HIGIENOS INSTITUTO
DIREKTORIUS

ĮSAKYMAS
DĖL TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLIŲ, TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO IR TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLIŲ PATVIRTINIMO

2023 m. gruodžio 5 d. Nr. V-156
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 43 straipsnio 2 dalimi ir Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“, 7 ir 8 punktais:

1. T v i r t i n u pridedamus:

1.1. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisykles;

1.2. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos veiklos tęstinumo valdymo planą;

1.3. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos naudotojų administravimo taisykles.

2. N u s t a t a u , kad šis įsakymas įsigalioja 2024 m. sausio 1 d.

Direktorius

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2023 m. lapkričio 23 d. raštu Nr. (4.1 E) 6K-912

PATVIRTINTA
Higienos instituto direktoriaus
2023 m. gruodžio 5 d.
įsakymu Nr. V-156

TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Taisyklės) tikslas – sudaryti sąlygas saugiai tvarkyti Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos (toliau – Informacinė sistema) elektroninę informaciją ir užtikrinti kibernetinį saugumą.

2. Taisyklės parengtos vadovaujantis:

2.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

2.2. Lietuvos Respublikos valstybės informacinių išteklių įstatymu;

2.3. Lietuvos Respublikos kibernetinio saugumo įstatymu;

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

2.5. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas).

3. Taisyklėse vartojamos sąvokos atitinka Taisyklių 2 punkte nurodytuose teisės aktuose vartojamas sąvokas.

4. Informacinėje sistemoje tvarkoma elektroninė informacija yra skirstoma į šias kategorijas:

4.1. Informacinės sistemos administratoriaus tvarkoma elektroninė informacija;

4.2. Informacinės sistemos naudotojų tvarkoma elektroninė informacija.

5. Elektroninės informacijos, priskirtos Taisyklių 4 punkte nurodytoms kategorijoms, sąrašas:

5.1. Informacinės sistemos administratoriaus tvarkoma elektroninė informacija:

5.1.1. Informacinės sistemos naudotojų prisijungimo vardai ir slaptažodžiai;

5.1.2. Informacinės sistemos klasifikatoriai;

5.1.3. Informacinės sistemos naudotojų teisės;

5.1.4. Informacinės sistemos naudotojų veiksmų registravimo duomenys.

5.2. Informacinės sistemos naudotojų tvarkoma informacija – Informacinės sistemos duomenys, nurodyti Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos nuostatų, patvirtintų Lietuvos Respublikos sveikatos apsaugos ministro 2014 m. liepos 9 d. įsakymu Nr. V-776 „Dėl Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos nuostatų ir duomenų saugos nuostatų patvirtinimo“ (toliau – Informacinės sistemos nuostatai), 13 punkte.

6. Už Taisyklių 5.1 papunktyje nurodytos elektroninės informacijos tvarkymą atsakingas Informacinės sistemos administratorius, o už Taisyklių 5.2 papunktyje nurodytos elektroninės informacijos tvarkymą atsakingi Informacinės sistemos naudotojai.

7. Informacinėje sistemoje tvarkoma elektroninė informacija pagal svarbą priskiriama vidutinės svarbos informacinių išteklių kategorijai.

8. Informacinės sistemos elektroninė informacija yra saugoma Informacinės visuomenės plėtros komiteto debesijos paslaugų platformoje (tarnybinėse stotyse).

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

9. Kompiuterinės įrangos saugos priemonės:

9.1. Informacinės sistemos tarnybinės stotys ir kompiuterinė įranga turi įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį Informacinės sistemos tarnybinių stočių veikimą;

9.2. Informacinės sistemos tarnybinėse stotyse ir Informacinės sistemos naudotojų kompiuterizuotose darbo vietose naudojamos kenksmingos programinės įrangos aptikimo, stebėjimo realiuoju laiku priemonės;

9.3. apsaugai naudojama programinė įranga privalo automatiškai informuoti Informacinės sistemos administratorių apie tai, kurių Informacinės sistemos posistemių, funkciškai savarankiškų sudedamųjų dalių kenkimo programinės įrangos aptikimo priemonių atsinaujinimo laikas yra pradelstas;

9.4. Informacinės sistemos komponentai be kenksmingo programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu Informacinės sistemos rizikos vertinimo metu yra patvirtinama, kad šių komponentų rizika yra priimtina;

9.5. Informacinės sistemos naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga. Informacinės sistemos saugos įgaliotinis turi parengti, su Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo vadovu suderinti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti leistinos programinės įrangos sąrašą;

9.6. Informacinės sistemos techninė ir programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

9.7. Informacinės sistemos techninės ir programinės įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai.

10. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

10.1. Informacinės sistemos tarnybinėse stotyse ir Informacinės sistemos naudotojų kompiuteriuose naudojama tik legali, Informacinės sistemos funkcijoms vykdyti būtina programinė įranga;

10.2. operatyviai įdiegiami Informacinės sistemos tarnybinių stočių ir Informacinės sistemos naudotojų darbo vietų kompiuterinės įrangos, operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

10.3. Informacinės sistemos administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie Informacinės sistemos posistemiams, funkciškai savarankiškoms sudedamosioms dalims, vidinių Informacinės sistemos naudotojų darbo vietų kompiuterinei įrangai neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumų svarbos lygius;

10.4. programinės įrangos diegimą, šalinimą ir konfigūravimą turi teisę atlikti tik Informacinės sistemos administratorius arba kitas Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo įgaliotas asmuo;

10.5. Informacinė sistema perspėja Informacinės sistemos administratorių, kai pagrindinėje informacinės sistemos kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

10.6. programinei įrangai testuoti naudojama atskira testavimo aplinka;

10.7. Informacinės sistemos neveikimo laikotarpis negali būti ilgesnis nei 16 val.;

10.8. atsarginės laikmenos su programinės įrangos kopijomis laikomos nedegioje spintoje, kitose patalpose arba kitame pastate nei yra informacinės sistemos tarnybinės stotys;

10.9. Informacinės sistemos tarnybinėse stotyse įrašomi ir saugomi duomenys apie Informacinės sistemos tarnybinių stočių ir taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis Informacinės sistemos tarnybinėse stotyse, kitus elektroninei saugai svarbius įvykius, nurodant naudotojo identifikatorių ir įvykio laiką. Šie duomenys yra saugomi 30 dienų atskirai nuo Informacinės sistemos, kurioje jie buvo įrašyti. Informacinės sistemos administratorius ne rečiau kaip kartą per savaitę analizuoja šiuos įrašus;

10.10. pagrindinėse tarnybinėse stotyse turi būti įjungtos saugasienės, sukonfigūruotos visam įeinančiam ir išeinančiam duomenų, išskyrus su Informacinės sistemos funkcionalumu ir administravimu susijusius duomenis, srautui blokuoti;

10.11. ne rečiau kaip kartą per mėnesį atliekama saugasienių užfiksuotų įvykių analizė ir pastebėtos neatitiktys saugumo reikalavimams šalinamos;

10.12. įsilaužimo aptikimo konfigūracijos ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo Informacinės sistemos techninės įrangos (kartu nurodant atitinkamas datas (įgyvendinimo, atnaujinimo ir panašiai), atsakingus asmenis, taikymo periodus ir panašiai);

10.13. draudžiama Informacinės sistemos techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į saugos reikalavimus atitinkančius slaptažodžius.

11. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

11.1. Informacinės sistemos elektroninės informacijos perdavimo tinklas atskirtas nuo viešųjų ryšių tinklų naudojant saugasienę, saugasienės įvykių žurnalai turi būti reguliariai analizuojami, o saugasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

11.2. Informacinės sistemos programinė įranga apsaugota nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų atakų;

11.3. Informacinės sistemos tinklo perimetro apsaugai naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių Informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

11.4. viešaisiais ryšių tinklais perduodamos Informacinės sistemos elektroninės informacijos konfidencialumas užtikrinamas naudojant šifravimą, virtualų privatų tinklą (VPN).

12. Belaidis tinklas nėra naudojamas Informacinės sistemos veiklai vykdyti.

13. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

13.1. Informacinės sistemos tarnybinių stočių patalpos apsaugotos nuo neteisėto asmenų patekimo į jas;

13.2. Informacinės sistemos tarnybinių stočių patalpose įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos;

13.3. naudotojų ir techninės įrangos patalpose įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos;

13.4. veikia patekimo į patalpas kontrolės sistema; asmenys, nesusiję su Informacinės sistemos tvarkymu, patekti į tarnybinių stočių patalpas ir patalpas, kuriose saugomos kopijos, gali tik lydimi Informacinės sistemos administratoriaus;

13.5. patalpose naudojami rezerviniai elektros maitinimo šaltiniai, užtikrinantys Informacinės sistemos pagrindinės kompiuterinės įrangos veikimą.

14. Atsarginės patalpos, į kurias būtų galima laikinai perkelti Informacinės sistemos įrangą, nesant galimybių tęsti veiklą pagrindinėse patalpose, turi tenkinti pagrindinėms patalpoms keliamus reikalavimus, numatytus Taisyklių 13.1–13.4 papunkčiuose.

15. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

15.1. Informacinė sistema turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones;

15.2. Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo vidiniame tinkle turi būti įdiegtos ir veikti automatizuotos įsibrovimo aptikimo sistemos, kurios stebėtų Informacinėje sistemoje įeinantį ir išeinantį duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų;

15.3. Per metus Informacinės sistemos prieinamumas yra ne mažiau kaip 90 procentų laiko darbo metu darbo dienomis.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

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

16.1. Informacinės sistemos duomenis įrašyti, keisti, atnaujinti ir naikinti gali tik Informacinės sistemos naudotojai pagal nustatytas prieigos teises;

16.2. Informacinės sistemos administravimo posistemyje naudotojų duomenis įvesti, keisti ir naikinti gali tik Informacinės sistemos administratorius;

16.3. Informacinės sistemos duomenys įvedami, atnaujinami, keičiami ir naikinami Informacinės sistemos nuostatuose nustatyta tvarka turint teisėtą pagrindą.

17. Informacinės sistemos naudotojų ir Informacinės sistemos administratoriaus atliekamų veiksmų auditui yra registruojama ši informacija:

17.1. Informacinės sistemos elementų įjungimas / išjungimas ar perkrovimas;

17.2. Informacinės sistemos naudotojų, administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti) / atsijungimas;

17.3. Audito funkcijos įjungimas / išjungimas;

17.4. audito įrašų trynimas, kūrimas ar keitimas.

18. Kiekviename audito duomenų įraše turi būti fiksuojama įvykio data, tikslus laikas, Informacinės sistemos naudotojo, Informacinės sistemos administratoriaus ir (arba) įrenginio, susijusio su įvykiu, duomenys; įvykio rezultatas.

19. Audito duomenų įrašai saugomi 30 dienų. Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas.

20. Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka:

20.1. Informacinės sistemos duomenų kopijos automatiniu būdu, esant aktyviai Informacinės sistemos duomenų bazei, daromos kiekvieną darbo dieną. Atsarginės Informacinės sistemos duomenų kopijos saugomos kitoje patalpoje nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota;

20.2. prarasti, iškraipyti ar sunaikinti Informacinės sistemos duomenys turi būti atkuriami iš Informacinės sistemos duomenų atsarginių kopijų. Už Informacinės sistemos duomenų atkūrimą iš atsarginių duomenų kopijų atsakingas Informacinės sistemos administratorius;

20.3. informacija apie elektroninės informacijos kopijavimą (kopijos įrašymo data ir laikas) automatiškai fiksuojama ir saugoma Informacinės sistemos tarnybinės stoties veiksmų žurnale.

21. Saugaus elektroninės informacijos perkėlimo ir teikimo susijusiems registrams ir informacinėms sistemoms, elektroninės informacijos gavimo iš jų tvarka:

21.1. duomenys iš susijusių registrų ir informacinių sistemų gaunami ir jiems teikiami šių registrų ir informacinių sistemų valdytojų / tvarkytojų ir Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo sudarytose duomenų teikimo ir gavimo sutartyse numatyta tvarka;

21.2. Informacinės sistemos duomenys kitai informacinei sistemai ir registrui perduodami laikantis Informacinės sistemos nuostatuose, Informacinės sistemos duomenų saugos nuostatuose ir kituose Informacinės sistemos saugos politiką įgyvendinančiuose dokumentuose nurodytų reikalavimų;

21.3. už duomenų, gaunamų iš susijusių registrų ir kitų informacinių sistemų, atnaujinimo procesą Informacinėje sistemoje yra atsakingas Informacinės sistemos administratorius.

22. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neteisėta veikla) nustatymo tvarka:

22.1. Informacinės sistemos naudotojai, pastebėję neteisėta veiklos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai Informacinės sistemos administratoriui;

22.2. Informacinės sistemos administratorius apie saugos pažeidimus informuoja Informacinės sistemos saugos įgaliotinį, imasi visų įmanomų veiksmų neteisėtai veiklai užkirsti bei išnagrinėja Informacinės sistemos duomenų bazės veiksmų žurnalo įrašus, siekdamas nustatyti neteisėtos veiklos šaltinį, laiką ir veiksmus;

22.3. Informacinės sistemos saugos įgaliotinis, gavęs pranešimą apie vykdomą neteisėtą veiklą, inicijuoja elektroninės informacijos saugos incidento valdymo veiksmus, kurie aprašyti Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos veiklos tęstinumo valdymo plane.

23. Informacinės sistemos programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

23.1. programinę ir techninę įrangą diegia ir tvarko Informacinės sistemos administratorius ir (ar) įstatymų nustatyta tvarka pasirinkti paslaugų teikėjai;

23.2. organizuojami Informacinės sistemos naudotojų darbo su nauja programine įranga mokymai;

23.3. naudojama tik sertifikuota programinė ir techninė įranga;

23.4. išvežant remontuoti sugedusią techninę įrangą, reikia imtis priemonių, užtikrinančių, kad su Informacinės sistemos elektronine informacija negalėtų susipažinti tam neįgalioti asmenys.

24. Informacinės sistemos funkcijų pokyčių (toliau – pokyčiai) valdymo tvarka:

24.1. Informacinės sistemos pokyčiai identifikuojami analizuojant vidinę ir išorinę Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo veiklos aplinką ir poreikius, kuriuos formuoja socialiniai, teisiniai, ekonominiai, technologiniai aspektai ir tendencijos, esama padėtis (Informacinės sistemos sąranka, pažeidžiamumai, atitiktis teisės aktų ir standartų reikalavimams ir panašiai);

24.2. Informacinės sistemos pokyčiai, atsižvelgiant į jų svarbą, aktualumą ir poreikį, skirstomi į kategorijas pagal pokyčio tipą (administracinis, organizacinis, funkcinis, programinis ir techninis). Tarpusavyje nesusiję Informacinės sistemos pokyčiai vienu metu neįgyvendinami. Pirmenybiniais laikomi Informacinės sistemos pokyčiai, susiję su duomenų apsauga ir Informacinės sistemos saugumu;

24.3. Informacinės sistemos pokyčius inicijuoti gali Informacinės sistemos duomenų valdymo įgaliotinis, Informacinės sistemos saugos įgaliotinis ar Informacinės sistemos administratorius, o įgyvendinti – Informacinės sistemos administratorius. Informacinės sistemos programinės ir techninės įrangos keitimo ir atnaujinimo tvarką ar Informacinės sistemos pokyčius, atsižvelgdamas į konkretų atvejį, derina Informacinės sistemos administratorius arba jie aprašomi paslaugų, susijusių su Informacinės sistemos programinės ir techninės įrangos keitimu ir atnaujinimu, teikimo sutartyse. Informacinės sistemos pokyčiai gali būti inicijuojami identifikavus Informacinės sistemos veikimo netikslumus, iškilus naujoms saugumo Informacinės sistemos grėsmėms ar siekiant gerinti Informacinės sistemos našumą;

24.4. prioritetas turi būti skiriamas pirmenybiniams ir plėtros (vystymo) Informacinės sistemos pokyčiams. Informacinės sistemos pokyčių prioritetas nustatomas pokyčių įtakos vertinimo metu;

24.5. funkcinių, programinių ir techninių pokyčių įtaką pagal kompetenciją vertina Informacinės sistemos tvarkytojas ir Informacinės sistemos valdytojas. Pokyčių įtakai įvertinti gali būti sudaroma darbo grupė, kurią gali sudaryti Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo kompetentingi darbuotojai, dirbantys pagal darbo sutartis, prireikus – nepriklausomi ekspertai;

24.6. Informacinės sistemos pokyčių įtakos vertinimo metu turi būti įvertinama Informacinės sistemos pokyčių nauda ir pagrįstumas, Informacinės sistemos pokyčių įgyvendinamumas ir alternatyvūs sprendimai, Informacinės sistemos pokyčiams atlikti reikalingos sąnaudos, taip pat Informacinės sistemos veiklos sutrikdymo ar sustabdymo rizika, Informacinės sistemos duomenų saugumo, elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo pažeidimo rizika;

24.7. numatomos Informacinės sistemos veiklos atkūrimo procedūros nesėkmingų Informacinės sistemos pokyčių atlikimo atvejais;

24.8. visi Informacinės sistemos pokyčiai, susiję su programinės ir (arba) techninės įrangos keitimu ir (arba) atnaujinimu, galintys sutrikdyti ar sustabdyti Informacinės sistemos darbą, įgyvendinami tik raštu suderinus su Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo vadovu ar Informacinės sistemos duomenų valdymo įgaliotiniu;

24.9. prieš atlikdamas Informacinės sistemos pokyčius, susijusius su programinės ir (arba) techninės įrangos keitimu ir (arba) atnaujinimu, kurių metu gali iškilti grėsmė Informacinės sistemos duomenų ir Informacinės sistemos konfidencialumui, vientisumui ar pasiekiamumui, Informacinės sistemos administratorius privalo planuojamus Informacinės sistemos pokyčius ištestuoti bandomojoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos Informacinės sistemos;

24.10. atlikęs vykdomų Informacinės sistemos pokyčių testavimą, konstatavęs keičiamos ir (arba) atnaujinamos Informacinės sistemos programinės ir (arba) techninės įrangos sėkmingą veikimą, Informacinės sistemos administratorius gali pradėti įgyvendinti Informacinės sistemos pokyčius;

24.11. planuodamas Informacinės sistemos pokyčius, kurių metu galimi Informacinės sistemos veikimo sutrikimai, Informacinės sistemos administratorius privalo ne vėliau kaip prieš vieną darbo dieną iki planuojamų pokyčių vykdymo pradžios informuoti Informacinės sistemos naudotojus (elektroniniu paštu arba telefonu) apie tokių darbų pradžią ir galimus sutrikimus;

24.12. Informacinės sistemos naudotojams privalo būti pateikta visa reikalinga informacija apie naudojimosi Informacine sistema pakitimus, susijusius su įvykdytais pokyčiais.

25. Mobiliųjų įrenginių naudojimo tvarka:

25.1. mobiliuosiuose įrenginiuose turi būti įdiegtos operacinės sistemos ir kiti naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

25.2. mobilieji įrenginiai turi būti atskirti nuo viešojo interneto tinklo užkarda;

25.3. mobiliuose įrenginiuose turi būti naudojamas slaptažodis, mobiliajame įrenginyje ar jo taikomoje programinėje įrangoje draudžiama išsaugoti slaptažodį;

25.4. baigus darbą ar pasitraukiant iš darbo vietos, Informacinės sistemos naudotojai privalo imtis priemonių, kad su Informacinės sistemos duomenimis negalėtų susipažinti pašaliniai asmenys (atsijungti nuo Informacinės sistemos, įjungti ekrano užsklandą su slaptažodžiu);

25.5. mobilieji įrenginiai, nedirbant su jais, turi būti saugomi saugioje vietoje;

25.6. turi būti užtikrinta kompiuterinių laikmenų apsauga.

IV SKYRIUS
REIKALAVIMAI PASLAUGOMS IR JŲ TEIKĖJAMS

26. Reikalavimai Informacinei sistemai funkcionuoti reikalingoms paslaugoms (projektavimo, aptarnavimo ir priežiūros) ir jų teikėjams nustatomi šių paslaugų teikimo sutartyse.

27. Informacinės sistemos valdytojas ir Informacinės sistemos tvarkytojas, pirkdamas paslaugas, darbus ar įrangą, susijusius su Informacine sistema, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi nustatyti, kad paslaugų teikėjas užtikrina atitiktį Kibernetinio saugumo reikalavimų apraše nustatytiems reikalavimams. Perkamos paslaugos, darbai ar įranga, susiję su Informacine sistema, turi atitikti teisės aktų ir standartų, kuriais vadovaujamasi užtikrinant Informacinės sistemos elektroninės informacijos saugą ir kibernetinį saugumą, reikalavimus, kurie iš anksto nustatomi paslaugų teikimo, darbų atlikimo ar įrangos tiekimo pirkimo dokumentuose.

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

28.1. paslaugų teikėjui prieiga prie Informacinės sistemos duomenų (peržiūrėti Informacinės sistemos duomenis, atlikti užklausas Informacinės sistemos, vykdyti veiksmus su Informacinės sistemos duomenimis ir kt.), fizinė prieiga prie Informacinės sistemos techninės ir programinės įrangos gali būti suteikiama tik pasirašius paslaugų teikimo sutartį, kurioje turi būti nustatytos paslaugų teikėjo teisės, pareigos, prieigos prie Informacinės sistemos lygiai ir sąlygos, elektroninės

informacijos saugos, kibernetinio saugumo, konfidencialumo reikalavimai, reikalavimai, keliami paslaugų teikėjų patalpoms, įrangai, Informacinės sistemos priežiūrai, duomenų perdavimui tinklais ir kitoms paslaugoms ir atsakomybė už jų nesilaikymą, reagavimas į paslaugos teikimo sutrikimus, elektroninės informacijos saugos ar kibernetinius incidentus;

28.2. Informacinės sistemos administratorius, suteikdamas prieigos prie Informacinės sistemos duomenų teisę, paslaugų teikėjo įgaliotą fizinį asmenį pasirašytinai supažindina su Informacinės sistemos nuostatais, Informacinės sistemos duomenų saugos nuostatais ir kitais Informacinės sistemos saugos politiką įgyvendinančiais dokumentais. Informacinės sistemos administratorius yra atsakingas už prieigos prie Informacinės sistemos paslaugų teikėjui suteikimą ar panaikinimą pasirašius sutartį, pasibaigus sutarties su paslaugų teikėju galiojimo terminui ar kitais sutartyje nurodytais prieigos prie Informacinės sistemos panaikinimo atvejais;

28.3. paslaugų teikėjui suteikiamas tik toks prieigos prie Informacinės sistemos duomenų lygis, kuris yra būtinas sutartyje nustatytiems įsipareigojimams vykdyti. Paslaugų teikėjo įgaliotam fiziniam asmeniui prieiga prie Informacinės sistemos duomenų suteikiama paslaugų teikimo sutartyje nurodytam laikotarpiui jo nustatytoms funkcijoms atlikti ir jis turi pasirašyti konfidencialumo pasižadėjimą;

28.4. pasibaigus paslaugų teikimo sutarties galiojimui ar šią sutartį nutraukus, Informacinės sistemos administratorius nedelsdamas, bet ne vėliau kaip kitą darbo dieną, panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie Informacinės sistemos duomenų teisę ir apie tai jį informuoja.

29. Paslaugos teikėjas, teikiantis Virtualių serverių nuomos paslaugą, atsakingas už Informacinės sistemos kompiuterinės įrangos saugos priemonių įgyvendinimą, tarnybinių stočių patalpų ir aplinkos saugumą, rezervinių duomenų kopijų darymą ir duomenų atkūrimą jų praradimo atveju.

_____

PATVIRTINTA
Higienos instituto direktoriaus
2023 m. gruodžio 5 d.
įsakymu Nr. V-156

TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos veiklos tęstinumo valdymo planas (toliau – Valdymo planas) reglamentuoja Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos (toliau – Informacinė sistema) veiklos tęstinumo užtikrinimą, siekiant tinkamai valdyti Informacinės sistemos elektroninės informacijos saugos ir kibernetinius incidentus (toliau – saugos incidentas).

2. Valdymo planas parengtas vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo“ (toliau – Bendrųjų reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu (toliau – Kibernetinio saugumo reikalavimų aprašas) ir Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintais Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nacionalinis kibernetinių incidentų valdymo planas).

3. Valdymo plane vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Bendrųjų reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše ir Nacionaliniame kibernetinių incidentų valdymo plane.

4. Valdymo planas taikomas įvykus saugos incidentui iki tol, kol bus atkurta Informacinės sistemos veikla. Plano vykdymą inicijuoja Informacinės sistemos veiklos tęstinumo valdymo grupės vadovas.

5. Valdymo planas privalomas Informacinės sistemos valdytojui ir Informacinės sistemos tvarkytojui, Informacinės sistemos saugos įgaliotiniui, Informacinės sistemos administratoriui, Informacinės sistemos naudotojams bei asmeniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą Higienos institute (toliau – HI) tvarkomuose registruose ir informacinėse sistemose (toliau – kibernetinio saugumo vadovas).

6. Informacinės sistemos veiklos tęstinumo valdymo grupės (toliau – Valdymo grupė), veiklos atkūrimo grupės (toliau – Atkūrimo grupė), Informacinės sistemos administratoriaus, Informacinės sistemos saugos įgaliotinio, kibernetinio saugumo vadovo įgaliojimai ir veiksmai įvykus saugos incidentui nurodyti Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos veiklos tęstinumo valdymo detaliajame plane (toliau – Detalusis planas) (1 priedas). Informacinės sistemos naudotojai privalo vykdyti kibernetinio saugumo vadovo, Valdymo grupės ir Atkūrimo grupės reikalavimus.

7. Saugos incidento metu patirti nuostoliai padengiami teisės aktų nustatyta tvarka iš Lietuvos Respublikos valstybės biudžeto ir kitų finansavimo šaltinių.

8. Informacinės sistemos veikla laikoma atkurta, jeigu atkurtas Informacinės sistemos prieinamumas (ne mažiau kaip 90 procentų darbo metu darbo dienomis) autorizuotiems Informacinės sistemos naudotojams ir yra užtikrintas Informacinės sistemos duomenų konfidencialumas ir vientisumas.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

9. Saugos incidentams valdyti ir veiklai atkurti sudarytos dvi grupės: Valdymo grupė ir Atkūrimo grupė.

10. Valdymo grupė užtikrina Informacinės sistemos veiklai kylančių grėsmių valdymą ir Informacinės sistemos atkūrimo koordinavimą įvykus saugos incidentui.

11. Valdymo grupės sudėtis:

11.1. HI Sveikatos informacijos centro (toliau – SIC) vadovas (toliau – Valdymo grupės vadovas);

11.2. HI kibernetinio saugumo vadovas (Valdymo grupės vadovo pavaduotojas);

11.3. HI duomenų apsaugos pareigūnas;

11.4. kiti Valdymo grupės nariai: Informacinės sistemos duomenų valdymo įgaliotinis, HI Bendrųjų reikalų skyriaus vadovas, HI SIC Sveikatos statistikos skyriaus specialistas.

12. Valdymo grupės funkcijos:

12.1. analizuoti Informacinės sistemos saugos incidentus;

12.2. priimti sprendimus Informacinės sistemos veiklos tęstinumo valdymo ir elektroninės informacijos fizinės saugos klausimais, įvykus elektroninės informacijos saugos incidentui;

12.3. bendrauti su viešosios informacijos rengėjų ir skleidėjų atstovais;

12.4. bendrauti su susijusių registrų ir informacinių sistemų veiklos tęstinumo valdymo grupėmis;

12.5. bendrauti ir bendradarbiauti su Informacinių technologijų paslaugų teikėju – Informacinės visuomenės plėtros komitetu (toliau – IVPK), Nacionaliniu kibernetinio saugumo centru (toliau – Centras), Valstybine duomenų apsaugos inspekcija (toliau – VDAI) ir teisėsaugos institucijomis vadovaujantis Kibernetinio saugumo įstatymo ir Kibernetinio saugumo reikalavimų aprašo nuostatomis;

12.6. kontroliuoti finansinių ir kitų išteklių, reikalingų Informacinės sistemos veiklai atkurti įvykus saugos incidentui, naudojimą;

12.7. organizuoti logistiką (darbuotojų, Informacinės sistemos techninės įrangos gabenimo organizavimas);

12.8. kontroliuoti ir koordinuoti Informacinės sistemos veiklos atkūrimą.

13. Atkūrimo grupė yra atskaitinga Valdymo grupei ir vykdo Informacinės sistemos veiklos atkūrimą ir veikimo užtikrinimą įvykus saugos incidentui.

14. Atkūrimo grupės sudėtis:

14.1. HI SIC Registrų skyriaus vadovas (toliau – Atkūrimo grupės vadovas);

14.2. Informacinės sistemos administratorius (Atkūrimo grupės vadovo pavaduotojas);

14.3. kiti Atkūrimo grupės nariai: Informacinės sistemos saugos įgaliotinis, HI SIC Registrų skyriaus specialistas.

15. Atkūrimo grupės funkcijos:

15.1. organizuoti Informacinės sistemos tarnybinių stočių veikimo atkūrimą;

15.2. organizuoti Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo kompiuterizuotų darbo vietų veikimo atkūrimą ir prijungimą prie kompiuterių tinklo;

15.3. organizuoti Informacinės sistemos elektroninės informacijos atkūrimą;

15.4. organizuoti Informacinės sistemos taikomųjų programų tinkamo veikimo atkūrimą;

15.5. vykdyti kitas Atkūrimo grupei pavestas funkcijas.

16. Kibernetinio saugumo vadovas atlieka šias funkcijas:

16.1. koordinuoja kibernetinių incidentų tyrimą, bendradarbiauja su kompetentingomis institucijomis, tiriančiomis kibernetinius incidentus;

16.2. atlieka kitas Informacinės sistemos saugos dokumentuose nurodytas ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, jam priskirtas funkcijas.

17. Esant paskelbtam saugos incidentui, Valdymo grupė ir Atkūrimo grupė organizuoja pasitarimus, atsižvelgdamos į pirmojo pasitarimo metu nustatytą jų dažnumą, palaiko ryšius visomis tuo metu prieinamomis ryšio priemonėmis (el. paštu, telefonu, mobiliuoju ryšiu ir kt.).

18. Reaguojant į saugos incidentus ir juos valdant, turi būti vadovaujamasi Detaliuoju planu ir šiais principais:

18.1. Informacinės sistemos veiklos atkūrimo principu – paskelbus saugos incidentą, jei būtina, organizuojama fizinė sauga ir nedelsiant pradedama atkurti Informacinės sistemos veikla. Pirmiausia atkuriamas Informacinės sistemos prieinamumas ir kritiškiausias funkcionalumas:

18.1.1. Informacinės sistemos administratorius ir, jei būtina, IVPK atstovas pagal kompetenciją atkuria Informacinės sistemos infrastruktūros ir taikomosios programinės įrangos funkcionavimą;

18.1.2. Informacinės sistemos administratorius ir, jei būtina, IVPK atstovas pagal kompetenciją iš atsarginių kopijų atkuria saugos incidento metu prarastus arba sugadintus Informacinės sistemos duomenis;

18.2. Informacinės sistemos naudotojų informavimo principu – Informacinės sistemos naudotojai turi būti informuoti apie Valdymo plane nustatytą atsakomybę įvykus Saugos incidentui.

19. Įvykus kibernetiniam incidentui, jo nustatymas, informavimas apie kibernetinį incidentą, kibernetinio incidento tyrimas ir kibernetinio incidento analizė, baigus kibernetinio incidento tyrimą, vykdomi Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka, o Valdymo plano nuostatos taikomos tiek, kiek kibernetinių incidentų valdymo nereglamentuoja Nacionalinis kibernetinių incidentų valdymo planas.

20. Įvykus saugos incidentui:

20.1. Informacinės sistemos naudotojai privalo nedelsdami žodžiu ar raštu pranešti Informacinės sistemos administratoriui apie įvykusį saugos incidentą. Patys Informacinės sistemos naudotojai neturi teisės imtis jokių veiksmų;

20.2. Informacinės sistemos administratorius, gavęs pranešimą apie saugos incidentą, nedelsdamas turi imtis veiksmų, reikalingų saugos incidentui stabdyti, ir, jei būtina, informuoti IVPK atstovą. Apie saugos incidentą Informacinės sistemos administratorius žodžiu arba raštu informuoja Informacinės sistemos saugos įgaliotinį ir HI kibernetinio saugumo vadovą, nurodydamas saugos incidento vietą, laiką, pobūdį ir kitą su įvykiu susijusią informaciją;

20.3. HI kibernetinio saugumo vadovas skiria prioritetą saugos incidento valdymui ir tyrimui bei apie jį informuoja Centrą Detaliajame plane nustatyta tvarka;

20.4. Informacinės sistemos saugos įgaliotinis apie saugos incidentą žodžiu arba raštu nedelsdamas informuoja Valdymo grupės vadovą, Atkūrimo grupės vadovą ir jei įtariami asmens duomenų apsaugos pažeidimai – HI duomenų apsaugos pareigūną;

20.5. Informacinės sistemos saugos įgaliotinis įrašo informaciją apie saugos incidentą į Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos elektroninės informacijos saugos ir kibernetinių incidentų registravimo žurnalą (2 priedas), vadovauja Detaliajame plane nurodytiems veiksmams;

20.6. Atkūrimo grupė atkuria Informacinės sistemos techninės ir programinės įrangos veikimą, kompiuterių tinklo veiklą, Informacinės sistemos elektroninę informaciją, Informacinės sistemos techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą. Atkūrimo grupės vadovas nedelsdamas apie atliktus veiksmus informuoja Valdymo grupės vadovą;

20.7. Valdymo grupė organizuoja žalos Informacinės sistemos elektroninei informacijai, Informacinės sistemos techninei, programinei įrangai vertinimą, koordinuoja Informacinės sistemos veiklai atkurti reikalingos techninės, sisteminės ir taikomosios programinės įrangos įsigijimą, parengia Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo vadovui tarnybinį pranešimą apie įvykusį saugos incidentą, atliktus veiksmus ir pasekmes.

21. Saugos incidento metu sunaikinta Informacinės sistemos techninė ir taikomoji programinė įranga keičiama turima rezervine įranga arba užsakomi papildomi reikalingi IT ištekliai ir paslaugos.

22. Turi būti užtikrintas Informacinės sistemos prieinamumas per metus ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis, neveikimo laikotarpis negali būti ilgesnis nei 16 val.

23. Vadovaujantis Informacinių technologijų paslaugų teikimo sutartimi, už atsarginių patalpų, naudojamų Informacinės sistemos veiklai atkurti įvykus elektroninės informacijos saugos incidentui, įrengimą atsakingas IVPK.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

24. Informacija apie Informacinės sistemos techninę ir programinę įrangą ir jos parametrus nurodyta Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos techninės ir programinės įrangos specifikacijoje.

25. Už Informacinės sistemos techninės ir programinės įrangos priežiūrą yra atsakingas Informacinės sistemos administratorius. Informacinės sistemos administratorių pavaduojančio asmens minimalus kompetencijos lygis negali būti žemesnis už Informacinės sistemos administratoriui keliamų reikalavimų, nustatytų jo pareigybės aprašyme, lygį.

26. Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo parengtų ir HI Bendrųjų reikalų skyriuje saugomų dokumentų sąrašas:

26.1. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos techninis aprašymas (specifikacija);

26.2. Informacinės sistemos programinės įrangos priežiūros sutarties kopija;

26.3. Informacinės sistemos techninės ir programinės įrangos sąrašai;

26.4. Informacinių technologijų paslaugų teikimo sutarties kopija;

26.5. dokumentas, kuriame pateikti kiekvieno pastato aukšto patalpų brėžiniai ir šiose patalpose esančios įrangos bei komunikacijų sąrašai, kompiuterių tinklo fizinio ir loginio sujungimo schemos.

27. Informacinių technologijų minimalaus funkcionalumo įrangos specifikacija turi būti analogiška pagrindinei Informacinės sistemos techninės ir programinės įrangos specifikacijai.

28. Informacinės sistemos saugos įgaliotinis parengia ir saugo Valdymo grupės ir Atkūrimo grupės narių sąrašą, kuriame nurodomi šių asmenų kontaktiniai duomenys, leidžiantys pasiekti šiuos asmenis bet kuriuo paros metu. Šie duomenys tvarkomi tik siekiant užtikrinti Saugos incidentų valdymą ir Informacinės sistemos veiklos tęstinumą, jeigu Valdymo grupės ar Atkūrimo grupės nario darbe nėra.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

29. Valdymo planas turi būti išbandomas esant esminiams Informacinės sistemos pokyčiams, bet ne rečiau kaip kartą per metus. Valdymo plano veiksmingumo išbandymo metu imituojamas saugos incidentas. Jo metu už saugos incidento padarinių likvidavimą atsakingi asmenys atlieka minėtų padarinių likvidavimo veiksmus.

30. Pagal bandymų rezultatus Informacinės sistemos saugos įgaliotinis, HI kibernetinio saugumo vadovas ir Informacinės sistemos administratorius parengia Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos veiklos tęstinumo valdymo plano veiksmingumo išbandymo ataskaitą (toliau – Ataskaita) (3 priedas), kurioje yra apibendrinami atliktų bandymų rezultatai, apibrėžiami pastebėti trūkumai ir pasiūlomos šių trūkumų šalinimo priemonės. Ataskaitą tvirtina Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo vadovas. Ataskaita ir susiję dokumentai ne vėliau kaip per penkias darbo dienas nuo jos priėmimo turi būti pateikti Centrui.

31. Informacinės sistemos saugos įgaliotinis nuolat kontroliuoja Ataskaitoje nurodytų prevencinių priemonių įgyvendinimą.

32. Veiklos tęstinumo valdymo plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami vadovaujantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

_____

Traumų ir nelaimingų atsitikimų
stebėsenos informacinės sistemos
veiklos tęstinumo valdymo plano
1 priedas

TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO DETALUSIS PLANAS

Incidentas	Veiklos tęstinumo valdymo (atkūrimo) veiksmai	Atsakingi vykdytojai	Incidento suvaldymo terminas
1. Oro sąlygos (klimatinių sąlygų poveikis informacinei sistemai)	1.1. Atitinkamos tarnybos informavimas apie pavojaus pobūdį.	Atkūrimo grupės vadovas IVPK atstovas	Nedelsiant
	1.2. Komunikacijų ar kitos techninės ir programinės įrangos, keliančių pavojų, išjungimas.	Informacinės sistemos administratorius IVPK atstovas	Nedelsiant
	1.3. Informacinės sistemos naudotojų informavimas.	Informacinės sistemos saugos įgaliotinis	per 2 val. nuo incidento nustatymo
	1.4. Incidento padarinių įvertinimas, priemonių plano padarytai žalai likviduoti sudarymas.	Valdymo grupės vadovas	per 4 val. nuo incidento nustatymo
	1.5. Priemonių plano incidento padarytai žalai likviduoti įgyvendinimas.	Atkūrimo grupės vadovas IVPK atstovas	Per 24 val. nuo padarytos žalos įvertinimo
2. Elektros energijos tiekimo sutrikimai	2.1. Energijos tiekimo sutrikimo priežasčių nustatymas.	Informacinės sistemos administratorius IVPK atstovas	Per 1 val. po incidento nustatymo
	2.2. Kreipimasis į energijos tiekimo tarnybą dėl sutrikimo trukmės ir pašalinimo galimybių.	Bendrųjų reikalų skyriaus vadovas IVPK atstovas	Nedelsiant
	2.3. Incidento padarinių įvertinimas, priemonių plano padarytai žalai likviduoti sudarymas.	Valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis	Per 2 val. nuo incidento nustatymo
	2.4. Priemonių plano incidento padarytai žalai likviduoti įgyvendinimas.	Atkūrimo grupės vadovas IVPK atstovas	Per 24 val. nuo žalos įvertinimo
3.Telekomunikacijų ir kitų ryšio tinklų sutrikimai	3.1. Telekomunikacijų ir kitų ryšio tinklų sutrikimų priežasčių nustatymas.	IVPK atstovas Informacinės sistemos administratorius	Per 1 val. nuo incidento nustatymo
	3.2. Kreipimasis į telekomunikacijų ir kitų ryšio tinklų paslaugų teikėją dėl sutrikimo trukmės ir pašalinimo	Bendrųjų reikalų skyriaus vadovas	Nedelsiant

	galimybių.		
	3.3. Incidento padarinių įvertinimas, priemonių plano padarytai žalai likviduoti sudarymas.	Valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis	Per 2 val. nuo incidento nustatymo
	3.4. Priemonių plano incidento padarytai žalai likviduoti įgyvendinimas.	Atkūrimo grupės vadovas IVPK atstovas	Per 24 val. nuo žalos įvertinimo
4. Programinės įrangos sugadinimas ar praradimas	4.1. Programinės įrangos sugadinimo priežasčių nustatymas.	Informacinės sistemos administratorius IVPK atstovas	Per 1val. nuo incidento nustatymo
	4.2. Sugadintos ar prarastos programinės įrangos atkūrimas ar naujos programinės įrangos įsigijimas arba reikiamų programinių išteklių duomenų centre užsakymas, kreipiantis į IT paslaugų teikėjus.	Atkūrimo grupės vadovas Informacinės sistemos administratorius IVPK atstovas	Prilauso nuo sutartyje nustatytų sąlygų
	4.3. Incidento padarinių įvertinimas, priemonių plano padarytai žalai likviduoti sudarymas.	Valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis	Per 2 val. nuo incidento nustatymo
	4.4. Priemonių plano incidento padarytai žalai likviduoti įgyvendinimas.	Atkūrimo grupės vadovas Informacinės sistemos administratorius IVPK atstovas	Per 24 val. nuo žalos įvertinimo
5. Duomenų pakeitimas, sunaikinimas, atskleidimas, dokumentų praradimas	5.1. Vertinama, ar yra pažeistas duomenų vientisumas, tikslumas, pasiekiamumas ir konfidencialumas, ir nustatoma, kokie konkrečiai duomenys yra pažeisti ar sugadinti. Jei incidentas susijęs su popierinių dokumentų praradimu, vertinamas prarastų dokumentų kiekis ir galimybės juos atgauti arba sunaikinti.	Informacinės sistemos administratorius Informacinės sistemos duomenų valdymo įgaliotinis Informacinės sistemos saugos įgaliotinis	Nedelsiant
	5.2. Atliekamas incidento vertinimas ir analizė, jei reikia, teikiamas pranešimas apie asmens duomenų saugumo pažeidimą VDAI ir (ar) pranešimas apie nusikalstamas veikas policijai.	Duomenų apsaugos pareigūnas Informacinės sistemos saugos įgaliotinis	Per 2 val. nuo incidento nustatymo
	5.3. Vertinamos pažeistų ar sugadintų duomenų atkūrimo ir koregavimo galimybės.	Informacinės sistemos administratorius Informacinės sistemos duomenų valdymo įgaliotinis	Per 2 val. nuo incidento nustatymo
	5.4. Imamasi priemonių neteisėtai atskleistų duomenų platinimui sustabdyti, prieigai prie atskleistų duomenų apriboti / panaikinti, diegiamos papildomos saugumo priemonės ir analizuojami žurnaliniai įrašai.	Informacinės sistemos administratorius IVPK atstovas	Nedelsiant
	5.5. Incidento padarinių įvertinimas, priemonių plano	Valdymo grupės vadovas	Per 24 val. nuo

	duomenų atkūrimui ir arba padarytai žalai likviduoti sudarymas.	Atkūrimo grupės vadovas Informacinės sistemos saugos įgaliotinis	incidento nustatymo
	5.6. Plano duomenų atkūrimo ir (arba) incidento padarytos žalos likvidavimo priemonių įgyvendinimas.	Atkūrimo grupės vadovas Informacinės sistemos administratorius IVPK atstovas	Per 24 val. nuo žalos įvertinimo
6. Įsilaužimas į vidinį kompiuterių tinklą	6.1. Įsilaužimo būdo nustatymas ir aptikto įsilaužimo sustabdymas ar užkardymas.	Informacinės sistemos administratorius IVPK atstovas	Nedelsiant
	6.2. Atliekamas incidento vertinimas ir analizė, jei reikia, teikiamas pranešimas apie kibernetinio saugumo incidentą Centrui ir (ar) pranešimas apie nusikalstamas veikas policijai.	Kibernetinio saugumo vadovas Informacinės sistemos saugos įgaliotinis Informacinės sistemos administratorius	Per 2 val. nuo incidento nustatymo
	6.3. Viso vidinio tinklo saugumo ir pažeidžiamumų patikra ir papildomų saugumo trūkumų analizė.	Atkūrimo grupės vadovas Informacinės sistemos administratorius	Per 2 val. nuo incidento nustatymo
	6.4. Incidento padarinių įvertinimas, priemonių plano nustatytiems saugumo trūkumams likviduoti sudarymas.	Valdymo grupės vadovas Informacinės sistemos saugos įgaliotinis	Per 2 val. nuo incidento nustatymo
	6.5. Priemonių plano incidento nustatytiems saugumo trūkumams likviduoti ar techninių ir programinių priemonių jų keliamai saugumo rizikai sumažinti įgyvendinimas.	Atkūrimo grupės vadovas Informacinės sistemos administratorius IVPK atstovas	Per 24 val. nuo žalos įvertinimo
7. Kibernetinis incidentas	7.1. Kibernetinio incidento įvertinimas ir priskyrimas poveikio kategorijai, priemonių pavojui sustabdyti ir padarytai žalai likviduoti sudarymas.	Kibernetinio saugumo vadovas Informacinės sistemos saugos įgaliotinis IVPK atstovas	Per 1val. nuo incidento nustatymo
	7.1.1. Kibernetinio incidento nustatymas (gavus informaciją iš kibernetinio saugumo priemonių, Registro naudotojų, Registro administratoriaus).	Kibernetinio saugumo vadovas Informacinės sistemos administratorius	Per 2 val. nuo incidento nustatymo
	7.1.2. Kibernetinio incidento įvertinimas, priskyrimas poveikio kategorijai ir užregistravimas.	Kibernetinio saugumo vadovas Informacinės sistemos saugos įgaliotinis	Nedelsiant
	7.1.3. Pranešimo parengimas Centrui apie: • didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per 1 val. nuo jų nustatymo; • vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per 4 val. nuo jų nustatymo; • nereikšmingo poveikio kibernetinius incidentus – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo	Kibernetinio saugumo vadovas Informacinės sistemos saugos įgaliotinis	Priklausomai nuo incidento poveikio kategorijos

	dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių. Pranešime nurodoma: • kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija; • trumpas kibernetinio incidento apibūdinimas; • tikslus laikas, kada kibernetinis incidentas įvyko ir buvo nustatytas; • kibernetinio incidento šalinimo tvarka (nurodant, ar tai prioritetas, ar ne); • tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita.		
	7.1.4. Informacijos apie kibernetinius saugumo incidentus, susijusius su asmens duomenų saugumo pažeidimais, ir taikytas šių saugos incidentų valdymo priemones pateikimas VDAI.	Informacinės sistemos saugos įgaliotinis Duomenų apsaugos pareigūnas	Per 2 val. nuo incidento nustatymo
	7.1.5. Informacijos, reikalingos kibernetiniams saugos incidentams, turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimas policijai.	Kibernetinio saugumo vadovas Informacinės sistemos saugos įgaliotinis	Per 2 val. nuo incidento nustatymo
	7.1.6. Kibernetinio incidento įrodymų surinkimas.	Informacinės sistemos administratorius Kibernetinio saugumo vadovas	Per 4 val. nuo incidento nustatymo
	7.1.7. Kibernetinio incidento pagal kompetenciją tyrimas.	Kibernetinio saugumo vadovas Informacinės sistemos saugos įgaliotinis	Per 24 val. nuo incidento nustatymo
	7.1.8. Priemonių, būtinų kibernetiniam incidentui suvaldyti ir Registro veiklai atkurti, pasirinkimas.	Atkūrimo grupės vadovas	Per 2 val. nuo incidento nustatymo
	7.2. Kibernetinio incidento pasekmes likviduojančių darbuotojų paskyrimas. Pasekmes likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas. Kibernetinio incidento pašalinimas.	Atkūrimo grupės vadovas	Per 4 val. nuo incidento nustatymo
	7.3. Parengimas kibernetinio incidento tyrimo ataskaitos, kurioje nurodoma: • kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija; • kibernetinio incidento veikimo trukmė;	Kibernetinio saugumo vadovas Informacinės sistemos saugos įgaliotinis Valdymo grupės vadovas	Per 2 val. nuo žalos įvertinimo

	• kibernetinio incidento šaltinis; • kibernetinio incidento požymiai; • kibernetinio incidento veikimo metodas; • galimos ir (ar) nustatytos kibernetinio incidento pasekmės; • kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas; • kibernetinio incidento būsena (aktyvus, pasyvus); • priemonės, kuriomis kibernetinis incidentas nustatytas; • galimos ir (ar) taikomos kibernetinio incidento valdymo priemonės.		
	7.4. Kibernetinio incidento tyrimo ataskaitos pateikimas Centrui: • apie didelio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per 4 val. nuo jų nustatymo ir ne rečiau kaip kas 4 val. atnaujintos informacijos teikimas, iki kibernetinis incidentas bus suvaldytas; • apie vidutinio poveikio kibernetinių incidentų valdymo būklę – ne vėliau kaip per 24 val. nuo jų nustatymo ir ne rečiau kaip kas 24 val. atnaujintos informacijos teikimas, iki kibernetinis incidentas bus suvaldytas ar pasibaigs.	Kibernetinio saugumo vadovas Informacinės sistemos saugos įgaliotinis	Priklausomai nuo incidento poveikio kategorijos
	7.5. Kreipimasis į Centrą, įvertinus, kad negalima savarankiškai ištirti ar suvaldyti kibernetinio incidento per maksimaliai leistiną Informacinės sistemos neveikimo laiką (ne vėliau kaip per 24 val. nuo šių aplinkybių nustatymo) ir jo nurodymų vykdymas.	Atkūrimo grupės vadovas	Nedelsiant
	7.6. Kibernetinio incidento sustabdymas ir pasekmių pašalinimas.	Atkūrimo grupės vadovas	Per 24 val. nuo incidento nustatymo
	7.7. Galutinės kibernetinio tyrimo ataskaitos parengimas (patikslinimas).	Kibernetinio saugumo vadovas Atkūrimo grupės vadovas	Per 4 val. nuo incidento sustabdymo
	7.8. Galutinės kibernetinio incidento tyrimo ataskaitos apie didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą / pasibaigimą pateikimas Centrui (ne vėliau	Kibernetinio saugumo vadovas Informacinės sistemos saugos įgaliotinis	Per 4 val. nuo incidento suvaldymo

	kaip per keturias valandas nuo jų suvaldymo ar pasibaigimo).		
	7.9. Organizacinių ir techninių kibernetinio saugumo priemonių, skirtų apsisaugoti nuo kibernetinių incidentų ar jų poveikiui sumažinti, nustatymas ir jų įgyvendinimo terminų nustatymas.	Valdymo grupės vadovas Kibernetinio saugumo vadovas IVPK atstovas	Priklausomai nuo incidento pobūdžio
8. Gaisras	8.1. Informuojama priešgaisrinės apsaugos ir gelbėjimo tarnyba ir vykdomi jos nurodymai	Bendrųjų reikalų skyriaus vadovas Veiklos valdymo grupės nariai	Nedelsiant
	8.2. Evakuojami Informacinės sistemos naudotojai (esant būtinumui ar priešgaisrinės apsaugos ir gelbėjimo tarnybos nurodymu)		
	8.3. Išjungiamos komunalinės komunikacijos, galinčios sukelti papildomą nenumatytą situaciją		
	8.4. Panaudojamos individualios gesinimo priemonės, jei tai nekelia pavojaus tai darantiems asmenims		
9. Darbuotojų praradimas	Trūkstamų darbuotojų paieška ir priėmimas į darbą.	Veiklos atkūrimo grupės vadovas	Nedelsiant pradėta darbuotojų paieška
* Apie kibernetinius incidentus Centras turi būti informuojamas užpildant pranešimo apie incidentą formą, esančią interneto svetainėje https://www.nksc.lt, arba išsiunčiant informaciją apie incidentą el. paštu cert@nksc.lt, arba skambinant telefonu 1843. ** Kibernetinių incidentų kategorijos nurodytos Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.			

_____

Traumų ir nelaimingų atsitikimų
stebėsenos informacinės sistemos
veiklos tęstinumo valdymo plano
2 priedas

(Informacinės sistemos elektroninės informacijos saugos incidentų registravimo žurnalo formos pavyzdys)

TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS ELEKTRONINĖS INFORMACIJOS SAUGOS IR KIBERNETINIŲ INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia 20__m. _____d.

Eil Nr.	Elektroninės informacijos saugos incidentas					
	Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo pavadinimas	Požymio kodas	Elektroninės informacijos saugos incidento aprašymas	Pradžia (metai, mėnuo, diena, valanda)	Pabaiga (metai, mėnuo, diena, valanda)	Saugos incidentą pašalino (vardas, pavardė)

Elektroninės informacijos saugos incidento požymiai:
1 – gaisras; 2 – elektros energijos tiekimo sutrikimai; 3 – įsilaužimas į vidinį kompiuterių tinklą; 4 – vandentiekio ir šildymo sistemos sutrikimai; 5 – kondicionavimo sistemos sutrikimas; 6 – ryšio sutrikimai; 7 – tarnybinių stočių vagystė arba sugadinimas; 8 – programinės įrangos sugadinimas ar praradimas; 9 – vagystė iš duomenų bazės ar jos fizinis sunaikinimas; 10 – nešiojamųjų kompiuterių ir juose saugomų duomenų praradimas; 11 – pavojingas (įtartinas) radinys; 12 – kompiuterių virusų, nepageidautinų laiškų (*spam*) atakos; 13 – dokumentų praradimas; 14 – duomenų iš duomenų teikėjų negavimas; 15 – dalinis Registro sutrikimas dėl neaiškių priežasčių; 16 – gamtos reiškiniai.

_____

Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos veiklos tęstinumo valdymo plano 3 priedas

(Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos veiklos tęstinumo valdymo eigos (plano išbandymo) ataskaitos forma)

TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO EIGOS (PLANO IŠBANDYMO) ATASKAITA

_____
(Veiklos tęstinumo valdymo grupės susitikimo data)

Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos elektroninės informacijos saugos incidento bandyme dalyvavo Veiklos tęstinumo valdymo grupės nariai:

1. _____
2. _____
3. _____

Elektroninės informacijos saugos ar kibernetinio incidento (toliau – saugos incidentas) scenarijus:

Informacinės sistemos funkcijos, kurias paveikė elektroninės informacijos saugos incidentas:

Saugos incidento valdymo eiga:

Rasti Informacinės sistemos veiklos tęstinumo valdymo plano trūkumai:

Pasiūlymai keisti arba papildyti veiklos tęstinumo valdymo planą:

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)

_____

PATVIRTINTA
Higienos instituto direktoriaus
2023 m. gruodžio 5 d.
įsakymu Nr. V-156

TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖS SISTEMOS NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos (toliau – Informacinė sistema) naudotojų administravimo taisyklių (toliau – Taisyklės) tikslas – reglamentuoti naudotojų prieigos prie Informacinės sistemos valdymą ir užtikrinti Informacinės sistemos elektroninės informacijos saugumą. Taisyklės yra taikomos visiems Informacinės sistemos naudotojams, Informacinės sistemos administratoriui ir Informacinės sistemos saugos įgaliotiniui.

2. Taisyklės parengtos vadovaujantis:

2.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

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

2.3. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

3. Prieigos prie Informacinės sistemos elektroninės informacijos suteikimo principai:

3.1. „būtina darbui“ – Informacinės sistemos naudotojams gali būti suteikta prieigos teisė tik prie tokios apimties duomenų, kokios reikia jo numatytoms funkcijoms atlikti;

3.2. „būtina žinoti“ – prieigos teisė prie duomenų gali būti suteikta tik atitinkamą leidimą dirbti ar susipažinti su šiais duomenimis turintiems asmenims.

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

4. Prieš tapdamas Informacinės sistemos naudotoju darbuotojas privalo susipažinti su, Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos duomenų saugos nuostatais, patvirtintais Higienos instituto direktoriaus 2023 m. spalio 25 d. įsakymu Nr. V-119 „Dėl Traumų ir nelaimingų atsitikimų stebėsenos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ (toliau – Informacinės sistemos duomenų saugos nuostatai) ir kitais saugos politiką įgyvendinančiais dokumentais (toliau visi kartu – saugos dokumentai) ir pasirašyti pasižadėjimą saugoti Informacinėje sistemoje tvarkomų asmens ir kitų duomenų paslaptį, laikytis duomenų saugos reikalavimų (priedas).

5. Informacinės sistemos naudotojai:

5.1. turi teisę tvarkyti Informacinės sistemos elektroninę informaciją tik atlikdami savo tiesiogines funkcijas;

5.2. turi teisę naudotis tik tomis funkcijomis (duomenų paieška, peržiūra, įvedimas, koregavimas, taisymas, keitimas ir kita) ir duomenimis, prie kurių prieigą jiems suteikė Informacinės sistemos administratorius;

5.3. privalo užtikrinti jų naudojamų Informacinėje sistemoje tvarkomų duomenų konfidencialumą ir vientisumą, savo veiksmais netrikdyti Informacinės sistemos duomenų prieinamumo;

5.4. turi teisę teikti siūlymus dėl papildomų elektroninės informacijos saugos priemonių taikymo;

5.5. privalo laikytis saugos dokumentuose nustatytų reikalavimų, pastebėję Informacinės sistemos sutrikimus, neįprastą jos veikimą, esamus arba galimus elektroninės informacijos saugumo reikalavimų pažeidimus, kitų naudotojų nederamus veiksmus, nedelsiant pranešti Informacinės sistemos administratoriui arba Informacinės sistemos saugos įgaliotiniui arba kibernetinio saugumo vadovui;

5.6. baigę darbą ar pasitraukdami iš darbo vietos turi imtis priemonių, kad su informacija, kuri tvarkoma Informacinėje sistemoje, negalėtų susipažinti pašaliniai asmenys: atsijungti nuo Informacinės sistemos, įjungti ekrano užsklandą su slaptažodžiu;

5.7. vykdyti kitas Informacinės sistemos naudotojų pareigas, nurodytas Informacinės sistemos saugos dokumentuose.

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

7. Informacinės sistemos administratorius vykdo Informacinės sistemos tarnybinių stočių, duomenų bazės ir Informacinės sistemos naudotojų administravimą. Jo įgaliojimai, teisės ir pareigos:

7.1. suteikti, apriboti ar panaikinti prieigą prie Informacinės sistemos naujiems naudotojams, keisti naudotojų teises;

7.2. užtikrinti, kad Informacinėje sistemoje nebūtų atliekami veiksmai, kurie gali sukelti bet kokio pobūdžio elektroninės informacijos saugos incidentą (neteisėtas Informacinės sistemos naudojimas, neteisėtas Informacinės sistemos elektroninės informacijos ir programinės įrangos kopijavimas ir kita);

7.3. atsakyti už atsarginių Informacinės sistemos elektroninės informacijos kopijų darymą ir elektroninės informacijos atkūrimą duomenų praradimo atveju;

7.4. pagal pasirinktus paieškos kriterijus atlikti užklausas Informacinėje sistemoje;

7.5. diegti naujas duomenų bazės valdymo sistemos versijas, prižiūrėti Informacinės sistemos duomenų bazę;

7.6. diegti tarnybinių stočių programinės įrangos atnaujinimus;

7.7. administruoti Informacinės sistemos tarnybines stotis ir Informacinės sistemos naudotojų kompiuterizuotas darbo vietas;

7.8. vykdyti kitas Informacinės sistemos administratoriaus pareigas, nurodytas Informacinės sistemos saugos dokumentuose.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO INFORMACINĖS SISTEMOS NAUDOTOJAMS KONTROLĖS TVARKA

8. Už Informacinės sistemos naudotojų registravimo ir išregistravimo Informacinėje sistemoje, prieigos prie Informacinės sistemos teisių suteikimo, pakeitimo ir panaikinimo bei unikalių prisijungimo prie Informacinės sistemos prisijungimo vardų ir pirminių prisijungimo slaptažodžių perdavimo Informacinės sistemos naudotojams tvarką atsakingas Informacinės sistemos administratorius.

9. Informacinės sistemos naudotojų įregistravimo tvarka:

9.1. Informacinės sistemos duomenų valdymo įgaliotinis Informacinės sistemos administratoriui el. paštu atsiunčia prašymą dėl naujo Informacinės sistemos naudotojo įregistravimo ir prieigos prie Informacinės sistemos suteikimo. Prašyme turi būti nurodyti Informacinės sistemos naudotojo duomenys ir naudotojo teisės darbui su Informacine sistema;

9.2. Informacinės sistemos administratorius, gavęs prašymą, užregistruoja naudotoją Informacinės sistemos naudotojų administravimo posistemėje, jam suteikia prisijungimo vardą, pirminį slaptažodį bei teises darbui su Informacine sistema. Užregistravus naują Informacinės sistemos naudotoją, jo prisijungimo duomenis administratorius išsiunčia Informacinės sistemos duomenų valdymo įgaliotiniui el. paštu;

9.3. Informacinės sistemos naudotojas, gavęs prisijungimo vardą ir pirminį slaptažodį, pirmą kartą jungdamasis prie Informacinės sistemos, privalo pasikeisti pirminį slaptažodį ir pakeistą slaptažodį įsiminti;

9.4. suteiktos teisės darbui Informacinėje sistemoje koreguojamos arba prieiga prie Informacinės sistemos sustabdoma pasikeitus Informacinės sistemos naudotojo darbo funkcijoms arba nutraukus darbo santykius. Informacinės sistemos naudotojai išregistruojami Informacinės sistemos duomenų valdymo įgaliotiniui el. paštu pateikus prašymą Informacinės sistemos administratoriui dėl Informacinės sistemos naudotojo išregistravimo.

10. Informacinės sistemos naudotojų tapatybei nustatyti turi būti suteikiamas unikalus prisijungimo prie Informacinės sistemos vardas ir slaptažodis (asmens kodas negali būti naudojamas Informacinės sistemos naudotojui atpažinti).

11. Gavęs suteiktą vardą ir slaptažodį ir pirmą kartą prisijungęs prie Informacinės sistemos duomenų bazės, Informacinės sistemos naudotojas nedelsdamas pirminį slaptažodį pakeičia nauju ir jį įsimena. Draudžiama slaptažodį atskleisti kitiems asmenims.

12. Reikalavimai Informacinės sistemos naudotojų ir Informacinės sistemos administratoriaus slaptažodžiams:

12.1. slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių;

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

12.3. slaptažodis negali būti saugomas ar perduodamas atviru tekstu ar užšifruojamas nepatikimu algoritmu. Kibernetinio saugumo vadovo sprendimu laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jeigu Informacinės sistemos naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių Informacinės sistemos naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu;

12.4. didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius – 5 kartai;

12.5. kilus įtarimui, kad slaptažodis galėjo būti atskleistas, slaptažodis turi būti nedelsiant pakeistas;

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

12.7. Informacinės sistemos naudotojui pamiršus slaptažodį, jis turi kreiptis į Informacinės sistemos administratorių arba į Informacinės sistemos valdytojo ir Informacinės sistemos tvarkytojo vadovo paskirtą atsakingą asmenį.

13. Papildomi reikalavimai Informacinės sistemos naudotojų slaptažodžiams:

13.1. pirmojo prisijungimo prie Informacinės sistemos metu iš Informacinės sistemos naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį;

13.2. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;

13.3. slaptažodis keičiamas kas 3 mėnesius;

13.4. keičiant slaptažodį informacinės sistemos taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių.

14. Papildomi reikalavimai Informacinės sistemos administratoriaus slaptažodžiui:

14.1. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

14.2 slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

14.3. keičiant slaptažodį informacinės sistemos taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių.

15. Informacinėje sistemoje vykdoma Informacinės sistemos naudotojų paskyrų kontrolė:

15.1. periodiškai tikrinama, ar Informacinės sistemos naudotojų paskyros atitinka kibernetinio saugumo reikalavimus, ir pranešama kibernetinio saugumo vadovui apie reikalavimų neatitinkančias Informacinės sistemos naudotojų paskyras;

15.2. nereikalingos ar nenaudojamos Informacinės naudotojų paskyros blokuojamos nedelsiant ir ištrinamos praėjus audito duomenų nustatytam saugojimo terminui.

16. Informacinėje sistemoje vykdoma Informacinės sistemos administratoriaus paskyrų kontrolė:

16.1. periodiškai tikrinama, ar Informacinės sistemos administratoriaus paskyra atitinka kibernetinio saugumo reikalavimus;

16.2. administratoriaus funkcijos atliekamos naudojant atskirą tam skirtą paskyrą, kuri nenaudojama kasdienėms Informacinės sistemos naudotojo funkcijoms atlikti;

16.3. nereikalinga ar nenaudojama Informacinės sistemos administratoriaus paskyra blokuojama nedelsiant ir ištrinama praėjus audito duomenų nustatytam saugojimo terminui.

17. Sąlygos ir atvejai, kada Informacinės sistemos administratoriaus arba Informacinės sistemos naudotojų teisės dirbti su Informacine sistema naikinamos nedelsiant:

17.1. kai Informacinės sistemos naudotojas nustoja vykdyti funkcijas, kurioms vykdyti buvo suteiktos teisės darbui su Informacine sistema;

17.2. kai įstatymų nustatytais atvejais Informacinės sistemos naudotojas ar administratorius nušalinamas nuo darbo (pareigų), pasibaigia jo darbo santykiai, praranda patikimumą;

17.3. nustačius elektroninės informacijos saugą ir tvarkymą reglamentuojančių teisės aktų nustatytų reikalavimų pažeidimą.

18. Draudžiama Informacinės sistemos techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti pagal saugos dokumentuose nustatytus reikalavimus.

19. Informacinės sistemos valdytojas ir Informacinės sistemos tvarkytojas turi parengti asmenų, kuriems suteiktos Informacinės sistemos administratoriaus teisės prisijungti prie Informacinės sistemos, sąrašą. Šis sąrašas periodiškai peržiūrimas kibernetinio saugumo vadovo. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais Informacinės sistemos administratorius nušalinamas nuo darbo (pareigų).

20. Nuotolinis Informacinės sistemos naudotojų prisijungimas prie Informacinės sistemos duomenų bazės leistinas per internetinę naudotojo sąsają, naudojant saugius duomenų perdavimo protokolus.

_____

Traumų ir nelaimingų atsitikimų stebėsenos
informacinės sistemos naudotojų
administravimo taisyklių
priedas

(Pasižadėjimo saugoti Traumų ir nelaimingų atsitikimų stebėsenos informacinėje sistemoje tvarkomų asmens ir kitų duomenų paslaptį, laikytis duomenų saugos reikalavimų forma)

PASIŽADĖJIMAS
SAUGOTI TRAUMŲ IR NELAIMINGŲ ATSITIKIMŲ STEBĖSENOS INFORMACINĖJE SISTEMOJE TVARKOMŲ ASMENS IR KITŲ DUOMENŲ PASLAPTĮ, LAIKYTIS DUOMENŲ SAUGOS REIKALAVIMŲ

_____ Nr. _____
(data) (registracijos numeris)

_____
(sudarymo vieta)

1. Aš suprantu, kad:

1.1. savo darbe susipažinsiu su konfidencialia informacija, kuri negali būti atskleista ar perduota neįgaliotiems asmenims ar institucijoms;

1.2. draudžiama perduoti neįgaliotiems asmenims slaptažodžius ir kitus duomenis, leidžiančius naudojantis programinėmis ar techninėmis priemonėmis sužinoti konfidencialią informaciją, arba kitaip sudaryti sąlygas susipažinti su tokia informacija;

1.3. informacijos skleidimu laikomas ne tik duomenų perdavimas, bet ir sąlygų sudarymas neįgaliotiems asmenims gauti informaciją;

1.4. netinkamas asmens duomenų tvarkymas gali užtraukti atsakomybę pagal 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – Reglamentas (ES) 2016/679), Lietuvos Respublikos įstatymus.

2. Man išaiškinta, kad konfidencialią informaciją pagal šį pasižadėjimą sudaro:

2.1. asmens duomenys, suprantami, kaip apibrėžta Reglamente (ES) 2016/679;

2.2. informacija, kurią darbo metu patikėta tvarkyti ar naudotis, išskyrus, kai tokią informaciją teikti įpareigoja teisės aktai ar kompetentingos institucijos;

2.3. žinios apie Informacinės sistemos kompiuterius, kompiuterinės įrangos sistemas, kompiuteriuose sukauptą informaciją, apsaugos ir signalizacijos informaciją.

3. Konfidencialia informacija nelaikoma tokia informacija, kuri:

3.1. jau yra žinoma informacijos gavėjui, jei dėl jos nėra sudaryta konfidencialumo susitarimų su informacijos teikėju bei nėra kitaip informacijos teikėjui ar kitiems asmenims prisiimta neatskleidimo įsipareigojimų;

3.2. tampa informacijos gavėjui prieinama nesant konfidencialumo įsipareigojimų iš šaltinio, kuris nėra informacijos teikėjas ar bet kurio iš jų atstovas ir kuris, informacijos gavėjo žiniomis, nėra susaistytas konfidencialumo sutartimi ar kitaip įsipareigojęs informacijos teikėjui ar bet kurio iš jų atstovams;

3.3. jau yra viešai prieinama ne dėl informacijos gavėjo neteisėto atskleidimo arba yra vieša pagal teisės aktus.

4. Aš įsipareigoju:

4.1. saugoti konfidencialią informaciją;

4.2. tvarkyti konfidencialią informaciją vadovaudamasis Reglamentu (ES) 2016/679, Lietuvos Respublikos įstatymais ir kitais teisės aktais;

4.3. neatskleisti, neperduoti ir nesudaryti sąlygų įvairiomis priemonėmis susipažinti su tvarkoma informacija nė vienam asmeniui, kuris nėra įgaliotas naudotis šia informacija tiek Registre, tiek už jo ribų;

4.4. pranešti savo tiesioginiam vadovui arba asmeniui, atsakingam už informacijos saugumą, apie bet kokius bandymus sužinoti man patikėtą konfidencialią informaciją ir apie bet kokią situaciją, kuri gali kelti grėsmę informacijos saugumui;

4.5. pasibaigus darbo santykiams ar pasikeitus pareigoms toliau saugoti darbo metu sužinotą konfidencialią informaciją.

5. Aš žinau, kad:

5.1. už konfidencialumo pasižadėjimo nesilaikymą, Reglamento (ES) 2016/679, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo pažeidimą turėsiu atsakyti pagal galiojančius teisės aktus;

5.2. asmuo, patyręs žalą dėl neteisėto konfidencialios informacijos tvarkymo ar kitų duomenų tvarkytojo neteisėtų veiksmų ar neveikimo, turi teisę reikalauti atlyginti jam padarytą turtinę ar neturtinę žalą;

5.3. institucija, atlyginusi žalą, patirtą nuostolį išsireikalauja įstatymų nustatyta tvarka iš informaciją tvarkančio darbuotojo, dėl kurio kaltės atsirado žala;

5.4. šis pasižadėjimas galios visą mano darbo laiką šioje įstaigoje, perėjus dirbti į kitas pareigas arba pasibaigus darbo ar sutartiniams santykiams.

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

_____
(data)

Šis pasižadėjimas buvo pasirašytas dalyvaujant:

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

_____
(data)

_____