ŽUVININKYSTĖS TARNYBOS
PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS
DIREKTORIUS

ĮSAKYMAS
DĖL ŽUVININKYSTĖS TARNYBOS PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS SAUGOS POLITIKOS ĮGYVENDINIMO DOKUMENTŲ PATVIRTINIMO

2025 m. rugsėjo 1 d. Nr. V1-83
Klaipėda

Vadovaudamasis Kibernetinio saugumo įstatymo 14 straipsnyje nustatytais ir Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ nurodytais kibernetinio saugumo reikalavimais:

1. Tvirtinu:

1.1. Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisykles (pridedama);

1.2. Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos informacinių sistemų veiklos tęstinumo valdymo planą (pridedama);

1.3. Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos informacinių sistemų kibernetinių incidentų valdymo planą (pridedama).

2. Nustatau, kad šis įsakymas įsigalioja 2025 m. rugsėjo 1 d.

Direktorius Tomas Kazlauskas

SUDERINTA
Lietuvos Respublikos žemės ūkio
ministerijos 2025-07-09
raštu Nr. 2D -1755 (13.10 E)

PATVIRTINTA
Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
direktoriaus 2025 m. rugsėjo 1 d.
įsakymu Nr. V1-83

ŽUVININKYSTĖS TARNYBOS PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Žuvininkystės tarnyba) informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Tvarkymo taisyklės) reglamentuoja tvarką, užtikrinančią saugų Žuvininkystės tarnybos informacinių sistemų (toliau – Informacinės sistemos) techninės, programinės įrangos funkcionavimą, saugų Informacinės sistemos elektroninės informacijos tvarkymą ir jos teikimą duomenų gavėjams laikantis teisės aktų reikalavimų.

2. Tvarkymo 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“, Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planu, patvirtintu Lietuvos Respublikos krašto apsaugos ministro 2023 m. spalio 16 d. įsakymu Nr. V-840 „Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“.

3. Tvarkymo 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** – Informacinės sistemos tvarkytojos direktoriaus įsakymu paskirtas asmuo, prižiūrintis Informacines sistemas, užtikrinantis jų veikimą ir elektroninės informacijos saugą.

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

3.7. Informacinės sistemos **kibernetinio saugumo vadovas** – Informacinės sistemos tvarkytojos direktoriaus įsakymu paskirtas asmuo, atsakingas už kibernetinio saugumo politikos įgyvendinimą, vidinių procedūrų kontrolę, stebėseną ir tobulinimą.

3.8. Kitos Tvarkymo taisyklėse vartojamos sąvokos atitinka Tvarkymo taisyklių 2 punkte nurodytuose teisės aktuose apibrėžtas sąvokas.

4. Tvarkymo taisyklės privalomos Informacinės sistemos naudotojams, Informacinės sistemos administratoriui, Informacinės sistemos saugos įgaliotiniui ir Informacinės sistemos kibernetinio saugumo vadovui.

5. Už Tvarkymo taisyklių įgyvendinimo organizavimą ir kontrolę atsako Informacinės sistemos saugos įgaliotinis.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

6. Saugiam Informacinės sistemos tvarkymui užtikrinti naudojamos kompiuterinės įrangos, programinės įrangos, duomenų perdavimo tinklai, fizinės, techninės ir organizacinės duomenų bei informacijos saugumo priemonės.

7. Informacinėse sistemose naudojamos saugos priemonės:

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

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

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

7.4. Informacinės sistemos sauga turi būti vertinama periodiškai, ne rečiau kaip kartą per metus, atliekant Informacinės sistemos rizikos vertinimą.

7.5. jungiantis prie administravimo skydų netiesiogiai (per internetą) naudojamas VPN (angl. *Virtual Private Network*), kad būtų apsisaugoma nuo nesankcionuoto prisijungimo iš išorės;

7.6. privilegijuotų vartotojų (IT administratorių, išorinės organizacijos atstovų, teikiančių IT sistemų ar programinės įrangos priežiūros ar diegimo darbus, duomenų analitikų, programuotojų ir kt.) prieiga valdoma naudojant privilegijuotų vartotojų valdymo sistemą (angl. *Privileged Access Management (PAM)*);

8. Kompiuterinės įrangos saugos priemonės:

8.1. prieigos prie Informacinės sistemos tarnybinių stočių (serverių) kontrolė užtikrinama suteikiant prieigos teises tik Informacinės sistemos administratoriui ir Informacinės sistemos saugos įgaliotiniui;

8.2. kompiuterinės įrangos sujungimas klasteriniu režimu (angl. *computer cluster*), t. y. kompiuterinės įrangos dubliavimas ir šios kompiuterinės įrangos techninės būklės nuolatinė stebėsena;

8.3. Informacinės sistemos naudotojų naudojamos techninės kompiuterinės įrangos priežiūrą ir tvarkymą atlieka Informacinės sistemos administratorius;

8.4. kompiuterinės įrangos gedimų registravimas kompiuterinės įrangos gedimų žurnale.

9. Informacinės sistemos sisteminės ir taikomosios programinės įrangos (toliau – programinė įranga) saugos priemonės:

9.1. naudojama legali Informacinės sistemos programinė įranga;

9.2. Informacinės sistemos programinės įrangos diegimą atlieka tik asmenys, turintys teisę atlikti programinės įrangos diegimą;

9.3. Informacinės sistemos programinė įranga prižiūrima laikantis gamintojo rekomendacijų;

9.4. Informacinėse sistemose naudojamos autorizuotos programinės įrangos sąrašą rengia ir reguliariai atnaujina Informacinės sistemos administratorius. Sąrašas turi būti suderintas su Informacinės sistemos tvarkytojos direktoriumi;

9.5. neutralizuotos programinės įrangos įdiegimo į Informacinės sistemos naudotojų kompiuterius ribojimas, nuolatinė naudojamos Informacinės sistemos programinės įrangos stebėsena Informacinės sistemos tvarkytojos prižiūrimose darbo vietose;

9.6. Informacinės sistemos tvarkytojos prižiūrimose kompiuterinėse Informacinės sistemos naudotojų darbo vietose naudojama pažeidžiamumų nustatymo programinė įranga ir centralizuotai valdomos kenkiančios programinės įrangos aptikimo priemonės, kurios automatiniu būdu atnaujinamos ne rečiau kaip kartą per 10 dienų;

9.7. ne rečiau kaip kartą per ketvirtį įvertinami kibernetiniam saugumui užtikrinti naudojamų priemonių programiniai atnaujinimai, klaidų taisymai ir šie atnaujinimai diegiami;

9.8. prisijungimo duomenis, suteikiančius teisę administruoti Informacinės sistemos tarnybines stotis (serverius), žino tik Informacinės sistemos administratorius;

9.9. prieigos teisė dirbti su Informacinės sistemos programine įranga suteikiama Informacinės sistemos naudotojams Informacinės sistemos naudotojų administravimo taisyklėse nustatyta tvarka;

9.10. Informacinės sistemos naudotojų tapatybei, Informacinės sistemos naudotojų veiksmams, atliekamiems Informacinėje sistemoje, nustatyti taikomos programinės priemonės;

9.11. Informacinės sistemos naudotojui 30 minučių neatliekant jokių veiksmų Informacinėje sistemoje, jo sesija pasibaigia. Toliau naudotis Informacine sistema naudotojas gali tik pakartotinai prisijungęs.

10. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

10.1. Informacinės sistemos naudotojai ir Informacinės sistemos paslaugų gavėjai prie Informacinės sistemos jungiasi internetu per užkardą (angl. *firewall*) apsaugotas virtualias tarnybines stotis (serverius), naudodami unikalius atpažinties prisijungimo duomenis;

10.2. Informacinės sistemos turi turėti ne mažiau kaip 2 laiko šaltinius;

10.3. priemonės, naudojamos vidinės Informacinės sistemos sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad žurnaliniuose įrašuose fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais;

10.4. Informacinės sistemos saugasienės saugumo taisyklės, nuolat peržiūrimos ir esant poreikiui atnaujinamos. Detali taisyklių analizė atliekama ne rečiau kaip kartą per 6 mėnesius;

10.5. viešaisiais ryšių tinklais perduodamos elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą;

10.6. nuotolinis prisijungimas prie Informacinės sistemos turi būti vykdomas taikant protokolą, skirtą duomenims šifruoti;

10.7. nuotolinis prisijungimas prie Informacinės sistemos turi būti vykdomas pagal protokolą, skirtą duomenims šifruoti ir (arba) virtualųjį privatųjį tinklą (angl. *Virtual Private Network*);

10.8. Informacinės sistemos duomenų perdavimo tinkle turi būti įdiegtos ir veikti automatinės įsilaužimo (įsibrovimo) aptikimo ir prevencijos priemonės:

10.8.1. turi būti įdiegtos ir veikti automatizuotos įsibrovimo aptikimo sistemos, kurios stebėtų į Informacines sistemas įeinančius ir išeinančius duomenis;

10.8.2. neįprasta veikla turi būti užfiksuojama žurnaliniuose įrašuose ir automatizuotai sukuriamas automatinis pranešimas, kurį matytų Informacinės sistemos kibernetinio saugumo vadovas ir Informacinės sistemos saugos įgaliotinis;

10.8.3. vidinės Informacinės sistemos turi būti atskirtos nuo viešųjų ryšių tinklų naudojant saugasienę;

10.9. papildomos elektroninės informacijos perdavimo belaidžiais tinklais saugumo ir kontrolės užtikrinimo priemonės:

10.9.1. leidžiama naudoti tik su Informacinės sistemos saugos įgaliotiniu suderintus belaidžio tinklo įrenginius ir belaidės prieigos taškus, atitinkančius techninius kibernetinio saugumo reikalavimus;

10.9.2. belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, Informacinės sistemos tvarkytojos kontroliuojamoje zonoje;

10.9.3. vykdoma belaidžių įrenginių kontrolė, tikrinama, ar Informacinės sistemos tvarkytojos eksploatuojami belaidžiai įrenginiai atitinka techninius kibernetinio saugumo reikalavimus;

10.9.4. naudojamos priemonės, kurios automatiškai apribotų neleistinus ar kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius;

10.9.5. naudojamos priemonės, kurios automatiškai apriboja neleidžiamus ar saugumo reikalavimų neatitinkančius belaidžius įrenginius arba apie tokių įrenginių aptikimą informuojamas Informacinės sistemos saugos įgaliotinis;

10.9.6. prisijungiant prie belaidžio tinklo, turi būti taikomas naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) arba TLS (angl. *Transport Layer Security*) protokolas;

10.9.7. draudžiama belaidėje sąsajoje naudoti SNMP (angl. *Simple Network Management Protocol*) protokolą bei visus kitus nebūtinus valdymo protokolus;

10.9.8. turi būti išjungti nenaudojami TCP (angl. *Transmission Control Protocol*) ar UDP (angl. *User Datagram Protocol*) prievadai;

10.10. elektroninis paštas naudojamas Informacinės sistemos tvarkytojos direktoriaus patvirtintuose dokumentuose nustatyta tvarka.

11. Patalpų, kuriose yra Informacinės sistemos tarnybinės stotys (serveriai) (toliau – patalpos) ir aplinkos saugumo užtikrinimo priemonės:

11.1. turi būti užtikrinamas išorės poveikio šaltinių – transporto priemonių keliamos vibracijos, eismo įvykių, radijo stočių, specialiųjų gamyklų, kitų išorės šaltinių minimalus poveikis patalpoms ir jose esančiai techninei ir programinei įrangai;

11.2. patalpos turi atitikti gaisrinės saugos reikalavimus, jose turi būti pirminių gaisro gesinimo priemonių, kurios turi būti reguliariai tikrinamos;

11.3. patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybos stebėjimo pulto;

11.4. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

11.5. patekimas į patalpas yra griežtai reglamentuojamas ir patvirtintas vidaus tvarkos taisyklėmis;

11.6. Informacinės sistemos tarnybinių stočių (serverių) techninė įranga įnešama į patalpas ar išnešama iš patalpų tik leidus Informacinės sistemos administratoriui;

11.7. Informacinės sistemos tarnybinių stočių (serverių) techninė įranga apsaugoma nuo elektros srovės svyravimų. Naudojami specialūs maitinimo šaltiniai, nenutrūkstamo maitinimo šaltinis su automatine apsauga nuo įtampos svyravimų;

11.8. rezervinio nenutrūkstamo maitinimo šaltinis turi užtikrinti Informacinės sistemos tarnybinių stočių (serverių) įrangos veikimą ne trumpiau kaip 30 minučių, jei neveiktų pagrindinis nenutrūkstamo maitinimo šaltinis;

11.9. ryšių kabeliai apsaugoti nuo nesankcionuoto prisijungimo prie jų ir jų pažeidimo;

11.10. įgyvendintos gamintojo nustatytos Informacinės sistemos tarnybinių stočių (serverių) techninės įrangos darbo sąlygos.

12. Informacinės sistemos darbo apskaitos ir kitos elektroninės informacijos saugos priemonės:

12.1. programiniu būdu registruojami Informacinės sistemos naudotojų ir Informacinės sistemos paslaugų gavėjų veiksmai su Informacinės sistemos duomenimis;

12.2. Informacinės sistemos naudotojams suteikiamos prieigos teisės atlikti veiksmus tik su jiems priskirtais duomenimis;

12.3. Informacinės sistemos tarnybinių stočių (serverių) įvykių žurnaluose registruojami, ne trumpiau kaip vienus metus saugomi ir ne rečiau kaip kartą per savaitę analizuojami duomenys nurodant įvykio laiką ir Informacinės sistemos naudotojo unikalius atpažinties prisijungimo duomenis apie:

12.3.1. Informacinės sistemos komponentų (serverių, virtualių serverių, saugasienių, maršrutizatorių, komutatorių ir kitų svarbių komponentų) įjungimas, išjungimas ar perkrovimas;

12.3.2. Informacinės sistemos naudotojų ir Informacinės sistemos administratorių autentifikavimo įvykiai;

12.3.3. Informacinės sistemos naudotojų ir Informacinės sistemos administratorių paskyrų sukūrimas, prieigų prie Informacinės sistemos pakeitimai;

12.3.4. Informacinės sistemos administratorių atliekami veiksmai;

12.3.5. Informacinės sistemos operacinėse sistemose sukurti ir atlikti sisteminiai uždavinių įvykiai (angl. *Scheduled task)*;

12.3.6. Informacinės sistemos grupinių politikų pakeitimai;

12.3.7. Informacinės sistemos saugasienių taisyklių pakeitimai;

12.3.8. Informacinės sistemos žurnalinių įrašų rinkimo funkcijos įjungimas, išjungimas;

12.3.9. Informacinės sistemos operacinių sistemų laiko ir datos pakeitimai;

12.3.10. Informacinės sistemos saugumo sistemų (antivirusinių, įsibrovimo aptikimo sistemų) įjungimas, išjungimas;

12.3.11. Informacinės sistemos operacinėse sistemos vykstančių procesų ar servisų įvykiai;

12.3.12. Informacinės sistemos galinių įrenginių autentifikavimo įvykiai;

12.3.13. Informacinės sistemos žurnalinių įrašų peržiūrėjimas, trynimas, kūrimas ar keitimas.

13. Informacinės sistemos žurnaliniuose įrašuose turi būti fiksuojami šie duomenys:

13.1. Informacinės sistemos įvykio data ir tikslus laikas;

13.2. Informacinės sistemos įvykio rūšis (informacija, klaida, saugumo pranešimas, sisteminis pranešimas, perspėjimas (angl. *warning*);

13.3. Informacinės sistemos naudotojo, Informacinės sistemos administratoriaus ir Informacinės sistemos įrenginio, susijusio su įvykiu, identifikavimo duomenys;

13.4. Informacinės sistemos įvykio aprašymas.

14. Informacinės sistemos fiksuojami žurnaliniai įrašai turi būti saugomi specializuotoje tam pritaikytoje techninėje ar programinėje įrangoje.

15. Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant (automatiniu pranešimu angl. *alert*), bet ne vėliau kaip per vieną darbo dieną turi būti informuojamas Informacinės sistemos kibernetinio saugumo vadovas ir (ar) Informacinės sistemos saugos įgaliotinis.

16. Informacinės sistemos žurnaliniai įrašai turi būti saugomi ne trumpiau kaip 90 kalendorinių dienų.

17. Draudžiama Informacinės sistemos žurnalinius įrašus trinti, keisti, kol nepasibaigęs Informacinės sistemos žurnalinių įrašų saugojimo terminas.

18. Informacinės sistemos žurnalinių įrašų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

19. Saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

19.1. Informacinės sistemos duomenis keisti, atnaujinti, įrašyti ir naikinti gali tik Informacinės sistemos naudotojai, kurių funkcijos aprašytos Informacinių sistemų naudotojų administravimo taisyklėse ir kituose teisės aktuose, reglamentuojančiuose Informacinės sistemos veiklą.

20. Informacinės sistemos naudotojų ir Informacinės sistemos paslaugų gavėjų veiksmų registravimo tvarka:

20.1. Informacinės sistemos naudotojų ir Informacinės sistemos paslaugų gavėjų tapatybė ir veiksmai su Informacinės sistemos duomenimis turi būti įrašomi automatiniu būdu Informacinės sistemos duomenų bazės veiksmų žurnale, apsaugotame nuo neteisėto jame esančių duomenų ir informacijos panaudojimo, pakeitimo, iškraipymo ar sunaikinimo;

20.2. naudojimasis Informacinės sistemos žurnaliniais įrašais turi būti kontroliuojamas ir fiksuojamas. Informacinės sistemos žurnaliniai įrašai turi būti pasiekiami tik Informacinės sistemos tvarkytojos direktoriaus įgaliotiems asmenims ir Informacinės sistemos kibernetinio saugumo vadovui (peržiūros teisėmis);

20.3. Informacinės sistemos žurnalinių įrašų duomenys turi būti analizuojami Informacinės sistemos tvarkytojos direktoriaus įgalioto asmens ne rečiau kaip kartą per mėnesį ir apie analizės rezultatų nuokrypius informuojamas Informacinės sistemos kibernetinio saugumo vadovas ir (ar) Informacinės sistemos saugos įgaliotinis.

21. Prarasti, iškraipyti ar sunaikinti Informacinės sistemos duomenys turi būti atkuriami iš atsarginių Informacinės sistemos duomenų kopijų, kurios turi būti šifruojamos arba naudojamos kitokios priemonės, užtikrinančios kopijų konfidencialumą. Atsarginės Informacinės sistemos duomenų kopijos daromos ir saugomos, o Informacinės sistemos duomenys atkuriami iš atsarginių Informacinės sistemos duomenų kopijų tokia tvarka:

21.1. už atsarginių Informacinės sistemos duomenų kopijų darymą, elektroninės informacijos atkūrimą ir atsarginių Informacinės sistemos duomenų kopijų apsaugą yra atsakingas Informacinės sistemos administratorius, kurio funkcijos aprašytos Informacinių sistemų naudotojų administravimo taisyklėse ir kituose teisės aktuose, reglamentuojančiuose Informacinės sistemos veiklą;

21.2. elektroninė informacija turi būti kopijuojama ir saugoma tokia apimtimi, kad Informacinės sistemos duomenų praradimo atveju visišką Informacinės sistemos funkcionalumą ir veiklą būtų galima atstatyti per 24 valandas darbo dienomis;

21.3. Informacinės sistemos archyvinės duomenų kopijos į rezervinio kopijavimo biblioteką turi būti daromos vieną kartą per 24 valandas;

21.4. Informacinės sistemos duomenų archyvinės kopijos turi būti saugomos patalpose, atspariose išorės aplinkos veiksnių poveikiui.

22. Informacinės sistemos duomenų atkūrimo bandymai turi būti vykdomi kuo mažiau trikdant Informacinės sistemos veiklą ir prieš tai visus Informacinės sistemos naudotojus informavus elektroniniu paštu apie planuojamus vykdyti bandymus.

23. Informacinės sistemos duomenų perkėlimo ir teikimo kitoms informacinėms sistemoms, duomenų gavimo iš jų tvarka:

23.1. už Informacinės sistemos naudotojų ir Informacinės sistemos paslaugų gavėjų administravimą ir iš susijusių registrų ir kitų informacinių sistemų teikiamų duomenų atnaujinimą Informacinės sistemos yra atsakingas įgaliotas Informacinės sistemos naudotojas;

23.2. duomenų mainai tarp Informacinės sistemos ir susijusių registrų ir kitų informacinių sistemų turi būti vykdomi sudarytose duomenų teikimo sutartyse numatytais būdais, terminais ir numatytos apimties arba pagal galiojančius Europos Sąjungos reikalavimus žuvininkystės srities duomenų mainams, kaip tai nustatyta 2009 m. lapkričio 20 d. Tarybos reglamente (EB) Nr. 1224/2009, nustatančiame Sąjungos kontrolės sistemą, kuria užtikrinamas bendrosios žuvininkystės politikos taisyklių laikymasis, iš dalies keičiančiame reglamentus (EB) Nr. 847/96, (EB) Nr. 2371/2002, (EB) Nr. 811/2004, (EB) Nr. 768/2005, (EB) Nr. 2115/2005, (EB) Nr. 2166/2005, (EB) Nr. 388/2006, (EB) Nr. 509/2007, (EB) Nr. 676/2007, (EB) Nr. 1098/2007, (EB) Nr. 1300/2008, (EB) Nr. 1342/2008 ir panaikinančiame reglamentus (EEB) Nr. 2847/93, (EB) Nr. 1627/94 ir (EB) Nr. 1966/2006, 2011 m. balandžio 8 d. Komisijos įgyvendinimo reglamento (ES) Nr. 404/2011, kuriuo nustatomos išsamios Tarybos reglamento (EB) Nr. 1224/2009, nustatančio Bendrijos kontrolės sistemą, kuria užtikrinimas bendrosios žuvininkystės politikos taisyklių laikymasis, įgyvendinimo taisyklėmis ir 2017 m. vasario 6 d. Komisijos įgyvendinimo reglamentu (ES) Nr. 218/2017 dėl Sąjungos žvejybos laivyno registro;

23.3. likviduojant Informacines sistemas, jos elektroninė informacija turi būti saugiai perduodama kitai valstybės informacinei sistemai / registrui, sunaikinama arba perduodama valstybės archyvams Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

24. Informacinės sistemos duomenų neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėti veiksmai) nustatymo tvarka:

24.1. Informacinės sistemos administratorius, užtikrindamas Informacinės sistemos duomenų vientisumą, privalo naudoti visas įmanomas fizines, programines ir organizacines priemones, skirtas Informacines sistemas ir joje tvarkomiems duomenims apsaugoti nuo neteisėtų veiksmų;

24.2. Informacinės sistemos administratorius, įtaręs, kad su Informacinės sistemos duomenimis vykdomi neteisėti veiksmai, privalo apie tai pranešti Informacinės sistemos saugos įgaliotiniui;

24.3. Informacinės sistemos saugos įgaliotinis, gavęs Informacinės sistemos administratoriaus pranešimą apie įvykdytus ar vykdomus neteisėtus veiksmus su Informacine sistema arba su Informacinės sistemos tvarkoma elektronine informacija, inicijuoja elektroninės informacijos

saugos (kibernetinio) incidento valdymo procedūras, nustatytas Informacinių sistemų veiklos tęstinumo valdymo plane.

25. Informacinės sistemos programinės ir techninės įrangos keitimo ir atnaujinimo tvarka ir Informacinės sistemos funkcijų pokyčių (toliau – Informacinės sistemos pokyčiai) valdymo tvarka:

25.1. Informacinės sistemos programinės ir techninės įrangos keitimo ir atnaujinimo tvarką ar Informacinės sistemos pokyčius derina Informacinės sistemos tvarkytoja derina su Informacinės sistemos valdytoja, įsigydama atitinkamas paslaugas iš atitinkamų paslaugų teikėjų;

25.2. prieš atliekant Informacinės sistemos keitimus ir atnaujinimus, turi būti numatomos Informacinės sistemos veiklos atkūrimo procedūros nesėkmingų Informacinės sistemos pokyčių atlikimo atvejais;

25.3. planuodamas Informacinės sistemos pokyčius, kurių metu galimi ilgesni kaip 4 val. Informacinės sistemos veikimo sutrikimai, Informacinės sistemos administratorius privalo ne vėliau kaip prieš 1 darbo dieną iki Informacinės sistemos pokyčių vykdymo pradžios, informuoti Informacinės sistemos naudotojus Informacinės sistemos paslaugų gavėjus apie tokių darbų pradžią ir galimus Informacinės sistemos veikimo sutrikimus.

26. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių (toliau – mobilieji įrenginiai), naudojamų Informacinės sistemos naudotojų tarnybinėms ar darbo funkcijoms vykdyti, naudojimo tvarka:

26.1. išnešti iš Informacinės sistemos tvarkytojos patalpų mobilieji įrenginiai negali būti palikti be priežiūros viešose vietose ir turi būti saugomi disponavimo jais metu;

26.2. duomenys, perduodami tarp mobiliojo įrenginio ir Informacinės sistemos, turi būti šifruojami;

26.3. turi būti užtikrinta kompiuterinių laikmenų apsauga, t. y. esant techninėms galimybėms turi būti šifruojami duomenys tiek mobiliųjų įrenginių laikmenose, tiek išorinėse kompiuterinėse laikmenose. Draudžiama saugoti neužšifruotose mobiliųjų įrenginių laikmenose konfidencialią ir (arba) asmens duomenų informaciją;

26.4. nešiojamojo kompiuterio ir / ar mobiliojo įrenginio grąžinimas turi būti dokumentuojamas;

26.5. už mobiliųjų įrenginių ir jame tvarkomų ar saugomų duomenų saugą teisės aktų nustatyta tvarka atsako naudotojas, kuriam šis įrenginys yra skirtas.

IV SKYRIUS
INFORMACINĖS SISTEMOS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS KELIAMI REIKALAVIMAI

27. Informacinės sistemos tvarkytoja, pirkdama paslaugas, darbus ar įrangą, susijusius su Informacine sistema, jų projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams.

28. Paslaugų teikėjų prieigos prie Informacinės sistemos lygiai ir sąlygos:

28.1. Informacinės sistemos administratorius suteikia prieigos prie Informacinės sistemos duomenų teisę (peržiūrėti Informacinės sistemos duomenis, atlikti užklausas Informacinės sistemos vykdyti veiksmus su Informacinės sistemos duomenimis ir kt.), fizinę prieigą prie Informacinės sistemos techninės ir programinės įrangos paslaugų teikėjo darbuotojui paslaugų teikimo sutartyje ir kituose susijusiuose dokumentuose nustatytomis sąlygomis ir tvarka paslaugų teikėjo funkcijoms atlikti;

28.2. Informacinės sistemos paslaugų teikėjas privalo būti susipažinęs su Informacinės sistemos saugos politiką įgyvendinančiais dokumentais ir vykdyti juose numatytus reikalavimus;

28.3. pasibaigus Informacinės sistemos paslaugų teikimo sutarties galiojimui ar šią sutartį nutraukus, Informacinės sistemos administratorius nedelsdamas, bet ne vėliau kaip kitą darbo dieną, panaikina paslaugų teikėjo darbuotojų ar kitų įgaliotų asmenų prieigos prie Informacinės sistemos duomenų teisę ir apie tai jį informuoja. Prieiga Informacinės sistemos paslaugų teikėjo darbuotojui ar įgaliotam asmeniui suteikiama pakartotinai tais atvejais, kai paslaugų teikimo garantiniu laikotarpiu, numatytu paslaugų pirkimo sutartyje, yra būtina ištaisyti aptiktus Informacinės sistemos neatitikimus ir klaidas.

29. Reikalavimai Informacinės sistemos tarnybinių stočių (serverių) patalpų, Informacinės sistemos programinės įrangos, Informacinės sistemos priežiūrai ir kitoms paslaugoms:

29.1. reikalavimai Informacinės sistemos paslaugų teikėjams ir jų teikiamoms Informacinės sistemos priežiūros paslaugoms nustatomi šių paslaugų teikimo sutartyse;

29.2. paslaugų teikimo sutartyje turi būti nurodoma, kad Informacinės sistemos paslaugų teikėjas kuria ar modifikuoja Informacinės sistemos programinę įrangą, naudodamas:

29.2.1. įgyvendintas Informacinės sistemos elektroninės informacijos saugos priemones, apsaugančias nuo neteisėto poveikio sisteminei, programinei įrangai ir patalpoms;

29.2.2. Informacinės sistemos tęstinės duomenų bazės duomenis (Informacinės sistemos programinei įrangai modifikuoti);

29.2.3. tik legalią programinę įrangą;

29.3. Informacinės sistemos veiklą palaikančių sistemų (elektros energijos, šildymo, vėdinimo ir oro kondicionavimo bei kitų sistemų) kokybė, atsižvelgiant į šių sistemų veiklai keliamus reikalavimus, turi būti reguliariai tikrinama, siekiant tinkamo paslaugų teikimo ir galimo šių paslaugų teikimo sutrikimo bei avarijos pasekmių sumažinimo.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

30. Informacinės sistemos sauga turi būti vertinama kasmet Informacinės sistemos rizikos vertinimo ir (arba) informacinių technologijų saugos atitikties vertinimo metu, kurį atlieka Informacinės sistemos saugos įgaliotinis.

31. Informacinės sistemos naudotojai, Informacinės sistemos paslaugų gavėjai, Informacinės sistemos saugos įgaliotinis ir Informacinės sistemos administratorius, pažeidę šių Tvarkymo taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____

PATVIRTINTA
Žuvininkystės tarnybos prie Lietuvos Respublikos
žemės ūkio ministerijos direktoriaus
2025 m. rugsėjo 1 d. įsakymu Nr. V1-83

ŽUVININKYSTĖS TARNYBOS PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Žuvininkystės tarnyba) informacinių sistemų (toliau – Informacinės sistemos) veiklos tęstinumo valdymo planas (toliau – Valdymo planas) nustato Informacinės sistemos saugos įgaliotinio, Informacinės sistemos administratoriaus, Informacinės sistemos naudotojų ir kitų asmenų veiksmus įvykus kibernetiniam incidentui, dėl kurio kyla pavojus Informacinės sistemos elektroninei informacijai, Informacinės sistemos techninės ir (ar) programinės įrangos funkcionavimui.

2. Valdymo planas parengtas 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. Valdymo plane 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. **Kibernetinis incidentas** – įvykis ar veika kibernetinėje erdvėje, galintis sukelti arba sukeliantis grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintis trikdyti arba trikdantis ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

3.4. Informacinės sistemos **administratorius** – Informacinės sistemos tvarkytojos direktoriaus įsakymu paskirtas asmuo, prižiūrintis Informacines sistemas, užtikrinantis jų veikimą ir elektroninės informacijos saugą.

3.5. 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.

3.6. 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.

3.7. Informacinių sistemų **paslaugų gavėjai** – fiziniai asmenys ir juridinių asmenų atstovai, naudojantys Informacinės sistemos duomenis.

3.8. Informacinės sistemos **kibernetinio saugumo vadovas** – Informacinės sistemos tvarkytojos direktoriaus įsakymu paskirtas asmuo, atsakingas už kibernetinio saugumo politikos įgyvendinimą, vidinių procedūrų kontrolę, stebėseną ir tobulinimą.

3.9. Kitos Valdymo plane vartojamos sąvokos atitinka Valdymo plano 2 punkte nurodytuose teisės aktuose apibrėžtas sąvokas.

4. Valdymo plano vykdymas yra privalomas kibernetinių incidentų atveju, kurių metu gali kilti pavojus Informacinės sistemos duomenims, Informacinės sistemos techninės, programinės įrangos funkcionavimui.

5. Valdymo planu privalo vadovautis Informacinės sistemos kibernetinio saugumo vadovas, Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius ir Informacinės sistemos naudotojai.

6. Informacinės sistemos naudotojai, pastebėję Informacinės sistemos veiklos sutrikimus ar neveikiančias arba netinkamai veikiančias Informacinės sistemos saugos užtikrinimo priemones, privalo nedelsdami apie tai informuoti Informacinės sistemos administratorių žodžiu arba raštu (el. paštu). Informacinės sistemos administratorius, gavęs informaciją apie Informacinės sistemos veiklos sutrikimus ar neveikiančias arba netinkamai veikiančias Informacinės sistemos saugos užtikrinimo priemones, nedelsdamas informuoja Informacinės sistemos saugos įgaliotinį.

7. Informacinės sistemos kibernetinio saugumo vadovo, Informacinės sistemos saugos įgaliotinio ir Informacinės sistemos administratoriaus atliekami veiksmai įvykus Informacinės sistemos kibernetiniam incidentui yra nurodyti Valdymo plano 1 priede.

8. Informacinės sistemos kibernetinio incidento metu patirti nuostoliai padengiami iš valstybės biudžeto ir kitų finansavimo šaltinių.

9. Per metus Informacinės sistemos prieinamumas užtikrinamas ne mažiau kaip 99 proc. darbo laiko darbo dienomis.

10. Valdymo planas grindžiamas nuostata, kad neveikiant Informacinei sistemai ar veikiant iš dalies, jų veikla turi būti atkurta per 24 val. arba kiek įmanoma greičiau.

11. Kriterijai, pagal kuriuos nustatoma, kad Informacinės sistemos veikla atkurta:

11.1. Informacinės sistemos prieinamumas (prisijungimas prie Informacinės sistemos ir naudojimasis ja vyksta be trikdžių);

11.2. Informacinės sistemos pagrindinių funkcijų veikimas (visos kritinės funkcijos veikia tinkamai);

11.3. Informacinės sistemos duomenų atkūrimas (visi reikalingi duomenys yra atkurti, jų vientisumas patikrintas);

11.4. Informacinės sistemos saugumo užtikrinimas (pašalintos saugumo spragos, patikrintas apsaugos priemonių veikimas);

11.5. Informacinės sistemos naudotojų autentifikacija (naudotojai gali saugiai prisijungti ir naudotis sistema);

11.6. Informacinės sistemos integracijų veikimas (užtikrintas sklandus ryšys su kitomis sistemomis ir paslaugomis);

11.7. Informacinės sistemos incidento analizė ir prevencija (nustatyta incidento priežastis, įgyvendintos korekcinės priemonės, atliktas veiklos testavimas).

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

12. Informacinės sistemos saugos įgaliotinis sudaro kibernetiniams incidentams valdyti ir veiklos atkūrimui organizuoti veiklos tęstinumo valdymo grupę (toliau – Veiklos tęstinumo valdymo grupė) ir veiklos atkūrimo grupę (toliau – Veiklos atkūrimo grupė) ir teikia tvirtinti Informacinės sistemos tvarkytojos direktoriui. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąrašas turi būti atnaujinamas, pasikeitus jame nurodytai informacijai.

13. Veiklos tęstinumo valdymo grupės tikslai – gavus tarnybinį pranešimą apie kibernetinį incidentą, jį ištirti, ieškoti priemonių ir būdų šio incidento sukeltiems padariniams bei žalai likviduoti, užtikrinti Informacinės sistemos veiklos tęstinumą.

14. Veiklos tęstinumo valdymo grupę sudaro:

14.1. Informacinių sistemų tvarkytojos direktorius (darbo grupės pirmininkas);

14.2. Bendrųjų reikalų skyriaus vedėjas (darbo grupės pirmininko pavaduotojas);

14.3. Informacinės sistemos kibernetinio saugumo vadovas;

14.4. Informacinės sistemos saugos įgaliotinis;

14.5. Informacinės sistemos administratorius;

14.6. kiti Informacinės sistemos direktoriaus įsakymu paskirti darbuotojai.

15. Veiklos tęstinumo valdymo grupės funkcijos užtikrinant Informacinės sistemos veiklos tęstinumą:

15.1. Informacinės sistemos kibernetinių incidentų analizė ir sprendimų Informacinės sistemos veiklos tęstinumo valdymo klausimais priėmimas;

15.2. bendravimas su susijusių registrų ir informacinių sistemų veiklos tęstinumo valdymo grupėmis;

15.3. bendravimas su teisėsaugos institucijų, kitų institucijų darbuotojais ir kitomis interesų grupėmis;

15.4. bendravimas ir bendradarbiavimas su Informacinės sistemos paslaugų teikėjais ir gavėjais;

15.5. finansinių ir kitų išteklių, būtinų Informacinės sistemos veiklai atkurti, įvykus Informacinės sistemos kibernetiniam incidentui, naudojimo kontrolė;

15.6. elektroninės informacijos fizinė sauga įvykus Informacinės sistemos kibernetiniam incidentui;

15.7. logistikos organizavimas (žmonių, daiktų, įrangos gabenimas ir jo organizavimas);

15.8. Informacinės sistemos veiklos atkūrimo priežiūra ir koordinavimas;

15.9. kitos Veiklos tęstinumo valdymo grupei pavestos funkcijos.

16. Veiklos atkūrimo grupę sudaro:

16.1. Informacinės sistemos kibernetinio saugumo vadovas (darbo grupės pirmininkas)

16.2. Informacinės sistemos administratorius (darbo grupės pirmininko pavaduotojas);

16.3. Bendrųjų reikalų skyriaus vedėjas;

16.4. kiti Informacinės sistemos tvarkytojos direktoriaus įsakymu paskirti darbuotojai.

17. Veiklos atkūrimo grupės funkcijos užtikrinant Informacinės sistemos veiklos atkūrimą:

17.1. Informacinės sistemos tarnybinių stočių veikimo atkūrimo organizavimas;

17.2. Informacinės sistemos tinkamo veikimo atkūrimo organizavimas;

17.3. Informacinės sistemos elektroninės informacijos atkūrimo organizavimas;

17.4. kompiuterių tinklo veikimo atkūrimo organizavimas;

17.5. darbo kompiuterių veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

17.6. žalos Informacinės sistemos duomenims, Informacinės sistemos techninei ir (ar) programinei įrangai vertinimo organizavimas ir laisvos formos žalos vertinimo ataskaitos rengimas;

17.7. kitos Veiklos atkūrimo grupei pavestos funkcijos.

18. Įvykus Informacinės sistemos kibernetiniam incidentui:

18.1. Informacinės sistemos naudotojai ir Informacinės sistemos paslaugų gavėjai privalo nedelsdami žodžiu ar raštu (el. paštu) pranešti Informacinės sistemos administratoriui apie Informacinės sistemos kibernetinį incidentą. Informacinės sistemos naudotojai ir Informacinės sistemos paslaugų gavėjai neturi teisės imtis jokių veiksmų susijusių su incidentu;

18.2. Informacinės sistemos administratorius nedelsdamas informuoja apie kibernetinį incidentą Informacinės sistemos saugos įgaliotinį;

18.3. Informacinės sistemos saugos įgaliotinis, gavęs pranešimą apie Informacinės sistemos kibernetinį incidentą, nedelsdamas turi imtis reikiamų veiksmų Informacinės sistemos kibernetiniam incidentui stabdyti. Įvykis aprašomas, nurodant Informacinės sistemos kibernetinio incidento vietą, laiką, pobūdį ir kitą svarbią su įvykiu susijusią informaciją;

18.4. Informacinės sistemos saugos administratorius pagal kompetenciją atkuria Informacinės sistemos tarnybinių stočių bei programinės įrangos veikimą ir apie atliktus veiksmus nedelsdamas informuoja Informacinės sistemos kibernetinio saugumo vadovą ir Informacinės sistemos saugos įgaliotinį;

18.5. Informacinės sistemos saugos įgaliotinis, įvertinęs Informacinės sistemos kibernetinio incidento reikšmingumą, turi teisę inicijuoti Veiklos atkūrimo grupės posėdį būtiniems Informacinės sistemos veiklos atkūrimo veiksmams aptarti, suderinti arba organizuoti. Apie Veiklos atkūrimo grupės posėdį Informacinės sistemos saugos įgaliotinis raštu (el. paštu) informuoja Veiklos atkūrimo grupę;

18.6. Informacinės sistemos kibernetinio saugumo vadovas nustato Informacinės sistemos kibernetinio incidentų valdymo, tyrimo šalinimo prioritetus ir apie juos informuoja nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos (toliau – NKSC) vadovaujantis Nacionaliniu kibernetinių incidentų valdymo plano nustatyta tvarka;

19. Techninė, sisteminė ir taikomoji programinė įranga, kuria turi būti pakeista kibernetinio incidento metu sunaikinta ar sugadinta įranga, įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo ir (ar) viešuosius pirkimus reglamentuojančių poįstatyminių ir kitų teisės aktų nustatyta tvarka.

20. Veiklos tęstinumo valdymo grupė ir Veiklos atkūrimo grupė tarpusavyje bendrauja telefonu, el. paštu ir (ar) tiesiogiai susitikdamos. Šių grupių posėdžiai organizuojami kartą per metus arba įvykus Informacinės sistemos kibernetiniam incidentui, taip pat – jei prireikia dėl kitų priežasčių.

21. Atsarginėms patalpoms, naudojamoms Informacinės sistemos veiklai atkurti Informacinės sistemos kibernetinio incidento atveju, keliami šie reikalavimai:

21.1. atsarginės patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

21.2. atsarginės patalpos turi atitikti gaisrinės saugos reikalavimus ir jose turi būti pirminių gaisro gesinimo priemonių;

21.3. atsarginėse patalpose turi būti įrengtas rezervinis Informacinės sistemos techninės įrangos elektros energijos šaltinis, užtikrinantis šios įrangos veikimą pagrindinio elektros energijos šaltinio neveikimo atveju ne trumpiau kaip 10 minučių;

21.4. ryšių kabeliai turi būti apsaugoti nuo nesankcionuoto prisijungimo;

21.5. patalpoje turi veikti oro temperatūros reguliavimo įranga (oro kondicionavimo sistema) ir turi būti palaikoma +22 (± 5) ºC temperatūra.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

22. Informacija apie techninę ir programinę įrangą ir jos parametrus nurodyta Informacinės sistemos techninės ir programinės įrangos specifikacijoje. Svarbiausia informacinių sistemų įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos yra dubliuoti ir jų techninė būklė nuolat stebima.

23. Už Informacinės sistemos techninės ir programinės įrangos priežiūrą yra atsakingas Informacinės sistemos administratorius.

24. Už Informacinės sistemos atsarginių kopijų darymą, saugojimą, duomenų iš atsarginių kopijų atkūrimą atsakingas Informacinės sistemos administratorius.

25. Atsarginių kopijų kūrimo, saugojimo ir duomenų atkūrimo tvarka nustatoma atsižvelgiant į Valdymo plane nustatytus (angl. *Recovery time objective,* RTO) ir (angl. *Recovery point objective*, RPO) parametrus.

25.1. Atsarginės kopijos daromos ne rečiau kaip kartą per 24 valandas darbo dienomis, jų saugojimo trukmė – ne trumpesnė kaip 14 kalendorinių dienų. Ne rečiau kaip kartą per ketvirtį atliekamas atsitiktinis atsarginės kopijos atkūrimo testas, įvertinant, ar atkūrimas vykdomas sėkmingai ir ar duomenys atitinka (RPO) reikalavimus.

25.2. Atsarginės duomenų kopijos saugomos geografiškai nutolusioje vietoje.

26. Informacinės sistemos administratorius parengia ir saugo Informacinės sistemos tvarkytojos direktoriaus patvirtintą dokumentą, kuriame:

26.1. nurodyti informacinių technologijų įrangos parametrai ir už šios įrangos priežiūrą atsakingas Informacinės sistemos administratorius, minimalus Informacinės sistemos veiklai atkurti nesant Informacinės sistemos administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą, reikiamos kompetencijos ar žinių lygis;

26.2. nurodyta minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos Informacinės sistemos tvarkytojos poreikius atitinkančiai Informacinės sistemos veiklai užtikrinti, įvykus kibernetiniam incidentui, specifikacija, kuri turi būti lygiavertė pagrindinei Informacinės sistemos techninės ir programinės įrangos specifikacijai;

26.3. nurodytos kompiuterių tinklo fizinio ir loginio sujungimo schemos;

26.4. nurodytos duomenų teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutartys, atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų pareigos;

26.5. nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis Informacinės sistemos duomenų kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos.

27. Informacinės sistemos saugos įgaliotinis ne rečiau kaip kartą per ketvirtį:

27.1. atlieka užfiksuotų kibernetinių incidentų analizę ir esant reikalui organizuoja pastebėtų neatitikčių saugumo reikalavimams šalinimą;

27.2. atlieka kibernetinių incidentų valdymo patirties vertinimą;

27.3. atlieka užkardų (angl. *firewall*) užfiksuotų įvykių analizę, organizuoja pastebėtų neatitikčių saugumo reikalavimams šalinimą;

27.4. įvertina kibernetiniam saugumui užtikrinti naudojamų priemonių programinius atnaujinimus, klaidų taisymus ir organizuoja atnaujinimų diegimą.

IV SKYRIUS
VALDYMO PLANO VEIKSMINGUMO IŠBANDYMAS

28. Valdymo plano veiksmingumas turi būti išbandomas kartą per dvejus metus.

29. Valdymo plano veiksmingumo išbandymo metu imituojamas Informacinės sistemos kibernetinis incidentas. Jo metu už Informacinės sistemos kibernetinio incidento padarinių likvidavimą atsakingi asmenys atlieka minėtų padarinių likvidavimo veiksmus. Iš atsarginių Informacinės sistemos duomenų kopijų atkuriami Informacinės sistemos duomenys ir Informacinės sistemos elektroninė informacija.

30. Jeigu Valdymo plano veiksmingumo išbandymo metu nustatoma incidentų valdymo ir šalinimo, taip pat Informacinės sistemos tvarkytojos nepertraukiamos veiklos užtikrinimo trūkumų, tikslinamas Valdymo planas.

31. Duomenų praradimo toleruojamas laikotarpis (RPO) ne ilgesnis nei 24 val. Valdymo plano veiksmingumo išbandymo metu atkuriami duomenys iš atsarginių kopijų ir įvertinamas galimas duomenų praradimo laikotarpis, siekiant įsitikinti, ar jis atitinka nustatytą (RPO).

32. Atsarginių duomenų kopijų atkūrimo parametrai nustatomi vadovaujantis Valdymo plano 10 punkte nurodytu atkūrimo laikotarpiu (RTO), kuris yra ne ilgesnis nei 24 valandos darbo dienomis Veiksmingumo išbandymo metu imituojamas atsarginių kopijų atkūrimas, vertinama, ar atkūrimo trukmė atitinka (RTO).

33. Pagal bandymų rezultatus Informacinės sistemos saugos įgaliotinis, Informacinės sistemos administratorius parengia Valdymo plano veiksmingumo išbandymo įvertinimo ataskaitą (toliau – ataskaita), kurioje aprašomi atliktų bandymų rezultatai (pastebėti trūkumai, pasiūlomos šių trūkumų šalinimo priemonės). Ataskaitą tvirtina Informacinės sistemos tvarkytojos direktorius.

34. Informacinės sistemos tvarkytoja teikia ataskaitos patvirtinimo duomenis, nurodydama patvirtinimo datą ir registracijos numerį į Kibernetinio saugumo informacinę sistemą (toliau – KSIS) ne vėliau kaip per 5 darbo dienas nuo ataskaitos patvirtinimo.

35. NKSC atliekant Informacinės sistemos tvarkytojos Informacinės sistemos patikrinimą, Informacinės sistemos tvarkytoja privalo pateikti ataskaitos kopiją KSIS per 5 darbo dienas nuo NKSC prašymo gavimo dienos.

36. Informacinės sistemos saugos įgaliotinis nuolat kontroliuoja ataskaitoje nurodytų trūkumų šalinimo priemonių įgyvendinimą.

37. Valdymo plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami laikantis šių principų:

37.1. operatyvumo: kuo greičiau išspręsti ir pašalinti trūkumus. Atliekant trūkumų šalinimo veiklą, turi būti atsižvelgiama į trūkumų sudėtingumą ir apimtį. Informacinės sistemos saugos įgaliotinis nusprendžia ir nustato, per kiek laiko turi būti atliktas konkretus trūkumų šalinimo veiksmas ir pašalinti trūkumai;

37.2. veiksmingumo: trūkumų šalinimas laikomas veiksmingu, jei pavyko sumažinti konkretaus trūkumo daroma neigiamą poveikį registrams;

37.3. ekonomiškumo: siekis pašalinti visus trūkumus taupiai naudojant turimus išteklius.

_____

Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
informacinių sistemų
veiklos tęstinumo valdymo plano
1 priedas

ŽUVININKYSTĖS TARNYBOS PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS INFORMACINIŲ SISTEMŲ VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Pavojaus rūšys	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Už veiklos atkūrimą atsakingi asmenys
1. Oro sąlygos (smarkus lietus, labai smarki audra, viesulas, škvalas, kruša, žemės drebėjimas, smarkus speigas ir t.t.)	1.1. Elektroninės informacijos saugos (kibernetinio) incidento pasekmių įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas	1.1.1. Elektroninės informacijos saugos (kibernetinio) incidento metu padarytos žalos įvertinimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos administratorius
		1.1.2. Pavojaus sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas ir paskelbimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos administratorius
		1.1.3. Priemonių plano įgyvendinimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos administratorius
	1.2. Darbuotojų elektroninės informacijos saugos (kibernetinio) incidento pasekmėms likviduoti paskyrimas	1.2.1. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos saugos įgaliotinis

Pavojaus rūšys	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Už veiklos atkūrimą atsakingi asmenys
		1.2.2. Žalą likviduojančių darbuotojų veiksmų koordinavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos saugos įgaliotinis
	1.3. Pavojaus vietų ženklinimas	1.3.1. Darbuotojų informavimas 1.3.2.Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos saugos įgaliotinis
2. Gaisras	2.1. Priešgaisrinės gelbėjimo tarnybos informavimas	2.1.1. Įvykio vietos lokalizavimas, jei gauta rekomendacija	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos darbuotojas, atsakingas už priešgaisrinę saugą
		2.1.2. Galimybių evakuoti darbuotojus paieška, jei yra rekomenduojama tai padaryti	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos darbuotojas, atsakingas už priešgaisrinę saugą
	2.2. Darbuotojų evakavimas (pagal priešgaisrinės gelbėjimo tarnybos rekomendaciją)	2.2.1. Darbuotojų informavimas apie evakavimą, jei yra rekomendacija	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos darbuotojas, atsakingas už priešgaisrinę saugą
	2.3. Komunikacijų, sukeliančių pavojų, išjungimas, gaisro gesinimas ankstyvoje stadijoje, jei yra rekomendacija dirbti pavojaus zonoje	2.3.1. Priešgaisrinės gelbėjimo tarnybos nurodymų vykdymas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos darbuotojas, atsakingas už priešgaisrinę saugą

Pavojaus rūšys	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Už veiklos atkūrimą atsakingi asmenys
3. Patalpų užgrobimas	3.1. Teisėsaugos institucijų informavimas	3.1.1. Įvykio vietos lokalizavimas, jei yra teisėsaugos institucijos rekomendacijos	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
		3.1.2. Galimybių evakuoti darbuotojus nagrinėjimas, jei gauta rekomendacija	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
	3.2. Darbuotojų evakavimas, jei yra teisėsaugos institucijos rekomendacija	3.2.1. Darbuotojų informavimas apie evakavimą	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
	3.3. Patalpų užrakinimas, jei yra galimybė	3.3.1. Teisėsaugos institucijos nurodymų vykdymas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
	3.4. Teisėsaugos institucijos nurodymų vykdymas	3.4.1. Darbuotojų informavimas apie nurodymų vykdymą	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
	3.5. Veiksmai išlaisvinus užgrobtas patalpas	3.5.1. Padarytos žalos įvertinimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas

Pavojaus rūšys	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Už veiklos atkūrimą atsakingi asmenys
		3.5.2. Padarytos žalos likvidavimo priemonių plano sudarymas, paskelbimas, vykdymas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
		3.5.3. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
4. Patalpai padaryta žala arba patalpos praradimas	4.1. Atitinkamos tarnybos informavimas apie pavojaus pobūdį	4.1.1. Suinteresuotos tarnybos rekomendacijų dėl galimybės dirbti pavojaus zonoje gavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai
		4.1.2. Darbuotojų informavimas apie rekomendacijas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai
	4.2. Portalo įrangos perkėlimas į atsargines patalpas	4.2.1. Darbuotojų informavimas apie darbą patalpose	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai
5. Energijos tiekimo sutrikimai	5.1. Energijos tiekimo sutrikimo priežasčių nustatymas, tarnybinių stočių, kitos techninės įrangos energijos maitinimo išjungimas	5.1.1. Sutrikimų šalinimo organizavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
	5.2. Kreipimasis į energijos tiekimo įmonę dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių	5.2.1. Rekomendacijų iš energijos tiekimo įmonės gavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
	5.3. Sutrikimų pašalinimas	5.3.1. Pavojaus sustabdymas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas

Pavojaus rūšys	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Už veiklos atkūrimą atsakingi asmenys
		5.3.2. Padarytos žalos įvertinimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
		5.3.3. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
6. Vandentiekio ir šildymo sistemos sutrikimai	6.1. Vandentiekio ar šildymo paslaugų teikėjų informavimas	6.1.1. Vandentiekio ar šildymo paslaugų teikėjų paklausimas dėl leidimo dirbti ir rekomendacijų gavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
		6.1.2. Darbuotojų informavimas apie rekomendacijas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
	6.2. Sutrikimo šalinimo prognozės skelbimas, sutrikimo pašalinimas	6.2.1. Padarytos žalos įvertinimas, sutrikimo sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas, plano įgyvendinimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas
		6.2.2. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos tvarkytojos direktoriaus paskirtas darbuotojas

Pavojaus rūšys	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Už veiklos atkūrimą atsakingi asmenys
7. Ryšio sutrikimai	7.1. Ryšio sutrikimo priežasčių nustatymas	7.1.1. Kreiptis į ryšio paslaugos teikėją	Bendrųjų reikalų skyriaus atsakingas darbuotojas
	7.2. Ryšio paslaugų teikėjo informavimas, paklausimo dėl sutrikimo trukmės ir pašalinimo prognozės	7.2.1. Nustatyti ir įgyvendinti priemones, apsaugančias nuo ryšio sutrikimų pasikartojimo	Bendrųjų reikalų skyriaus atsakingas darbuotojas
	7.3. Sutrikimo pašalinimas	7.3.1. Kreiptis į kitą ryšio paslaugos teikėją, jei sutrikimas nepašalintas	Bendrųjų reikalų skyriaus atsakingas darbuotojas
8. Tarnybinės stoties, komutacinės įrangos sugadinimas, praradimas	8.1. Pranešti teisėsaugos institucijai (tyčinio sugadinimo ar praradimo atveju), draudimo bendrovei apie įvykį	8.1.1. Darbuotojų elektroninės informacijos saugos (kibernetinio) incidento pasekmėms likviduoti paskyrimas, instruktavimas, jų veiksmų nustatymas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai
	8.2. Elektroninės informacijos saugos(kibernetinio) incidento pasekmių šalinimas	8.2.1. Kreiptis į įrangos tiekėjus dėl įrangos remonto ar naujos įrangos įsigijimo	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai
		8.2.2. Įsigytos įrangos diegimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai
9. Programinės įrangos sugadinimas, praradimas	9.1. Elektroninės informacijos saugos (kibernetinių) incidento pasekmių įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas	9.1.1. Elektroninės informacijos saugos (kibernetinio) incidento metu padarytos žalos įvertinimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos saugos įgaliotinis
		9.1.2. Priemonių plano sudarymas, paskelbimas ir įgyvendinimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos saugos įgaliotinis
	9.2. Darbuotojų elektroninės informacijos saugos (kibernetinio) incidento pasekmėms likviduoti paskyrimas, žalą likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas	9.2.1. Žalą likviduojančių darbuotojų instruktavimas	Informacinės sistemos saugos įgaliotinis
2.		9.2.2. Kreipimasis į teisėsaugos institucijas dėl programinės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos saugos įgaliotinis

Pavojaus rūšys	Pirmaeiliai veiksmai	Veiklos atkūrimo veiksmai	Už veiklos atkūrimą atsakingi asmenys
10. Duomenų pakeitimas, sunaikinimas, atskleidimas, dokumentų praradimas	10.1. Elektroninės informacijos saugos (kibernetinio) incidento pasekmių įvertinimas	10.1.1. Prarastų IS / registrų duomenų įvertinimas ir jų atkūrimo organizavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos saugos įgaliotinis
		10.1.2. Prarastų, iškraipytų ar sunaikintų IS / registrų duomenų atkūrimo kontrolė	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos saugos įgaliotinis

_____

Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
informacinių sistemų
veiklos tęstinumo valdymo plano
2 priedas

ŽUVININKYSTĖS TARNYBOS PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS INFORMACINIŲ SISTEMŲ ATKŪRIMO PIRMAEILIŲ VEIKSMŲ IR ATSAKINGŲ ASMENŲ PAREIGYBIŲ SĄRAŠAS

Eil. Nr. (pirmaeilis veiksmas)	Veikla	Atsakingi už Informacinės sistemos atkūrimą
	Kompiuterių tinklo veikimo atkūrimo organizavimas	Bendrųjų reikalų skyriaus atsakingas darbuotojas Atkūrimo grupė
	Tarnybinių stočių veikimo atkūrimo organizavimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Atkūrimo grupė
	Kompiuterizuotų darbo vietų veikimo atkūrimo organizavimas	Bendrųjų reikalų skyriaus atsakingas darbuotojas Atkūrimo grupė
	Informacinės sistemos duomenų bazės valdymo sistemos funkcijų atkūrimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai
	Informacinės sistemos funkcijų atkūrimas	Informacinės sistemos paslaugas teikiantys paslaugų tiekėjai Informacinės sistemos administratorius

_____

PATVIRTINTA
Žuvininkystės tarnybos prie
Lietuvos Respublikos žemės
ūkio ministerijos direktoriaus
2025 m. rugsėjo 1 d. įsakymu
Nr. V1-83

ŽUVININKYSTĖS TARNYBOS PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS INFORMACINIŲ SISTEMŲ KIBERNETINIŲ INCIDENTŲ VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos (toliau – Žuvininkystės tarnyba) informacinių sistemų kibernetinių incidentų valdymo plano (toliau – Planas) tikslas – nustatyti kibernetinių incidentų valdymo procedūras, atliekamas valdant kibernetinius incidentus informacinėse sistemose (toliau – Informacinės sistemos).

2. Planas parengtas 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“, Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planu, patvirtintu Lietuvos Respublikos krašto apsaugos ministro 2023 m. spalio 16 d. įsakymu Nr. V-840 „Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“.

3. Vartojamos sąvokos:

3.1. **Kibernetinis incidentas** – įvykis ar veika kibernetinėje erdvėje, galintis sukelti arba sukeliantis grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintis trikdyti arba trikdantis ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

3.2. **Kibernetinius incidentus tiriančios ir valdančios organizacijos** – Valstybinė duomenų apsaugos inspekcija, Policijos departamentas prie Vidaus reikalų ministerijos, Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos.

3.3. Informacinės sistemos **kibernetinio saugumo vadovas –** Žuvininkystės tarnybos direktoriaus įsakymu paskirtas asmuo, atsakingas už kibernetinio saugumo politikos įgyvendinimą, vidinių procedūrų kontrolę, stebėseną ir tobulinimą.

3.4. Informacinės sistemos **saugos įgaliotinis –** Žuvininkystės tarnybos 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 **administratorius** – Žuvininkystės tarnybos direktoriaus įsakymu paskirtas asmuo, prižiūrintis Informacinės sistemos, užtikrinantis jų veikimą ir elektroninės informacijos saugą.

3.6. Kitos Plane vartojamos sąvokos atitinka Plano 2 punkte nurodytuose teisės aktuose apibrėžtas sąvokas.

4. Už Planui įgyvendinti būtinų žmogiškųjų bei materialinių resursų užtikrinimą atsako Žuvininkystės tarnybos direktorius.

II SKYRIUS
KIBERNETINIO INCIDENTO VALDYMO ORGANIZAVIMAS

5. Asmenų, dalyvaujančių kibernetinio incidento valdymo veikloje, kontaktinė informacija ir funkcijos nurodyti Plano 2 priede.

6. Kibernetinio incidento valdymo schema pateikta Plano 3 priede.

7. Ypatingos svarbos informacinės infrastruktūros techninė specifikacija, topologija, nuostatai, saugos dokumentai ir kita kibernetiniams incidentams valdyti svarbi informacija pateikti Žuvininkystės tarnybos dokumentų valdymo platformos Informacinės sistemos saugos įgaliotinio direktorijoje.

8. Didžiausias leistinas ypatingos svarbos informacinės infrastruktūros neveikimo laikas nurodytas Žuvininkystės tarnybos Poveikio veiklai vertinimo dokumente.

9. Informacinės sistemos kibernetinės saugos vadovas, atsakingas už kibernetinio saugumo politikos įgyvendinimą *(paskirtas Žuvininkystės tarnybos direktoriaus įsakymu)*.

10. Informacinės sistemos saugos įgaliotinis, atsakingas už kibernetinių incidentų valdymą *(paskirtas Žuvininkystės tarnybos direktoriaus įsakymu)*.

11. Informacinės sistemos administratorius, atsakingas už Informacinės sistemos priežiūrą, užtikrinant jų veikimą ir elektroninės informacijos saugą *(paskirtas Žuvininkystės tarnybos direktoriaus įsakymu).*

12. Žuvininkystės tarnyba kibernetinio incidento valdymo metu informacija su Nacionaliniu kibernetinio saugumo centru prie krašto apsaugos ministerijos (toliau – NKSC), kibernetinius incidentus tiriančiomis ir valdančiomis organizacijomis keičiamasi turimomis informacijos perdavimo priemonėmis (fiksuotojo ryšio telefonais, mobiliaisiais telefonais, elektroniniu paštu, palydoviniu ryšiu ir pan.).

13. Informacinės sistemos kibernetinės saugos vadovo, Informacinės sistemos saugios įgaliotinio, taip pat kitų asmenų, susijusių su kibernetinių incidentų valdymu, kontaktinė informacija – elektroninio pašto adresas, telefono numeriai – pateikiami NKSC, naudojantis Kibernetinio saugumo informaciniu tinklu (toliau – KSIT), organizacijos posistemyje.

III SKYRIUS
KIBERNETINIO INCIDENTO NUSTATYMAS

14. Informacija apie galimą kibernetinį incidentą gali būti gauta iš įvairių informacijos šaltinių: Žuvininkystės tarnybos valstybės tarnautojo arba darbuotojo, dirbančio pagal darbo sutartį

(toliau – darbuotojas), kuris atlieka kibernetinių incidentų stebėseną, automatizuotų kibernetinių incidentų aptikimo priemonių, kompetentingų valstybės institucijų, kitų juridinių arba fizinių asmenų, taip pat kitų valstybių, tarptautinių organizacijų arba institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas.

15. Kiekvienas darbuotojas, pastebėjęs ar sužinojęs apie kibernetinį incidentą, privalo nedelsdamas žodžiu ar raštu (el. paštu) apie tai pranešti Informacinės sistemos administratoriui. Informacinės sistemos administratorius, gavęs informaciją apie Informacinės sistemos kibernetinį incidentą, nedelsdamas informuoja Informacinės sistemos saugos įgaliotinį.

16. Informacinės sistemos saugos įgaliotinis gavęs informacijos apie galimą kibernetinį incidentą, pagal kompetenciją jį įvertina ir patvirtina arba paneigia kibernetinio incidento nustatymo faktą.

IV SKYRIUS
KIBERNETINIO INCIDENTO VERTINIMAS IR INFORMAVIMAS APIE KIBERNETINĮ INCIDENTĄ

17. Informacinės sistemos saugos įgaliotinis:

17.1. patvirtinęs kibernetinio incidento nustatymo faktą, vadovaujasi Nacionaliniu kibernetinių incidentų valdymo planu ir nedelsdamas pagal kriterijus, kuriais vadovaujantis kibernetiniai incidentai priskiriami kibernetinių incidentų kategorijoms, sąrašą nustato kibernetinio incidento kategoriją (Plano 6 priedas);

17.2. užregistruoja Žuvininkystės tarnybos informacinių sistemų ir registrų elektroninės informacijos saugos (kibernetinių) incidentų registravimo žurnale (Plano 1 priedas);

17.3. apie kibernetinius incidentus informuoja NKSC, juos registruodamas Kibernetinio saugumo informacinės sistemos posistemyje – Nacionalinėje kibernetinių incidentų valdymo platformoje (toliau – Platforma). Dėl kibernetinio incidento neturint galimybės apie kibernetinius incidentus informuoti automatizuotu būdu per Platformą, NKSC informuoja užpildydamas formą Platformoje, NKSC interneto svetainėje, NKSC nurodytu elektroninio pašto adresu arba telefonu.

17.4. Pranešant apie *didelį kibernetinį incidentą* pateikia:

17.4.1. nedelsiant, bet ne vėliau kaip per 24 valandas nuo sužinojimo apie didelį kibernetinį incidentą momento – *ankstyvasis perspėjimas*, kuriame pagal galimybes nurodoma, ar didelį kibernetinį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai ir ar jis galėtų daryti tarpvalstybinį poveikį;

17.4.2. nedelsiant, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie didelį kibernetinį incidentą momento – *pranešimas apie kibernetinį incidentą*, kuriame pagal galimybes atnaujinama ankstyvojo perspėjimo metu nurodyta informacija ir nurodomas didelio kibernetinio incidento, įskaitant jo sunkumą ir poveikį, pradinis vertinimas, taip pat nurodomi įsilaužimo įrodymai, jeigu tokių yra;

17.4.3. Nacionalinio kibernetinio saugumo centro prašymu – tarpinė atitinkamų atnaujintų padėties duomenų ataskaita per Nacionalinio kibernetinio saugumo centro nurodytą pateikimo terminą;

17.4.4. ne vėliau kaip per vieną mėnesį nuo ankstyvojo perspėjimo pranešimo apie kibernetinį incidentą pateikimo dienos – *galutinė ataskaita*, kurioje pateikiama ši informacija:

17.4.4.1. išsamus kibernetinio incidento, įskaitant jo sunkumą ir poveikį, aprašymas;

17.4.4.2. grėsmės arba pagrindinės priežasties, dėl kurios kibernetinis incidentas galėjo įvykti, rūšis;

17.4.4.3. taikomos ir įgyvendinamos kibernetinio incidento poveikio mažinimo priemonės;

17.4.4.4. tarpvalstybinis kibernetinio incidento poveikis, jeigu toks buvo;

17.4.5. jeigu galutinės ataskaitos pateikimo metu kibernetinis incidentas tebevyksta, pateikiama pažangos ataskaita (kas mėnesį atnaujinama *pranešimo apie kibernetinį incidentą* duomenys), o galutinė ataskaita – per vieną mėnesį nuo dienos, kai kibernetinis incidentas buvo suvaldytas.

17.5. Pranešant apie *nedidelį kibernetinį incidentą* pateikia:

17.5.1. nedelsiant, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie kibernetinį incidentą momento, *pranešimą apie kibernetinį incidentą*, jame pateikiant 16.4.2. punkte nurodytą informaciją;

17.5.2. per vieną mėnesį nuo *pranešimo apie kibernetinį incidentą* registravimo dienos *galutinę ataskaitą* apie nedidelį kibernetinį incidentą, joje pateikiant 16.4.4. punkte nurodytą informaciją. Galutinė ataskaita apie nedidelį kibernetinį incidentą neteikiama, jei pranešime apie kibernetinį incidentą pateikta visa galutinės ataskaitos informacija.

17.6. Teikiant *galutinę ataskaitą*, grėsmės arba pagrindinės priežasties, dėl kurios kibernetinis incidentas galėjo įvykti, rūšis parenkama viena iš išvardytų kibernetinių grėsmių ir pagrindinių incidentų priežasčių, nurodytų 5 Priede.

17.7. jei kibernetinis incidentas turi nusikalstamos veikos požymių (informacijos sunaikinimas ar pakeitimas, kompiuterių tinklo trikdymas, neteisėtas prisijungimas ir informacijos pasisavinimas, neteisėtas disponavimas kitais įrenginiais ir duomenimis ar pan.), informuoja Policijos departamentą Plano 4 priede nurodytais kontaktais;

17.8. jei kibernetinio incidento metu buvo paveiktas valdomų ir (ar) tvarkomų asmens duomenų konfidencialumas, autentiškumas, vientisumas, prieinamumas, informuoja Valstybinę duomenų apsaugos inspekciją Plano 4 priede nurodytais kontaktais;

17.9. gavęs kibernetinius incidentus tiriančių ir valdančių organizacijų prašymus, per nurodytą terminą patikslina arba papildo informaciją apie kibernetinį incidentą;

17.10. jeigu kibernetinio incidento buvimo faktas paneigiamas, apie tai informuoja NKSC, nurodydamas kibernetinio incidento paneigimo priežastis.

V SKYRIUS
KIBERNETINIO INCIDENTO VALDYMAS

18. Siekdami suvaldyti kibernetinį incidentą ir atkurti įprastą ypatingos svarbos informacinės infrastruktūros veiklą, Plano 2 priede nurodyti asmenys, atlikdami savo funkcijas, imasi visų galimų organizacinių, techninių ir teisinių priemonių.

19. Pagrindiniai kriterijai, kuriais vadovaujantis priimamas sprendimas dėl kibernetinio incidento valdymo priemonių:

19.1. Plano 2 priede nurodytų asmenų pasiūlymai dėl kibernetinio incidento valdymo;

19.2. kibernetinio incidento įrodymų išsaugojimas (įrašų išsaugojimas, jų patikimumo, vientisumo ir pasiekiamumo užtikrinimas);

19.3. didžiausias leistinas ypatingos svarbos informacinės infrastruktūros neveikimo laikas;

19.4. kibernetinio incidento valdymo sprendimui įgyvendinti reikalingas laikas ir ištekliai;

19.5. numatoma galima žala, kurią gali padaryti kibernetinis incidentas, priėmus jo valdymo sprendimą.

20. Kibernetinį incidentą priskyrus nedidelio poveikio kibernetinių incidentų kategorijai Informacinės sistemos saugos įgaliotinis, atsižvelgdamas į kibernetinio incidento tipą ir galimas jo valdymo priemones, parenka efektyviausią galimą kibernetinio incidento valdymo priemonę ir organizuoja jos taikymą.

21. Kibernetinį incidentą priskyrus didelio poveikio kibernetinių incidentų kategorijai:

21.1. Informacinės sistemos saugos įgaliotinis, informuoja Plano 2 priede nurodytus asmenis apie galimas kibernetinio incidento valdymo priemones;

21.2. Plano 2 priede nurodyti asmenys, gavę iš Informacinės sistemos saugos įgaliotinio, išsamią informaciją apie galimas kibernetinio incidento valdymo priemones, per kuo trumpesnį laiką įvertina padėtį, priima sprendimą dėl efektyviausių ir mažiausiai žalos padarysiančių kibernetinio incidento valdymo priemonių taikymo ir jas taiko.

22. Išnykus kibernetinio incidento poveikiui, didelio poveikio kibernetinio incidento tyrimas baigiamas ir kibernetinis incidentas laikomas suvaldytu ir (ar) pasibaigusiu.

23. Suvaldęs kibernetinį incidentą Informacinės sistemos saugos įgaliotinis:

23.1. apie kibernetinio incidento suvaldymo rezultatus informuoja Plano 2 priede nurodytus asmenis;

23.2. per kuo trumpesnį laiką nuo kibernetinio incidento sustabdymo imasi priemonių pažeidžiamumui, dėl kurio įvyko kibernetinis incidentas, pašalinti arba užkardyti;

23.3. NKSC platformoje užpildo kibernetinio incidento galutinę ataskaitą.

24. Prieš atkuriant ypatingos svarbos informacinės infrastruktūros veiklą, vadovaujamasi NKSC ir kitų kibernetinius incidentus tiriančių organizacijų nurodymais bei imamasi visų priemonių kibernetinio incidento įrodymams išsaugoti.

VI SKYRIUS
KIBERNETINIO INCIDENTO PERĖMIMAS

25. Informacinės sistemos saugos įgaliotinis, nustatęs, kad nepavyks savarankiškai ištirti kibernetinio incidento per maksimaliai leistiną ypatingos svarbos informacinės infrastruktūros valdytojo nustatytą ypatingos svarbos paslaugos neveikimo laiką, kreipiasi į NKSC prašydamas pagalbos suvaldyti kibernetinį incidentą.

26. NKSC elektroniniu paštu arba telefonu patvirtinus, kad perima kibernetinio incidento valdymą Informacinės sistemos saugos įgaliotinis:

26.1. nuolat renka, apdoroja informaciją, susijusią su kibernetiniu incidentu;

26.2. nuolat, pagal poreikį, teikia informaciją apie kibernetinį incidentą NKSC, taip pat informaciją apie atliktus kibernetinio incidento tyrimo ir (ar) valdymo veiksmus ir jų rezultatus.

26.3. vykdo NKSC nurodymus ir užtikrina visų būtinų resursų suteikimą kibernetiniam incidentui suvaldyti.

VII SKYRIUS
YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VEIKLOS ATKŪRIMAS

27. Informacinės sistemos saugos įgaliotinis:

27.1. įvykus kibernetiniam incidentui, pagal kompetenciją įvertina ypatingos svarbos informacinės infrastruktūros būklę, nustato pažeistas jos dalis ir per kuo trumpesnį laiką imasi veiksmų pažeistoms dalims atkurti arba pakeisti ir (arba) teikia 2 priede nurodytiems asmenims pagalbą dėl pažeistų dalių atkūrimo arba pakeitimo, jeigu to negali padaryti savo jėgomis;

27.2. prieš atkurdamas ypatingos svarbos informacinės infrastruktūros veiklą ir ypatingos svarbos paslaugos teikimą, įsitikina, jog nėra galimybės išnaudoti pažeidžiamumo, dėl kurio įvyko kibernetinis incidentas;

27.3. apie atkurtą ypatingos svarbos informacinės infrastruktūros veiklą ir (ar) ypatingos svarbos paslaugos teikimą bei pašalintą arba užkardytą pažeidžiamumą informuoja NKSC;

27.4. įvertina ryšių ir informacinės sistemos riziką ir atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams.

28. Informacinės sistemos kibernetinio saugumo vadovas ir (ar) Informacinės sistemos saugos įgaliotinis, po kibernetinio incidento tyrimo išanalizavęs ir įvertinęs visą informaciją, susijusią su kibernetiniu incidentu, atliktus veiksmus ir panaudotas priemones, ne vėliau kaip per trisdešimt darbo dienų po kibernetinio incidento suvaldymo ar pasibaigimo pateikia kibernetinio incidento analizės rezultatus NKSC ir KSIT paskelbia susistemintą ir aktualią neįslaptintą informaciją apie kibernetinio incidento nustatymą ir suvaldymą.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

29. Informacinės sistemos kibernetinio saugumo vadovas:

29.1. sudaro su ypatingos svarbos informacinės infrastruktūros funkcionalumu susijusių paslaugos teikėjų (trečiųjų šalių), į kuriuos būtų kreipiamasi kibernetinio incidento valdymo metu, kontaktų sąrašą ir kas metus jį atnaujina;

29.2. vertina kibernetinio incidento valdymo procedūras ir nustatęs neatitikčių inicijuoja Plano pakeitimus. Nustatęs kitų teisinio reguliavimo trūkumų, inicijuoja ir kitų kibernetinio saugumo teisės aktų pakeitimus arba juo keičia;

29.3. organizuoja Plano veiksmingumo išbandymą ne rečiau kaip kartą per metus, kai imituojamas kibernetinis incidentas ir kibernetinio incidento valdymo veiklos dalyviai atlieka būtinus tokiomis aplinkybėmis veiksmus. Plano veiksmingumo išbandymo ataskaita perduodama NKSC Plano 4 priede nurodytu elektroniniu paštu.

30. Atsižvelgdami į gautus Plano veiksmingumo išbandymo rezultatus, Plano veiksmingumo išbandymo dalyviai, taip pat kibernetinio incidento valdymo veiklos dalyviai, įvertinę kibernetinio incidento valdymo metu įgytą patirtį ir nustatę galimus teisinio reguliavimo trūkumus, pateikia Plano 2 priede nurodytiems asmenimis siūlymus dėl Plano ir (ar) kitų kibernetinį saugumą reglamentuojančių ir su ypatingos svarbos informacinės infrastruktūros kibernetiniu saugumu susijusių procedūrų gerinimo ir papildomų kibernetinio saugumo priemonių įsigijimo.

Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
informacinių sistemų
kibernetinių incidentų valdymo plano
1 priedas

ŽUVININKYSTĖS TARNYBOS PRIE LIETUVOS RESPUBLIKOS ŽEMĖS ŪKIO MINISTERIJOS INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS (KIBERNETINIŲ) INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia 20___m._____d.

Eil. Nr.	Elektroninės informacijos saugos (kibernetinis) incidentas						
	Įstaigos pavadinimas	Pavojaus rūšies numeris	Įvykio aprašymas	Pradžia (metai, mėnuo, diena, valanda)	Pabaiga (metai, mėnuo, diena, valanda)	Incidentą pašalino (vardas, pavardė ir pareigos)	Informacinės sistemos saugos įgaliotinis (vardas, pavardė, parašas)
1.							
2.							
3.							
4.							
5.							

Elektroninės informacijos saugos (kibernetinio) incidento pavojaus rūšis:
1 – oro sąlygos; 2 – gaisras; 3 – patalpų užgrobimas; 4 – patalpai padaryta žala arba patalpos praradimas; 5 – energijos tiekimo sutrikimai; 6 – vandentiekio ir šildymo sistemos sutrikimai; 7 – ryšio sutrikimai; 8 – tarnybinės stoties, komutacinės įrangos sugadinimas, praradimas; 9 – programinės įrangos sugadinimas, praradimas; 10 – duomenų pakeitimas, sunaikinimas, atskleidimas, dokumentų praradimas; 11 – darbuotojų kaita, praradimas.

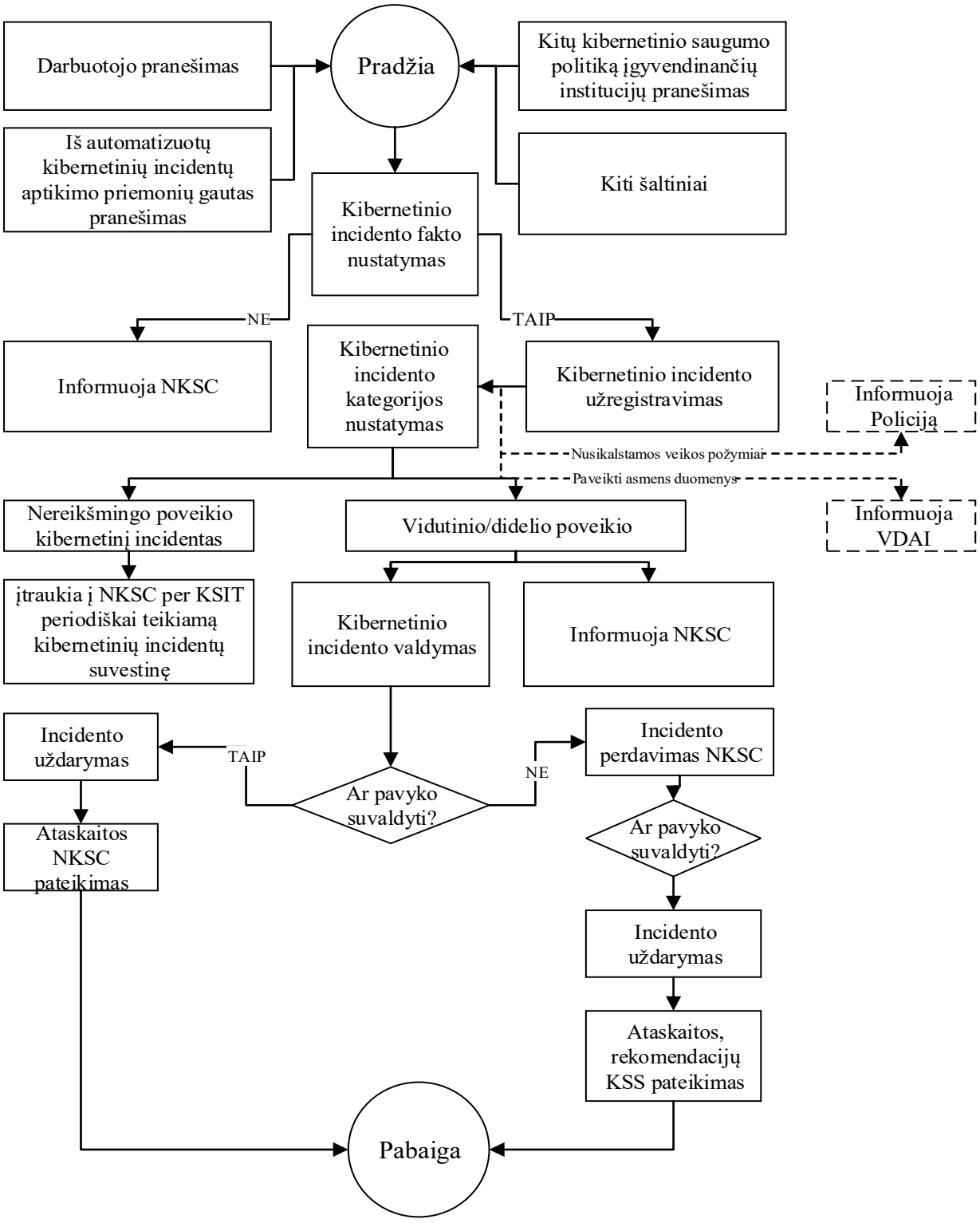
Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
informacinių sistemų
kibernetinių incidentų valdymo plano
2 priedas

ASMENŲ, DALYVAUJANČIŲ KIBERNETINIO INCIDENTO VALDYMO VEIKLOJE, KONTAKTINĖ INFORMACIJA IR FUNKCIJOS

Vardas pavardė	Kontaktinė informacija (telefono numeris, el. pašto adresas)	Funkcijos
Sigitas Narkus, Informacinės sistemos administratorius	*Sigitas Narkus, sigitas.narkus@zuv.lt +370 700 14 906*	*Vykdo kibernetinio incidento suvaldymo veiksmus; Išsaugo su kibernetiniu incidentu susijusius įrodymus*
Marius Kaziliūnas, Informacinės sistemos administratorius	*Marius Kaziliūnas, marius.kaziliunas@zuv.lt +370 700 14 958*	
Advisense, UAB, Informacinės sistemos kibernetinės saugos vadovas, Informacinės sistemos saugos įgaliotinis	*Sandra Aleksiūnaitė, Sandra.aleksiunaite@advisense.com +37067113977* *Erika Vaškelevičienė, Erika.vaskeleviciene@advisense.com +37062265862* *Paulius Širvaitis Paulius.sirvaitis@advisense.com*	*Įvertina kibernetinį incidentą, bei nustato jo kategoriją. Informuoja NKSC apie Incidentą Organizuoja kibernetinio incidento suvaldymą.*
Evelina Vaiginė, Duomenų apsaugos pareigūnas	*Evelina Vaiginė, evelina.vaigine@zuv.lt +370 700 14 979*	*Padeda nustatyti ar incidentas galėjo sukelti duomenų pažeidimą, apie kurį turi būti informuota VDAI*

Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos informacinių sistemų kibernetinių incidentų valdymo plano 3 priedas

KIBERNETINIO INCIDENTO VALDYMO SCHEMA



_____

Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
informacinių sistemų
kibernetinių incidentų valdymo plano
4 priedas

INSTITUCIJŲ, DALYVAUJANČIŲ KIBERNETINIO INCIDENTO VALDYMO VEIKLOJE, KONTAKTINĖ INFORMACIJA

Institucija	**Kontaktinė informacija (telefono numeris, el. pašto adresas ir pan.)**	**Pastabos**
Nacionalinis kibernetinio saugumo centras prie KAM	Tel. 1843 el. p. cert@nksc.lt, https://www.nksc.lt/pranesti.html	*Nustatytas vidutinio ar didelio poveikio kibernetinis incidentas.*
Policija	Tel. (8 5) 271 7933, el. p. cyberpolice@policija.lt	*Jei kibernetinis incidentas turi nusikalstamos veikos požymių (informacijos sunaikinimas ar pakeitimas, kompiuterių tinklo trikdymas, neteisėtas prisijungimas ir informacijos pasisavinimas, neteisėtas disponavimas kitais įrenginiais ir duomenimis ar pan.).*
Valstybinė duomenų apsaugos inspekcija	Tel. (8 5) 271 28 04, (8 5) 279 1445, el. p. ada@ada.lt	*Jei kibernetinio incidento metu buvo paveiktas valdomų ir (ar) tvarkomų asmens duomenų konfidencialumas, autentiškumas, vientisumas, prieinamumas*

_____

Žuvininkystės tarnybos prie Lietuvos
Respublikos žemės ūkio ministerijos
informacinių sistemų
kibernetinių incidentų valdymo plano
5 priedas

GRĖSMĖS ARBA PAGRINDINĖS PRIEŽASTIES, DĖL KURIOS KIBERNETINIS INCIDENTAS GALĖJO ĮVYKTI, RŪŠIS

1. Nepageidaujamų laiškų ir (ar) klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content, spam*) ir (ar) tinklų informacinės sistemos veiklos trikdymas.

2. Kenkimo programinė įranga (*angl. malicious software / code*): programinė įranga ar jos dalis, kuri padeda neteisėtai prisijungti prie tinklų ir informacinės sistemos, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti skaitmeninius duomenis, panaikinti ar apriboti galimybę jais naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešus skaitmeninius duomenis tokios teisės neturintiems asmenims ir kuri identifikuota kaip:

2.1. pažangi kenkimo programinė įranga (angl. *advanced persistent threat, APT*);

2.2. tinklų ir informacinės sistemos duomenis šifruojantis ir naikinantis (angl. *wiper*) ar išpirkos reikalaujantis programinis kodas (angl. *ransomware*);

2.3. tinklų ir informacinės sistemos dalys, aktyviai kontroliuojamos įsibrovėlių;

2.4. kenkimo programinės įrangos platinimas.

3. Informacijos rinkimas (angl. *information gathering*): žvalgyba ar kita įtartina veikla, manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. *social engineering*), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti naudotoją atskleisti informaciją (angl. phishing) arba atlikti norimus veiksmus. Naudojami socialinės inžinerijos metodai, siekiant išvilioti prisijungimo prie tinklų ir informacinės sistemos ir (ar) kitą svarbią informaciją.

4. Mėginimas įsilaužti (angl. *intrusion attempts*). Mėginimas įsilaužti arba sutrikdyti tinklų ir informacinės sistemos veikimą išnaudojant žinomas spragas (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą įsilaužimo būdą (angl. *new attack signature),* kurie gali būti skirstomi į:

4.1. išnaudojama viena ar kelios nežinomos spragos (angl. *zero day*);

4.2. tinklų ir informacinės sistemos žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita);

4.3. išnaudojamos žinomos ir viešai publikuotos spragos;

5. Įsilaužimas (angl. *intrusions*). Sėkmingas įsilaužimas ir (ar) neteisėtas tinklų ir informacinės sistemos, taikomosios programinės įrangos ar paslaugos naudojimas (angl. *privileged account compromise, unprivileged account compromise, application compromise*), kuris skirstomas taip:

5.1. veiksmai prieš tinklų ir informacinę sistemą ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, tinklų ir informacinės sistemos ar jos dalies pažeidimas, sutrikdantis

tinklų ir informacinės sistemos teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti tinklų ir informacinės sistemos naudotojų pasitikėjimą jais;

5.2. gaunama neteisėta prieiga prie tinklų ir informacinės sistemos, taikomosios programinės įrangos ar paslaugos.

6. Paslaugų trikdymas, prieinamumo pažeidimai (angl. *availability*): veiksmai, kuriais trikdoma tinklų ir informacinės sistemos veikla, teikiamos paslaugos (angl. *DoS, DDoS*), tinklų ir informacinės sistemos ar jos dalies pažeidimas, sutrikdantis tinklų ir informacinės sistemos ir (ar) jos teikiamas paslaugas, kuris skirstomas taip:

6.1. teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas;

6.2. teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui.

7. Tiekimo grandinės atakos (angl. *supply chain attack*): išnaudojama trečiųjų šalių, teikiančių paslaugas tinklų ir informacinės sistemos valdytojui ir (ar) tvarkytojui, infrastruktūra, siekiant įgauti ar turėti įtaką paslaugos gavėjo tinklų ir informacinės sistemos infrastruktūrai.

8. Informacijos turinio saugumo pažeidimai (angl. *information content security*): neteisėta prieiga prie informacijos, galinčios turėti įtakos tinklų ir informacinės sistemos veiklai ir (ar) teikiamoms paslaugoms, ar jos neteisėtas keitimas.

9. Neteisėta veikla, sukčiavimas (angl. *fraud*): vagystė, apgavystė, neteisėtas išteklių (angl. *unauthorized use of resources*), nelegalios programinės įrangos ar autorių teisių (angl. *copyright*) naudojimas, tapatybės klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai.

10. Kitos grėsmės ar priežastys.

Žuvininkystės tarnybos prie Lietuvos Respublikos žemės ūkio ministerijos informacinių sistemų kibernetinių incidentų valdymo plano 6 priedas

KRITERIJŲ, KURIAIS VADOVAUJANTIS KIBERNETINIAI INCIDENTAI PRISKIRIAMI KIBERNETINIŲ INCIDENTŲ KATEGORIJOMS, SĄRAŠAS

<table>
<tr><td rowspan="11">Didelis incidentas</td><td rowspan="7">Kibernetinio saugumo subjektas patiria ar gali patirti didelių paslaugų teikimo sutrikimų ir kibernetinis incidentas atitinka bent vieną iš šių kriterijų:</td><td>Paslaugos trikdomos visoje Lietuvos teritorijoje ir (ar) bent vienoje Europos sąjungos arba nato šalyje;</td></tr>
<tr><td>Tinklų ir informacinės sistemos veikla trikdoma 2 ar daugiau valandų;</td></tr>
<tr><td>Paveiktų paslaugų gavėjų ar kompiuterizuotų darbo vietų skaičius lygus arba didesnis nei 1 000, arba 25 procentai (atsižvelgiant į tai, kuris dydis yra mažesnis);</td></tr>
<tr><td>Paveikti 1 000 arba 25 procentų (atsižvelgiant į tai, kuris dydis yra mažesnis) paslaugų gavėjų asmens duomenys ar kiti kibernetinio saugumo subjekto saugomi paslaugų gavėjų duomenys;</td></tr>
<tr><td>Kibernetinio saugumo subjektas nebegali užtikrinti teisės aktuose jo veiklai nustatytų reikalavimų įgyvendinimo;</td></tr>
<tr><td>Prarastos arba atskleistos komercinės paslaptys arba įslaptinta informacija;</td></tr>
<tr><td>Per 6 mėnesius patiriamas daugiau nei vienas analogiškas kibernetinis incidentas, incidentų pagrindinė priežastis sutampa, o finansinių nuostolių dydis siekia 9.2 papunktyje numatytas vertes;</td></tr>
<tr><td colspan="2">Kibernetinio saugumo subjektas patiria ar gali patirti didelių finansinių nuostolių, lygių arba didesnių nei 500 000 eur, arba 5 procentų kibernetinio saugumo subjekto praėjusių finansinių metų apyvartos (atsižvelgiant į tai, kuri suma yra mažesnė);</td></tr>
<tr><td rowspan="3">Kibernetinis incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą, atitinkančią bent vieną iš šių kriterijų:</td><td>Galimos turtinės žalos dydis yra lygus arba didesnis nei 400 bazinių socialinių išmokų;</td></tr>
<tr><td>Galimos neturtinės žalos dydis lygus arba didesnis nei 10 000 eur;</td></tr>
<tr><td>Sutrikdyta bent vieno žmogaus sveikata arba bent vienas žmogus žuvo.</td></tr>
<tr><td>Nedidelis incidentas</td><td colspan="2">Kitais atvejais.</td></tr>
</table>