga. Nustačius, kad kritinė ar aukšto rizikos lygio saugumo spraga su TIS PĮ atnaujinimu nebuvo tinkamai pašalinta jis turi inicijuoti kompensacinių priemonių įgyvendinimą, siekiant, kad kritinė ar aukšto rizikos lygio saugumo spraga nebūtų lengvai išnaudota.

96. IS administratorius nustatęs, kad TIS PĮ gamintojas paskelbė TIS PĮ atnaujinimą, kuris nėra susijęs su kritine ar aukštos rizikos saugumo spraga, apie tai turi informuoti saugos įgaliotinį ir už TIS PĮ atnaujinimą atsakingo padalinio vadovas ar darbuotoją ir (ar) paslaugų tiekėją.

97. Už TIS PĮ atnaujinimą atsakingo padalinio vadovas ar darbuotojas nuo informacijos gavimo momento turi įvertinti galimybes organizuoti tokios TIS PĮ atnaujinimą pagal standartinį ar plėtros pokyčio valdymo būdą bei suorganizuoti susitikimą su TIS savininku, suplanuoti ir suderinti tokios TIS PĮ atnaujinimo planą ir grafiką.

98. Už TIS PĮ atnaujinimą atsakingo padalinio vadovas ar darbuotojas, gavęs TIS savininko sprendimą dėl TIS PĮ atnaujinimo inicijavimo, pagal standartinį ar plėtros pokyčio valdymo būdą ir

patvirtintą TIS PĮ atnaujinimo planą turi atnaujinti TIS PĮ plane nustatytais terminais arba kreiptis į paslaugų tiekėją su prašymu atnaujinti TIS PĮ plane nustatytais terminais.

99. Saugos įgaliotinis papildomai turi įvertinti, ar suplanuoto TIS PĮ atnaujinimo metu turi būti atlikti saugumo vertinimas ir jų vientisumo tikrinimas. Jie taip, jis turi įgyvendinti TIS PĮ atnaujinimo saugumo vertinimą ir jų vientisumo tikrinimą šioje Tvarkoje nustatyta tvarka.

100. Saugos įgaliotinis turi užtikrinti, kad TIS PĮ pataisos, kuriomis yra šalinamos nustatytos saugumo spragos (toliau – Saugos pataisos) turi būti testuojamos testinėje aplinkoje prieš jas diegiant į gamybinę aplinką.

101. Saugos įgaliotinis turi užtikrinti, kad būtų diegiamos tik oficialių TIS PĮ gamintojų saugos pataisos.

102. Draudžiama diegti Saugos pataisas, jei jose aptinkama saugumo spraga, kuri gali daryti didesnę žalą TIS, nei jų diegimo nauda.

VII SKYRIUS
TAIKOMŲ TECHNINIŲ REIKALAVIMŲ, ĮGYVENDINIMAS

103. Saugos įgaliotinis turi užtikrinti, kad organizacijoje taikomi techniniai reikalavimai, numatyti šios Tvarkos 1 priede, būtų tinkamai įgyvendinti viso TIS gyvavimo ciklo metu, atliekant TIS pokyčius ir pataisas bei saugumo spragų valdymo ir atskleidimo metu. Šiam tikslui jie turi teisę duoti organizacijos padaliniams ar darbuotojams bei paslaugų tiekėjams pavedimus, taip pat koordinuoti ir kontroliuoti jų įgyvendinimą.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

104. Visi organizacijos valdomų TIS darbuotojai privalo laikytis šios Tvarkos.

105. Atitinkamų organizacijos padalinių vadovai ar jų paskirti darbuotojai turi užtikrinti ir kontroliuoti, jog darbuotojų, atsakingų už TIS įsigijimo, kūrimo, priežiūros ir plėtros, TIS saugumo vertinimų, TIS saugumo spragų valdymo ir atskleidimo planavimą ir įgyvendinimą, veiksmai atitiktų Tvarkos nuostatas.

106. Ši Tvarka turi būti peržiūrima ir atnaujinama bent kartą per metus arba kai įvyksta esminiai pokyčiai Žuvininkystės tarnyboje, kurie turi įtakos šiai Tvarkai. Už šios Tvarkos peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas.

_____

TINKLŲ IR INFORMACINIŲ SISTEMŲ ĮSIGIJIMO, PLĖTOJIMO IR PRIEŽIŪROS SAUGUMO, ĮSKAITANT SPRAGŲ VALDYMO IR ATSKLEIDIMO, TVARKOS PERŽIŪRA

Dokumento versija	Patvirtinimo data ir Nr.	Dokumento savininkas	Pagrindinės korekcijos
v1.0	2025-06-06 Nr. XXX-I23-130	Kibernetinio saugumo vadovas	Naujai tvirtinama tvarka

Tinklų ir informacinių sistemų įsigijimo,
plėtojimo ir priežiūros saugumo,
įskaitant spragų valdymą ir atskleidimą,
tvarkos
1 priedas

Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams[1]	Esminiams	Svarbiems
1.	Kibernetinio saugumo subjektas turi turėti aktualią tinklų ir informacinių sistemų infrastruktūros loginę schemą ir visų tinklų ir informacinių sistemų schemas (atnaujinti joms pasikeitus).	x	x
2.	Įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu kibernetinio saugumo subjekto sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio kibernetinio saugumo subjekto veiklai vertinimas (testavimas).	x	
3.	Serveriuose (įskaitant ir virtualias mašinas) ir darbo stotyse turi būti įjungtos ir sukonfigūruotos saugasienės, kurios kontroliuoja visą įeinantį ir išeinantį srautą.	x	x
4.	Iš išorės gaunami elektroniniai laiškai turi būti filtruojami, siekiant aptikti ir blokuoti kenksmingą turinį.	x	x
5.	Techninės ir programinės įrangos, kuri skirta kibernetiniams incidentams aptikti, konfigūracijos taisyklės turi būti saugomos elektronine forma atskirai nuo tinklų ir informacinių sistemų techninės įrangos (kartu nurodant atitinkamas datas (įgyvendinimo, atnaujinimo), atsakingus asmenis, taikymo periodus).	x	x
6.	Prisijungiant prie belaidžio tinklo (jeigu jungiamasi prie tinklų ir informacinės sistemos vidinio tinklo), turi būti taikomas tinklų ir informacinių sistemų naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas arba naujesnis protokolas, visuotinai pripažįstamas saugiu.	x	x
7.	Tinklui valdyti turi būti naudojami saugūs tinklo protokolai.	x	x
8.	Turi būti uždrausti / išjungti visi nebūtini protokolai ir atviri prievadai (angl. *port)*.	x	x
9.	Kompiuteriuose, mobiliuosiuose įrenginiuose turi būti išjungtas lygiarangis (angl. *peer to peer*) funkcionalumas, jei tai nėra reikalinga darbo funkcijoms atlikti.	x	

[1] Kibernetinio saugumo subjektams taikomi techniniai reikalavimai pagal Kibernetinio saugumo reikalavimų aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams[1]	Esminiams	Svarbiems
10.	Turi būti diegiami naudojamos programinės įrangos gamintojų ir operacinių sistemų rekomenduojami atnaujinimai.	x	x
11.	Tinklų ir informacinės sistemos, dėl objektyvių priežasčių naudojančios nepalaikomas operacinių sistemų ir kitos programinės įrangos versijas, turi veikti atskirame tinklo segmente, atskirtame nuo pagrindinių kibernetinio saugumo subjekto veiklos funkcijų.	x	x
12.	Vidinis kibernetinio saugumo subjekto kompiuterių tinklas turėtų būti segmentuotas, jame atskiriant bent:		
12.1.	tinklų ir informacinių sistemų valdymo ir administravimo potinklį;	x	x
12.2	atskirą potinklį kiekvienai trečiajai šaliai arba kitais būdais užtikrinant trečiųjų šalių prieigą tik prie tai šaliai reikalingų resursų, kur įmanoma taikant kelių veiksnių prisijungimo autentifikaciją. Prisijungimas turi būti atliekamas naudojant saugų virtualųjį privatų tinklą (angl. *Virtual private network,* VPN). Prisijungimas registruojamas įvykių registravimo žurnaluose;	x	x
12.3.	tinklinių daugiafunkcių įrenginių bei spausdintuvų ir skenerių potinklį;	x	x
12.4.	IP telefonijos potinklį;	x	x
12.5.	darbo vietų potinklį;	x	x
12.6.	testavimo potinklį.	x	x
13.	Mobiliuosiuose įrenginiuose ir kompiuterinėse darbo vietose turi būti naudojamos vykdomojo kodo (angl. *Executable code*) kontrolės priemonės, kuriomis apribojamas neleistino vykdomojo kodo naudojimas ar informuojamas administratorius apie neleistino vykdomojo kodo naudojimą.	x	x
14.	Turi būti parengti ir įdiegti kompiuterinių darbo vietų (įskaitant nešiojamuosius įrenginius) operacinių sistemų atvaizdai ir (arba) kitos priemonės su integruotomis saugumo nuostatomis. Atvaizde turi būti nustatyti tik veiklai būtini operacinių sistemų komponentai (administravimo paskyros, paslaugos (angl. *Services*), taikomosios programos, tinklo prievadai, atnaujinimai, sisteminės priemonės). Atvaizdai turi būti reguliariai peržiūrimi ir atnaujinami, iškart atnaujinami nustačius naujų spragų ar atakų. Pagal parengtus atvaizdus į kompiuterines darbo vietas (įskaitant nešiojamuosius įrenginius) turi būti įdiegiama operacinė sistema su saugumo nuostatomis.	x	x
15.	Draudžiama svetainės serveriuose saugoti sesijos duomenis (identifikatorių) prisijungimo tikslams, pasibaigus susijungimo sesijai.	x	x
16.	Internetu prieinamoms svetainėms, tinklų ir informacinėms sistemoms turi būti naudojama svetainės saugasienė (angl. *Web Application Firewall*).	x	x
17.	Internetu prieinamoms svetainėms, tinklų ir informacinėms sistemoms turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų remiantis OWASP (angl. *The Open*	x	x

Nr.	Techniniai reikalavimai, taikomi kibernetinio saugumo subjektams[1]	Esminiams	Svarbiems
	Worldwise Application Security Project) Top 10 geriausiomis praktikomis (www.owasp.org).		
18.	Žiniatinklio (angl. *Web*) formose turi būti naudojama svetainės naudotojo įvedamų duomenų kontrolė (angl. *Input validation*).	x	x
19.	Internetu prieinamos tinklų ir informacinės sistemos neturi rodyti naudotojui klaidų pranešimų apie tinklų ir informacinės sistemos ir programinį kodą ar serverį.	x	x
20.	Internetu naudojant HTTPS protokolą (angl. *HyperText Transfer Protocol Secure,* HTTPS) prieinamos tinklų ir informacinės sistemos saugumo priemonės turi leisti tik jų funkcionalumui užtikrinti reikalingus protokolo metodus.	x	x
21.	Kibernetinio saugumo subjekto serveriuose ir kompiuterinėse darbo vietose turi būti naudojamos (jei įmanoma, centralizuotai) valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, stebėjimo realiu laiku priemonės.	x	x
22.	Naudojama tik legali ir leistina (pagal kibernetinio saugumo subjekto patvirtintą sąrašą) programinė įranga.	x	x
23.	Nuolatos turi būti stebimas tinklų ir informacinių sistemų įrangos laisvos atminties ar vietos diske kiekis, stebima apkrova, resursų naudojimas. Pasiekus nustatytas ribines reikšmes, apie tai turi būti informuojami atsakingi asmenys.	x	x

PATVIRTINTA
Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
direktoriaus 2026 m. vasario 9 d.
įsakymu Nr. V1-27

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų kibernetinio saugumo politikos dokumentas (toliau – Kibernetinio saugumo politikos dokumentas) yra pagrindinis Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Žuvininkystės tarnyba) kibernetinio saugumo valdymo dokumentas, kuris apibrėžia kibernetinio saugumo tikslus, teisės aktus, atsakingų asmenų funkcijas ir atsakomybes, įsipareigojimus darbuotojams ir trečiosioms šalims.

2. Kibernetinio saugumo politikos dokumento tikslas – užtikrinti kibernetinį saugumą, kuris apima tris pagrindinius aspektus:

2.1. Konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo;

2.2. Vientisumą – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;

2.3. Prieinamumą – užtikrinimą, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti Žuvininkystės tarnybos veiklą.

3. Žuvininkystės tarnybos kibernetinis saugumas grindžiamas kibernetinio saugumo principais, kurie numatyti Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje.

4. Kibernetinio saugumo politikos dokumente vartojamos sąvokos:

4.1. **Atitikties vertinimas** – Žuvininkystės tarnybos atitikties reikalavimams, nustatytiems Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nutarimas Nr. 818), šiame Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose bei standartuose vertinimas;

4.2. **Kibernetinio saugumo vadovas** – Žuvininkystės tarnybos ar trečiosios šalies darbuotojas paskirtas Žuvininkystės tarnybos direktoriaus įsakymu atsakingu už kibernetinio saugumo subjekto atitikties Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

4.3. **Rizikos vertinimas** – rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal Žuvininkystės tarnybos patvirtintą Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarką;

4.4. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.

5. Kitos šiame Kibernetinio saugumo politikos dokumente vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

II SKYRIUS
TEISĖS AKTAI

6. Kibernetinį saugumą reglamentuojančių teisės aktų ir standartų, kuriais vadovaujasi Žuvininkystės tarnyba, sąrašas:

6.1. Kibernetinio saugumo įstatymas;

6.2. Lietuvos Respublikos komercinių paslapčių teisinės apsaugos įstatymas;

6.3. Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

6.4. Lietuvos Respublikos konkurencijos įstatymas;

6.5. Lietuvos Respublikos viešųjų pirkimų įstatymas;

6.6. Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

6.7. Nutarimas Nr. 818;

6.8. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

6.9. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

6.10. Kibernetinio saugumo įgyvendinimą reglamentuojantys vidaus dokumentai.

6.11. kitais teisės aktais, reglamentuojančiais kibernetinį saugumą.

III SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

7. Žuvininkystės tarnybos direktorius privalo užtikrinti žmogiškųjų ir finansinių išteklių skyrimą kibernetinio saugumo valdymui.

8. Žuvininkystės tarnybos direktorius ar jo įgaliotas asmuo įsakymu paskiria:

8.1. Kibernetinio saugumo vadovą. Žuvininkystės tarnyba privalo Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – NKSC) pateikti kibernetinio saugumo vadovo kontaktinę informaciją Kibernetinio saugumo informacinėje sistemoje (toliau – KSIS), ir informuoti Žuvininkystės tarnybos darbuotojus apie paskyrimą.

8.2. Saugos įgaliotinį.

8.3. IS administratorių;

8.4. Fizinės apsaugos įgaliotinį;

8.5. Saugumo operacijų centrą (toliau – SOC). SOC funkcijas gali vykdyti ir trečiosios šalys pagal TIS paslaugų teikimo sutartis.

8.6. Veiklos tęstinumo valdymo grupę.

8.7. Veiklos atkūrimo grupę.

9. Kibernetinio saugumo vadovas, koordinuodamas ir prižiūrėdamas Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų įgyvendinimą, turi atlikti šias funkcijas:

9.1. užtikrinti, kad Kibernetinio saugumo politikos dokumentas ir kibernetinio saugumo įgyvendinimą reglamentuojantys dokumentai būtų parengti ir periodiškai atnaujinami;

9.2. organizuoti Žuvininkystės tarnybos atitikties vertinimą, rengti ir teikti tvirtinti organizacijos vadovui ar jo įgaliotam asmeniui Atitikties vertinimo ataskaitą ir Neatitikčių šalinimo planą bei jų patvirtinimo datas ir registracijos numerius Kibernetinio saugumo įstatymo nustatyta tvarka, ne vėliau kaip per 5 darbo dienas, pateikti į NKSC administruojamą KSIS;

9.3. organizuoti rizikos vertinimą ir dalyvauti rizikos vertinimo procese, rengti ir teikti tvirtinti organizacijos vadovui ar jo įgaliotam asmeniui Rizikos vertinimo ataskaitas ir rizikos valdymo planus bei jų patvirtinimo datas ir registracijos numerius Kibernetinio saugumo įstatymo nustatyta tvarka, ne vėliau kaip per 5 darbo dienas, pateikti į NKSC administruojamą KSIS;

9.4. organizuoti TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymą, rengti ir teikti tvirtinti organizacijos vadovui ar jo įgaliotam asmeniui TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo rezultatų ataskaitas ir jų patvirtinimo datas ir registracijos numerius Kibernetinio saugumo įstatymo nustatyta tvarka, ne vėliau kaip per 5 darbo dienas, pateikti į NKSC administruojamą KSIS;

9.5. organizuoti darbuotojų mokymus kibernetinio saugumo klausimais;

9.6. koordinuoti TIS kibernetinių incidentų tyrimus ir bendradarbiauti su kompetentingomis institucijoms, tiriančiomis kibernetinius incidentus bei neteisėtas veikas, susijusias su kibernetiniais incidentais;

9.7. teikti IS administratoriui, saugos įgaliotiniui ir (ar) naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų įgyvendinimu;

9.8. atlikti kitas Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose bei kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

10. Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis negali vykdyti funkcijų, susijusių su TIS administravimu ar kitomis pareigybėmis, susijusiomis su techninės kompiuterinės įrangos ar programinės įrangos priežiūra ir valdymu.

11. Saugos įgaliotinio funkcijos:

11.1. užtikrinti, kad Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatyti reikalavimai būtų įgyvendinami priskirtuose TIS;

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

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

11.4. koordinuoti darbuotojų mokymus, susijusius su kibernetiniu saugumu, bei užtikrinti darbuotojų informuotumą apie grėsmes ir prevencines priemones;

11.5. teikti nurodymus IS administratoriams ir kitiems atsakingiems asmenims, siekiant laiku identifikuoti ir pašalinti saugumo spragas;

11.6. teikti kibernetinio saugumo vadovui reguliarias ataskaitas apie priskirtų TIS būklę, incidentus ir rizikos valdymo veiksmus;

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

11.8. dalyvauti veiklos tęstinumo valdymo planų rengime, testavime ir įgyvendinime;

11.9. atlikti kitas Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose bei kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

12. IS administratoriaus funkcijos:

12.1. valdyti TIS naudotojų prieigos teises;

12.2. prižiūrėti TIS komponentus (kompiuterių, operacinių sistemų, duomenų bazių, taikomųjų programų, saugasienių, įsibrovimo aptikimo sistemų);

12.3. valdyti TIS komponentų sąranką;

12.4. nustatyti TIS pažeidžiamas vietas;

12.5. nustatyti ir stebėti saugumo reikalavimų atitiktį, reagavimą į kibernetinius incidentus.

13. Fizinės apsaugos įgaliotinio funkcijos nustatytos Fizinės apsaugos tvarkoje.

14. SOC funkcijos nustatytos Kibernetinių incidentų valdymo plane.

15. Veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės funkcijos nustatytos Veiklos tęstinumo valdymo tvarkoje.

IV SKYRIUS
ĮSIPAREIGOJIMAI

16. Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų privalo laikytis visi darbuotojai ir trečiosios šalys.

17. Darbuotojai pasirašytinai supažindinami su Kibernetinio saugumo politikos dokumentu ir kibernetinio saugumo įgyvendinimą reglamentuojančiais dokumentais. Už supažindinimą su Kibernetinio saugumo politikos dokumentu ir kibernetinio saugumo įgyvendinimą reglamentuojančiais dokumentais bei jų pakeitimais yra atsakingas Kibernetinio saugumo vadovas.

18. Organizacija vadovaudamasi Nutarimu Nr. 818, 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 Tiekimo grandinės saugumo valdymo tvarką ir juos numato sutartyse su trečiųjų šalių paslaugų tiekėjais (įskaitant subtiekėjus).

19. Žuvininkystės tarnybos kibernetinio saugumo vadovas sudaro trečiųjų šalių paslaugų tiekėjų sąrašą (įskaitant subtiekėjus), jį tvarko ir pasikeitus sutartims peržiūri ir atnaujina periodiškai, bet ne rečiau kaip kartą per metus, ir kai įvyksta reikšmingi pokyčiai arba reikšmingi incidentai, susiję su trečiųjų šalių paslaugų tiekėjais (įskaitant subtiekėjus).

20. NKSC, atlikdamas Žuvininkystės tarnybos patikrinimą, turi teisę pareikalauti, o organizacija privalo per 5 darbo dienas nuo NKSC prašymo gavimo dienos, pateikti:

20.1. Patvirtintus Kibernetinio saugumo politikos dokumento ir kibernetinio saugumo įgyvendinimą reglamentuojančių dokumentų kopijas;

20.2. Atliktų kibernetinio saugumo auditų, atitikties vertinimo ataskaitos ir nustatytų neatitikčių šalinimo plano, rizikų vertinimo ataskaitos ir rizikos valdymo planų kopijas;

20.3. Veiklos tęstinumo valdymo plano išbandymo ataskaitos kopiją.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

21. Kibernetinio saugumo politikos dokumentas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba kai atsiranda esminiai pokyčiai.

_____

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKOS DOKUMENTO PERŽIŪRA

Dokumento versija	Patvirtinimo data ir Nr.	Dokumento savininkas	Pagrindinės korekcijos
v1.0	2025-06-06 Nr. XXX-I23-130	Kibernetinio saugumo vadovas	Naujai tvirtinama tvarka

PATVIRTINTA
Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos direktoriaus 2026 m. vasario 9 d. įsakymu Nr. V1-27

FIZINĖS APSAUGOS TVARKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Fizinės apsaugos tvarka (toliau – Tvarka) reglamentuoja Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Žuvininkystės tarnyba) už fizinę apsaugą atsakingo darbuotojo funkcijas ir atsakomybes, patalpų kategorijoms keliamus reikalavimus ir darbuotojų įsipareigojimus, taikomus fizinei apsaugai organizacijoje užtikrinti.

2. Tvarkos tikslas – nustatyti fizinės apsaugos reikalavimus Žuvininkystės tarnybos patalpoms.

3. Tvarka siekiama užtikrinti:

3.1. tinkamą prieigų suteikimą įėjimui į patalpas, kuriose laikoma tinklų ir informacinių sistemų (toliau – TIS) įranga, serveriai, naudotojų ir administratorių darbo vietos (toliau – patalpos);

3.2. tinkamą patalpų saugumą.

4. Tvarkoje vartojamos sąvokos:

4.1. **Asmuo atsakingas už fizinę saugą** – Žuvininkystės tarnybos direktoriaus paskirtas darbuotojas, atsakingas už fizinės apsaugos reikalavimų ir fizinio saugumo priemonių įgyvendinimą organizacijoje.

4.2. **„Švaraus stalo“ politika** – Žuvininkystės tarnybos nustatyta tvarka, įpareigojanti darbuotojus darbo vietose nepalikti nesaugomos informacijos (dokumentų, laikmenų, įrenginių ar kitų duomenų laikmenų) pasitraukus iš darbo vietos. Ši politika skirta sumažinti neteisėtos prieigos riziką ir užtikrinti, kad informacija nebūtų palikta atvirai prieinama.

4.3. **Budėtojas** – saugos tarnybos ar Žuvininkystės tarnybos darbuotojas atsakingas už įėjimo į organizacijos teritoriją, pastatą ar patalpas kontrolę, atvykstančių ir išeinančių asmenų (ar/ir transporto) fiksavimą, taip pat pranešimą apie incidentus ar įtartinus įvykius atsakingiems asmenims.

4.4. **Fizinė apsauga** – Žuvininkystės tarnybos naudojamų administracinių, organizacinių, fizinių, technologinių saugumo priemonių visuma, užtikrinanti apsaugą nuo neteisėto patekimo į organizacijos teritoriją ir patalpas, bei saugomos informacijos apsaugą nuo konfidencialumo, vientisumo ar prieinamumo pažeidimo. Fizinė apsauga taikoma atsižvelgiant į saugomos informacijos svarbą organizacijoje, šios informacijos apimtį ir tokių teritorijų, patalpų ar darbo vietų priskyrimą atitinkamai saugos zonai.

4.5. **Fizinio saugumo priemonės** – fizinės (pvz., rakinama spinta, durys, grotos ant langų ir kt.) ir (ar) technologinės (pvz., biometrinė prieigos kontrolė, vaizdo stebėjimo kameros, dokumentų smulkintuvas, apsaugos signalizacija, automatinis durų rakinimas, automatinė gaisro aptikimo sistema ir kt.), skirtos informacijai apsaugoti nuo konfidencialumo, vientisumo ir prieinamumo pažeidimo ir užkirsti kelią neteisėtam asmenų patekimui į saugomas patalpas ar teritorijas, neteisėtam susipažinimui su šiose vietose saugoma informacija ir kitiems neteisėtiems šių asmenų veiksmams.

4.6. **Kibernetinio saugumo vadovas** – Žuvininkystės tarnybos arba trečiosios šalies darbuotojas atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

5. Kitos šioje Tvarkoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

6. Tvarkos reikalavimų privalo laikytis visi organizacijos darbuotojai.

II SKYRIUS
UŽ FIZINĘ APSAUGĄ ATSAKINGO DARBUOTOJO FUNKCIJOS IR ATSAKOMYBĖS

7. Asmens atsakingo už fizinę saugą funkcijos:

7.1. atsako už fizinio saugumo priemonių įgyvendinimą ir priežiūrą;

7.2. vykdo darbo kabinetų (patalpų) raktų (elektroninių ar fizinių) išdavimą ir apskaitą;

7.3. užtikrina, kad ši Tvarka atitiktų galiojančius teisės aktus, standartus ir organizacijos vidaus politiką;

7.4. pagal kompetenciją užtikrina tinkamą fizinio saugumo priemonių funkcionavimą ir techninę priežiūrą;

7.5. organizuoja darbuotojų mokymus apie fizinės saugos reikalavimus, įskaitant saugaus elgesio procedūras;

7.6. pagal savo kompetencijas dalyvauja darbo grupėse (pvz., su fiziniu saugumu susijusiuose procesuose);

7.7. periodiškai (bent kartą per metus) vykdo fizinio saugumo priemonių profilaktinį patikrinimą;

7.8. po įvykdytų patikrinimų (arba pagal poreikį) teikia ataskaitas su rekomendacijomis Žuvininkystės tarnybos direktoriui dėl esamos fizinės apsaugos situacijos ir papildomų fizinio saugumo priemonių įdiegimo ar esamų priemonių tobulinimo;

7.9. įvykus incidentui, susijusiam su fizine apsauga, koordinuoja veiksmus incidentui suvaldyti ir užtikrina greitą jų sprendimą;

7.10. bendradarbiauja su teisėsaugos ar kitomis išorinėmis institucijomis, jei to reikalauja incidentas, susijęs su fizine apsauga;

7.11. užtikrina, kad visi incidentai, susiję su fizine apsauga, būtų tinkamai registruojami, tiriami ir analizuojami, o išvados būtų taikomos fizinio saugumo priemonių tobulinimui;

7.12. saugo visą informaciją, apie incidentus, susijusius su fizine apsauga.

III SKYRIUS
PATALPOMS KELIAMI REIKALAVIMAI

8. Žuvininkystės tarnybos naudojamos patalpos skirstomos į šias kategorijas:

8.1. A – specialios paskirties patalpos: TIS serverių, atsarginių kopijų laikymo patalpos, patalpos, kuriose saugomos atsarginės duomenų kopijos ir kitos patalpos, kurioms reikalingas aukščiausias saugumo lygis.

8.2. B – darbo vietų (darbinės) patalpos: patalpos į kurias gali patekti tik organizacijos darbuotojai, kuriems nustatyta tvarka yra suteikti leidimai patekti į teritoriją;

8.3. C – patalpos: patalpos, į kurias gali patekti tretieji asmenys, nedirbantys organizacijoje.

9. Patalpos, kurios turi būti apsaugotos, registruojamos Reikalingų apsaugoti patalpų sąraše (žr. 1 priedą), kuris yra tvirtinimas Žuvininkystės tarnybos direktoriaus. Atsiradus poreikiui šį sąrašą keisti, jo pakeitimus ir (ar) papildymus tvirtina Žuvininkystės tarnybos direktorius arba jo įgaliotas asmuo. Šis sąrašas yra laikomas konfidencialia informacija ir jis yra saugomas vadovaujantis konfidencialios informacijos valdymo taisyklėmis nurodytomis Turto valdymo tvarkoje.

10. Tais atvejais, kai specialiosios paskirties patalpos sutampa su kitų kategorijų patalpomis, taikomi griežtesni, specialios paskirties patalpų saugumo reikalavimai.

11. Reikalavimai specialios paskirties patalpų fizinei apsaugai (A kategorija):

11.1. patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas, taikant atitinkamas fizinio saugumo priemones;

11.2. prieiga prie šių patalpų suteikiama tik įgaliotiems darbuotojams, kurie yra įtraukti į reikalingų apsaugoti patalpų sąrašą kaip už šias patalpas atsakingi darbuotojai, arba kurių tiesioginės darbo funkcijos yra susijusios su TIS įrangos šiose patalpose priežiūra;

11.3. Į patalpas gali patekti tik asmenys kurių darbo funkcijos yra susijusios su toje patalpoje esančia įrangos kontrole, visi kiti asmenys turi būti lydimi atsakingo darbuotojo;

11.4. Asmenų patekimas į patalpas turi būti kontroliuojamas įeigos kontrolės sistemos pagalba;

11.5. bet koks apsilankymas šiose patalpose turi būti registruojamas Įėjimo į specialios paskirties patalpas kontrolės žurnale;

11.6. numatytos procedūros, kaip elgtis įvykus avarinei situacijai (pvz., gaisrui, patalpų užliejimu vandeniu, ar kitai panašu poveikį galinčiai turėti situacijai), siekiant apsaugoti svarbius įrenginius, turtą ir duomenis. Šios ir kitos potencialios situacijos yra aprašomos Veiklos tęstinumo valdymo plane;

11.7. patalpos turi būti be langų;

11.8. sienos, perdangos turi būti įrengtos iš tvirtų konstrukcijų (gelžbetonio arba tvirto mūro);

11.9. patalpose turi būti įrengta perspėjimo nuo įsilaužimo patalpas signalizacija kurio galinė įranga turi būti suvesta į patalpa kurioje vykdomas budėjimas ar apsaugos tarnybos stebėjimo pulto;

11.10. jei TIS serverių patalpose esančios įrangos bendras galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga, užtikrinanti tinkamą aplinkos temperatūrą ir drėgnumą;

11.11. jei šiose patalpose naudojama TIS kompiuterinė įranga, patalpoje turi būti įtampos filtras ir nepertraukiamo maitinimo šaltinis, užtikrinantis techninės įrangos veikimą;

11.12. patalpose, kuriose laikomi serveriai turi būti oro kondicionavimo ir drėgmės kontrolės įranga.

12. Reikalavimai darbo vietų patalpų fizinei apsaugai (B kategorija):

12.1. prieiga prie darbo vietų patalpų suteikiama tik darbuotojams, kurie pagal einamas pareigas dirba arba vykdo užduotis šiose patalpose arba asmenims dirbantiems paslaugas teikiančiose įmonėse, su kuriomis organizacija yra pasirašiusi paslaugų teikimo sutartį;

12.2. patekimas į patalpas turi būti kontroliuojamas elektronine įeigos kontrolės sistemos pagalba;

12.3. patalpose turi būti įrengta perspėjimo nuo įsilaužimo patalpas signalizacija, valdoma iš patalpos, kurioje vykdomas budėjimas ar iki apsaugos tarnybos stebėjimo pulto.

12.4. lankytojai į patalpą gali patekti tik su jam išduota svečio kortele. Lydintis asmuo yra atsakingas už lydimą asmenį visą jo vizito laikotarpį. Tretieji asmenys, išeidami iš patalpų, turi grąžinti budėtojui svečio kortelę.

13. Reikalavimai viešai prieinamų patalpų fizinei apsaugai (C kategorija):

13.1. į patalpas gali laisvai patekti visi lankytojai organizacijos darbo valandomis;

13.2. Pagal poreiki, patekimo į patalpas prieigos turi būti filmuojamos. Patalpose turi būti vaizdo stebėjimo kameros skirtos užtikrinti viešosios tvarkos laikymąsi ir galimų incidentų fiksavimą;

14. Ne darbo valandomis visos organizacijos pastatų durys turi būti užrakintos.

15. Visose patalpose turi būti įrengta priešgaisrinė signalizacija, sujungta su pastato apsaugos sistema.

16. Darbo vietų patalpos gali būti stebimos vaizdo kameromis.

17. Raktai nuo patalpų turi būti apskaitomi ir išduodami darbuotojams pasirašytinai. naujiems darbuotojams prieiga (pvz., išduodami raktai, individualūs slaptažodžiai ir pan.) prie darbo vietų patalpų suteikiama po Žuvininkystės tarnybos direktoriaus pasirašyto naujo darbuotojo priėmimo į darbą įsakymo. Atleidžiant darbuotojus šios prieigos ne vėliau, kaip paskutinė darbo dieną yra panaikinamos;

18. Patalpose naudojami kritiniai elementai (oro kondicionavimo įranga, vėdinimas ir drėgmės kontrolė, el. energijos tiekimas) turi būti dubliuojami, siekiant užtikrinti aukštą patalpoms eksploatuoti būtinų įrenginių patikimumą.

19. Elektros maitinimo ir ryšių kabeliai, vedami į pastatus, kuriuose yra organizacijos patalpos ar įranga, turi būti įrengti rakinamoje patalpoje ir apsaugoti nuo neleistinos prieigos. Raktus (pagrindinį ir atsarginį komplektus) saugo ir naudoja fizinės saugos įgaliotinis.

IV SKYRIUS
DARBUOTOJŲ ĮSIPAREIGOJIMAI

20. Darbuotojai turi susipažinti su šia Tvarka, kad užtikrintų patalpų fizinės apsaugos reikalavimus.

21. Darbuotojai, pastebėję incidentus, susijusius su fizine apsauga, turi nedelsiant pranešti už fizinę apsaugą atsakingam asmeniui fizinės saugos įgaliotiniui. Ekstremalių įvykių atvejais, pvz., gaisras, darbuotojai turi laikytis sudarytų evakuacijos planų.

22. Reguliariai, ne rečiau kaip kartą per metus arba įvykus esminiams pokyčiams Žuvininkystės tarnyboje, kurie turi didelę įtaką fizinei apsaugai, darbuotojai turi išklausyti instruktažą ir dalyvauti mokymuose šia tema.

23. Darbuotojas, pastebėjęs kad į darbines patalpas nesankcionuotai (be leidimo) pateko neturintys teisės to daryti darbuotojai ar tretieji asmenys, apie tai nedelsdamas žodžiu, telefonu ir (ar) raštu informuoja už fizinę apsaugą atsakingą darbuotoją ar budėtoją.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

24. Ši Tvarka turi būti peržiūrima ir atnaujinama bent kartą per metus arba kai atsiranda esminiai pokyčiai Žuvininkystės tarnyboje, kurie turi įtakos šiai Tvarkai. Už šios Tvarkos peržiūrėjimą ir atnaujinimą yra atsakingas už fizinę apsaugą atsakingas asmuo.

_____

FIZINĖS APSAUGOS TVARKOS PERŽIŪRA

Dokumento versija	Patvirtinimo data ir Nr.	Dokumento savininkas	Pagrindinės korekcijos
v1.0	2025-06-06 Nr. XXX-I23-130	Kibernetinio saugumo vadovas	Naujai tvirtinama tvarka

Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
Fizinės apsaugos tvarkos
1 priedas

REIKALINGŲ APSAUGOTI PATALPŲ SĄRAŠAS

(Reikalingų apsaugoti patalpų sąrašo forma)

Eil. Nr.	Patalpos paskirtis	Patalpos vieta	Patalpos kategorija	Atsakingas darbuotojas	Pastabos

Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
Fizinės apsaugos tvarkos
2 priedas

ĮĖJIMO Į PATALPAS KONTROLĖS ŽURNALAS

(Įėjimo į patalpas kontrolės žurnalo forma)

_____

(nurodyti patalpų kategoriją)

Eil. Nr.	Data	Asmens vardas, pavardė	Įmonė	Apsilankymo tikslas	Patalpos pavadinimas (numeris)	Atvykimo / įėjimo laikas	Svečio kortelės Nr. (jei išduodama)	Lankytojo parašas	Išėjimo laikas	Lydinčio asmens / budėtojo vardas ir pavardė	Parašas

PATVIRTINTA
Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos direktoriaus 2026 m. vasario 9 d. įsakymu Nr. V1-27

TIEKIMO GRANDINĖS SAUGUMO VALDYMO TVARKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tiekimo grandinės saugumo valdymo tvarka (toliau – Tvarka) reglamentuoja Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Žuvininkystės tarnyba) trečiųjų šalių teikiamoms paslaugoms ir (ar) produktams (įrangai), susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra ir modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, kibernetinio saugumo, kokybės ir prieigos kontrolės reikalavimus.

2. Tvarka taikoma, kai Žuvininkystės tarnyba bendradarbiauja (pvz., vykdo bendrus projektus, sudaro sutartis, vykdo paslaugų ir (ar) produktų pirkimą) arba planuoja bendradarbiauti su trečiąja šalimi, kurios paslaugos ir (ar) produktai, tiesiogiai ar netiesiogiai susiję su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, naujinimu ar kibernetinio saugumo užtikrinimu, siekiant mažinti galimas kilti organizacijos tinklų ir informacinių sistemų kibernetinio saugumo rizikas.

3. Tvarkoje vartojamos sąvokos:

3.1. **„Būtina žinoti“** – minimalus informacijos kiekis, kurį būtina žinoti prekėms pateikti, darbui atlikti ar paslaugai suteikti;

3.2. **Kibernetinio saugumo vadovas** – Žuvininkystės tarnybos darbuotojas atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

3.3. **Privalomas paslaugų teikimo lygis** (angl. *Service Level Agreement*) (toliau – SLA) – sutartinis susitarimas tarp trečiosios šalies ir Žuvininkystės tarnybos, kuriame nustatomi konkretūs paslaugų teikimo kokybės, prieinamumo, reagavimo į incidentus, problemų sprendimo ir kiti su paslaugų teikimu susiję rodikliai;

3.4. **Sutartis** – tarp Žuvininkystės tarnybos ir trečiosios šalies pasirašyta tinklų ir informacinių sistemų valdymo ir (ar) kibernetinio saugumo užtikrinimo paslaugų ir (ar) produktų pirkimo sutartis;

3.5. **Tinklų ir informacinė sistema** (toliau – TIS**)** – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal

programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

3.6. **Trečioji šalis** – tai išorinė organizacija, asmuo ar subjektas, kuris teikia Žuvininkystės tarnybai TIS ir kibernetinio saugumo valdymo paslaugas, produktus ar vykdo veiklą, susijusią su organizacijos tinklais, informacinėmis sistemomis ar duomenimis pagal sudarytą sutartį.

4. Kitos šioje Tvarkoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

II SKYRIUS
TREČIŲJŲ ŠALIŲ ATITIKTIES VALDYMAS

5. Kibernetinio saugumo reikalavimai nustatomi vadovaujantis šia Tvarka ir aktualiais teisės aktais, reglamentuojančiais kibernetinį saugumą:

5.1. Kibernetinio saugumo įstatymu;

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

5.3. Kitais teisės aktais, reglamentuojančiais kibernetinį saugumą ar visuotinai pripažintais gerosios praktikos standartais.

6. Trečioji šalis privalo atitikti šioje Tvarkoje ir kituose aktuose nustatytus reikalavimus, kurie perkeliami į sutartis ir viešojo pirkimo dokumentus.

III SKYRIUS
KOKYBĖS REIKALAVIMAI TREČIŲJŲ ŠALIŲ TEIKIAMOMS PASLAUGOMS IR (AR) PRODUKTAMS

7. Žuvininkystės tarnybos darbuotojai, atsakingi už trečiųjų šalių paslaugų ir (ar) produktų įsigijimo inicijavimą, rengdami technines specifikacijas, užduoties aprašymus ar kitus dokumentus, turi nustatyti detalius įsigyjamų TIS valdymo ir (ar) kibernetinio saugumo užtikrinimo paslaugų ir (ar) produktų reikalavimus, kokybės vertinimo kriterijus bei SLA, tačiau neapsiribojant reagavimo į problemas ir problemų spendimo laikais.

8. Su trečiosiomis šalimis sudarant TIS valdymo ir (ar) kibernetinio saugumo užtikrinimo paslaugų ir (ar) produktų sutartis, į jas turi būti perkelti visi įsigyjamų paslaugų ir (ar) produktų kokybės vertinimo kriterijai ir SLA, o organizacijos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, šioje Tvarkoje numatyta tvarka turi užtikrinti įsigyjamų paslaugų ir (ar) produktų kokybės vertinimo atitiktį kriterijams ir SLA stebėjimą bei fiksavimą.

9. Trečiosios šalies fizinė apsauga užtikrinama vadovaujantis fizinės apsaugos reikalavimais pagal Kibernetinio saugumo reikalavimų aprašą, patvirtintą Nutarimu Nr. 818 (toliau –

Kibernetinio saugumo reikalavimo aprašas). Privaloma užtikrinti ne žemesnį fizinės apsaugos lygį nei nurodyta Fizinės apsaugos tvarkoje.

10. Trečioji šalis įsipareigoja saugoti organizacijos konfidencialią informaciją pasirašydama konfidencialumo ir duomenų neatskleidimo įsipareigojimus.

11. Kibernetinio saugumo vadovas priklausomai nuo įsigyjamos paslaugos ir (ar) produktų turi teisę įsitikinti trečiosios šalies darbuotojų kvalifikacija prašydamas pateikti atitinkamus kvalifikaciją patvirtinančius įrodymus leidžiančius dirbti su TIS.

12. Trečioji šalis, ne rečiau kaip kartą per metus, privalo organizuoti darbuotojų kibernetinio saugumo mokymus.

13. Žuvininkystės tarnyba turi nustatyti trečiajai šaliai keliamus kvalifikacijos ir pajėgumų reikalavimus, įskaitant, tačiau neapsiribojant personalui reikalingais įgūdžiais, mokymais, sertifikatais, kvalifikacija, bei prašyti pateikti jų atitiktį pagrindžiančius dokumentus, pvz., įmonės sertifikatus, ekspertų gyvenimo aprašymus ir sertifikatus ir pan.). Šie reikalavimai turi būti aiškiai apibrėžti techninėje specifikacijoje, reikalavimų sąvade ar kituose pirkimo dokumentuose.

14. Žuvininkystės tarnyba turi užtikrinti, kad prieš paslaugų ir (ar) produktų įsigijimą trečiajai šaliai būtų aiškiai apibrėžti taikytini kibernetinio saugumo reikalavimai;

14.1. Sutartyje turi būti nustatytos sąlygos, kad trečioji šalis:

14.1.1. bendradarbiaus su organizacijos atsakingais asmenimis;

14.1.2. teiks informaciją ir įrodymus apie reikalavimų įgyvendinimą;

14.1.3. kartą per metus atliks TIS veiklos tęstinumo valdymo plano išbandymą;

14.1.4. kartą per metus atliks atitikties vertinimą teisės aktams, reglamentuojantiems kibernetinio saugumo valdymą;

14.1.5. kartą per 6 mėnesius atliks TIS spragų testavimą;

14.1.6. leis atlikti patikrinimus ar vertinimus, jei tai būtina.

14.2. trečiosios šalies prieiga prie TIS suteikiama tik sutartyje nurodytai paslaugai įgyvendinti, tiksliai apibrėžtam laikotarpiui.

14.3. trečiosios šalies galimi, pagrįsti nukrypimai nuo reikalavimų turi būti aiškiai įvardinti ir dokumentuoti.

14.4. trečioji šalis užtikrins:

14.4.1. žurnalinių įrašų rinkimą, saugojimą ir prieinamumą;

14.4.2. prieigos valdymo kontrolę ar audito vykdymo galimybes;

14.4.3. įsipareigojimus dėl programinės įrangos atnaujinimų vykdymo.

15. Trečioji šalis turi iš anksto pranešti apie bet kokį esminį paslaugų teikimo pakeitimą, įskaitant TIS pakeitimus (pvz., perkėlimas, techninės ar programinės įrangos pakeitimas ir perkonfigūravimas), kurie turi įtakos paslaugų teikimo sutarčiai, informacijos apdorojimui arba

saugojimui naujoje geografinėje ar teisinėje jurisdikcijoje, sprendimui naudotis naujų subrangovų paslaugomis (įskaitant esamų subrangovų keitimą).

IV SKYRIUS
TREČIŲJŲ ŠALIŲ TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO RIZIKOS VALDYMAS

16. Trečioji šalis, vadovaujantis Kibernetinio saugumo reikalavimo aprašo reikalavimais ne rečiau kaip kartą per metus arba įvykus esminiams organizaciniams ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliam kibernetiniam incidentui, nustatomam pagal Kibernetinių incidentų valdymo planą, turi atlikti TIS kibernetinio saugumo rizikos vertinimą.

17. Žuvininkystės tarnybos prašymu trečioji šalis turi neatlygintinai sudaryti sąlygas kibernetinio saugumo vadovui ar saugos įgaliotiniui atlikti TIS kibernetinio saugumo rizikos vertinimą ar kitus kibernetinio saugumo patikrinimo veiksmus potencialių pažeidžiamumų nustatymui.

18. Trečioji šalis neatlygintinai turi pateikti duomenis, kurie reikalingi įsitikinti, jog trečioji šalis atitinka ir laikosi sutartyje, kibernetinį saugumą ir asmens duomenų apsaugą reglamentuojančiuose teisės aktuose ir visuotinai pripažintuose gerosios praktikos standartuose nustatytų reikalavimų.

V SKYRIUS
PRIEIGŲ VALDYMAS

19. Trečiųjų šalių prieigos yra valdomos vadovaujantis Prieigų valdymo tvarka, papildomai įgyvendinant šioje Tvarkoje toliau numatytus reikalavimus.

20. Trečioji šalis gali gauti prieigas prie TIS tik pasirašę sutartį ir konfidencialumo, duomenų neatskleidimo įsipareigojimus su organizacija, įskaitant abiejų šalių atsakomybes dėl organizacijos informacijos saugumo reikalavimų įgyvendinimo užtikrinimo bei baudų už įsipareigojimų nevykdymą.

21. Prieigos suteikimo faktas turi būti aprašytas sutartyje nurodant kaip identifikuojami asmenys, kurie turės prieigą, prieigos naudotojų teisės, suteikiamos prieigos laikotarpis ir prieigos aktyvumo periodas (pvz., darbo valandas).

22. Suteikus trečiajai šaliai galimybę dirbti kompiuterinėje darbo vietoje priklausančioje trečiajai šaliai, bei suteikiant nuotolinę prieigą prie TIS, privaloma:

22.1. kompiuterinę darbo vietą sukonfigūruoti taip, jog prisijungti prie TIS būtų galima tik naudojant VPN (angl. *Virtual Private Network*) arba alternatyvią, didesnį ar tą patį saugumą užtikrinančią technologiją;

22.2. įsitikinti, kad TIS iš kurios jungiamasi per nuotolį yra saugi;

22.3. užtikrinti nuolatinę prieigos teisių kontrolę;

22.4. vykdyti nuolatinį veiksmų stebėjimą ir kontrolę arba rinkti ir ne trumpiau kaip 6 mėnesius saugoti žurnalinius įrašus apie atliktus veiksmus, užtikrinant jų vientisumą, konfidencialumą ir prieinamumą pagal pareikalavimą;

22.5. užtikrinti organizacijos viešai neskelbtinos informacijos apsaugą organizacinėmis ir techninėmis priemonėmis;

22.6. užtikrinti, kad nuotolinio prisijungimo ryšys būtų kontroliuojamas ir sutaptų su iš anksto tarpusavyje suderintais keliamais tikslais;

22.7. užtikrinti, kad prisijungimas per nuotolinį ryšį ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „būtina žinoti“ bei turėtų sutartą galiojimo terminą, kuris būtų nurodytas sutartyje;

22.8. kiekvienam vartotojui turi būti sukurtas individualus prisijungimo identifikatorius;

22.9. prisijungdama nuotoline prieiga prie TIS trečioji šalis privalo patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksnių tapatumo nustatymo priemonės, angl. *Multi-factor authentication*);

22.10. prisijungimo slaptažodis trečiajai šaliai privalo būti perduotas atskirai nuo naudotojo prisijungimo identifikatoriaus, naudojant saugius ryšio kanalus.

23. Bet kokia nuotolinė prieiga neatitinkanti šiame skyriuje aprašytų reikalavimų prie TIS yra draudžiama.

24. Pasibaigus sutarties terminui ar pilnai suteikus paslaugas prieš sutarties pasibaigimo terminą, trečiųjų šalių prieigos prie TIS turi būti nedelsiant sustabdytos ir (ar) panaikintos.

VI SKYRIUS
SUTARČIŲ SUDARYMO REIKALAVIMAI

25. Organizacijos darbuotojai, įgyvendindami organizacijos sutarčių sudarymo ir trečiųjų šalių valdymo procesus, privalo užtikrinti, kad perkant TIS ar kibernetinio saugumo valdymo paslaugas ir (ar) produktus būtų derinamos sutarties sąlygos su organizacijos kibernetinio saugumo vadovu ar saugos įgaliotiniu, siekiant įtraukti kibernetinio saugumo reikalavimus.

26. Organizacijos sutartyse su trečiosiomis šalimis (tiekėjais, įskaitant subtiekėjus), kiek tai susiję su teikiamomis paslaugomis ir (ar) produktais, turi numatyti:

26.1. trečiosios šalies atitiktį Kibernetinio saugumo reikalavimų aprašo reikalavimams;

26.2. trečiosios šalies personalui reikalingus įgūdžius, mokymus, sertifikatus, kvalifikaciją;

26.3. trečiosios šalies pareigą ne rečiau kaip kartą per metus arba įvykus esminiams trečiosios šalies organizaciniams ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliam

kibernetiniam incidentui atlikti TIS kibernetinio saugumo rizikos vertinimą (toliau – Rizikos vertinimas), parengti ir organizacijos atsakingiems darbuotojams pateikti rizikos vertinimo ataskaitą ir rizikų valdymo planą;

26.4. trečiosios šalies pareigą pranešti organizacijai apie visus didelius ir kitus incidentus, susijusius su organizacijos TIS, kai tik trečioji šalis sužino apie incidentą, ir neatlygintinai pateikti organizacijai kibernetinio incidento tyrimo ataskaitą pagal Kibernetinių incidentų valdymo tvarką;

26.5. teisę organizacijai arba jo įgaliotiems paslaugų teikėjams atlikti trečiosios šalies Kibernetinio saugumo reikalavimų aprašo auditą (įskaitant neplaninį) ir trečiosios šalies pareigą neatlygintinai sudaryti sąlygas tokiam auditui atlikti sutarties vykdymo laikotarpiu ar įvykus dideliam incidentui;

26.6. trečiosios šalies pareigą užtikrinti spragų, keliančių riziką TIS, valdymą;

26.7. trečiosios šalies konfidencialumo ir duomenų neatskleidimo įsipareigojimus pagal Turto valdymo tvarką;

26.8. trečiajai šaliai taikomą SLA;

26.9. apibrėžti trečiosios šalies prieigos (loginės ir fizinės) prie TIS lygius ir sąlygas pagal šios Tvarkos V skyrių;

26.10. numatyti reikalavimus, keliamus trečiosios šalies patalpoms, įrangai, TIS priežiūrai, informacijos perdavimui tinklais;

26.11. numatyti trečiosios šalies ir organizacijos teises ir pareigas.

27. Organizacijos su interneto paslaugos, jei duomenų perdavimo paslauga yra esminė paslaugai teikti, teikėju turi būti sudaręs sutartį (-is), kurioje (-iose) būtų numatyta:

27.1. reagavimas į kibernetinius incidentus įprastomis darbo valandomis;

27.2. reagavimas į kibernetinius incidentus po darbo valandų;

27.3. nepertraukiamas interneto paslaugos teikimas: 24 valandas per parą, 7 dienas per savaitę;

27.4. paslaugos sutrikimų registravimas: 24 valandas per parą, 7 dienas per savaitę;

27.5. apsaugos nuo TIS trikdymo taikymas (angl. *Denial of Service, DoS*).

VII SKYRIUS
TREČIŲJŲ ŠALIŲ SĄRAŠO VALDYMAS

28. Organizacijos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą pagal Trečiųjų šalių sąrašo formą (žr. 1 priedą) rengia ir nuolat atnaujina Trečiųjų šalių sąrašą, kuriame pateikia informaciją apie trečiąją šalį, jos teikiamas paslaugas ir (ar) produktus, atsakingus asmenis, apie sutartį ir joje numatytus pagrindinius SLA bei įvykusius incidentus.

29. Trečiųjų šalių sąrašas turi būti peržiūrimas ir atnaujinamas inicijuojant numatytus IT

ir kibernetinio saugumo reikalavimų pakeitimus naujoms sutartims ir pasikeitus sutartims arba kai įvyksta reikšmingi pokyčiai ar reikšmingi incidentai, susiję su trečiosiomis šalimis.

VIII SKYRIUS
TREČIŲJŲ ŠALIŲ INCIDENTŲ IR TEIKIAMŲ PASLAUGŲ IR (AR) PRODUKTŲ KOKYBĖS VALDYMAS

30. Organizacijos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, pateiktame Trečiųjų šalių incidentų ir SLA neatitikčių valdymo registre (žr. 2 priedą) turi fiksuoti visus pas trečiąsias šalis įvykusius incidentus ir SLA neatitikimus, susijusius su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais. Kibernetinio saugumo vadovas ar saugos įgaliotinis privalo pateikti organizacijos darbuotojui, atsakingam už sutarties įgyvendinimą, reikiamą informaciją apie įvykusius trečiųjų šalių incidentus, kurie turėjo įtakos organizacijos naudojamomis trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais.

31. Organizacijos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, turi vertinti trečiųjų šalių incidentų ir SLA neatitikčių valdymo registre užfiksuotus trečiųjų šalių SLA neatitikimus, susijusius su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais bei nutarti, ar šie neatitikimai organizacijai yra priimtini. Nustačius, kad trečiųjų šalių neatitikimai organizacijai yra nepriimtini, organizacijos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, turi inicijuoti sutartyje numatytų sankcijų taikymą ir (ar) sutarties su trečiąja šalimi nutraukimą.

32. Kibernetinio saugumo vadovas ar saugos įgaliotinis periodiškai (ne rečiau kaip vieną kartą per ketvirtį) turi vertinti trečiųjų šalių incidentų ir SLA neatitikčių valdymo registre fiksuotus incidentus, susijusius su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais bei nutarti, ar rizika dėl pas trečiąsias šalis įvykusių incidentų, susijusių su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais, organizacijai vis dar yra priimtina. Nustačius, kad pas trečiąsias šalis įvykę incidentai organizacijai yra nepriimtini, kibernetinio saugumo vadovas turi inicijuoti sutartyje numatytų sankcijų taikymą ir (ar) sutarties su trečiąja šalimi nutraukimą.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

33. Sutartyse dėl paslaugų ir (ar) produktų pirkimo privaloma numatyti, kad šios Tvarkos reikalavimai yra neatsiejama sutarties dalis. Taip pat organizacija ir trečioji šalis gali susitarti dėl šios Tvarkos reikalavimų taikymo papildomais susitarimais.

34. Tvarkos reikalavimai trečiajai šaliai galioja tol, kol galioja sutartis.

35. Jei kuri nors šios Tvarkos nuostata pripažįstama negaliojančia dėl prieštaravimo imperatyvioms teisės aktų nuostatoms, ji keičiama vadovaujantis sutartyje nustatyta tvarka.

36. Ši Tvarka turi būti peržiūrima ir atnaujinama bent kartą per metus arba kai atsiranda esminiai pokyčiai Žuvininkystės tarnyboje, kurie turi įtakos šiai Tvarkai. Už šios Tvarkos peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas.

_____

TIEKIMO GRANDINĖS SAUGUMO VALDYMO TVARKOS PERŽIŪRA

Dokumento versija	Patvirtinimo data ir Nr.	Dokumento savininkas	Pagrindinės korekcijos
v1.0	2025-06-06 Nr. XXX-I23-130	Kibernetinio saugumo vadovas	Naujai tvirtinama tvarka