PATVIRTINTA
VšĮ Visagino ligoninės
direktoriaus 2024 m. balandžio 24 d.
įsakymu Nr. 1- 57

VIEŠOSIOS ĮSTAIGOS VISAGINO LIGONINĖS KIBERNETINIO SAUGUMO POLITIKA

I. BENDROSIOS NUOSATOS

1. Kibernetinio saugumo politika (toliau – Politika) yra skirta pateikti vieningus ir veiksmingus Viešosios įstaigos Visagino ligoninės (toliau – Įstaiga), kibernetinio saugumo (toliau – Saugumo) valdymo principus, vadovybės poziciją kibernetinio saugumo atžvilgiu bei užtikrinti efektyvų Įstaigos kibernetinio saugumo valdymo proceso įgyvendinimą.
2. Ši Politika privaloma visiems Įstaigos darbuotojams, prekių ir (ar) paslaugų teikėjams ar kitiems asmenims, susijusiems su Įstaigos veikla, kur yra valdoma, perduodama ar kitaip tvarkoma informacija/ duomenys, valdomi procesai.

II. TEISINIS PAGRINDAS

1. Kibernetinio saugumo įstatymas – nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžia kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas, ypatingos svarbos informacinės infrastruktūros valdytojų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones. Informacinės saugos reikalavimai taikomi strateginę ar svarbią reikšmę saugumui turinčioms įstaigoms, nustato įrenginių informacinės saugos organizavimo principus, pagrindus ir pagrindinius informacinės saugos reikalavimus. Kibernetinio saugumo reikalavimai nustato organizacinius ir techninius kibernetinio saugumo reikalavimus ypatingos svarbos informacinės infrastruktūros valdytojams ir viešosioms įstaigoms.

III. SĄVOKOS

2. **Informacija** – bet koks žinių elementas, pateiktas tinkama naudoti, saugoti, perduoti ar apdoroti forma. Informacija apima žodine, rašytine, audiovizualine, skaitmenine ar bet kokia kita forma išreikštus ir apibendrintus arba interpretuotus duomenis.
3. **Informacijos saugumas** – informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas. Kai tai tikslinga, papildomai gali būti įtraukti ir kiti kriterijai, tokie kaip atsakingumas, apskaita, autentiškumas/patikimumas, nepaneigiamumas ir privatumas.
4. **Informacinė aplinka** – individai (naudotojai), organizacijos ir (ar) sistemos, kurios renka, apdoroja arba platina informaciją. Taip pat, ir pati informacija.
5. **Informacinė sistema** – informacijos apdorojimo sistemos ir organizacijos išteklių (pačios informacijos, žmonių, techninių priemonių, finansų ir pan.) visuma, skirta

informacijai apdoroti, formuoti (kurti), skleisti (siųsti ir gauti). Tai struktūrizuotas procesų ir procedūrų rinkinys, kuriame yra kaupiami duomenys, organizuojami ir perduodami vartotojui.

6. **Informaciniai ištekliai** – informacija (duomenų bazės, duomenų rinkmenos, sutartys ir kiti dokumentai, sisteminė ir projektinė dokumentacija, mokymų medžiaga, eksploatavimo ir priežiūros procedūros, tęstinumo ir atkūrimo planai); programinė įranga (taikomoji ir sisteminė programinė įranga, jos kūrimo priemonės); aparatinė įranga (duomenų laikmenos, organizacinė, kompiuterinė ir ryšių įranga); informacinių technologijų ir telekomunikacijų (toliau – ITT) funkcionavimui reikalingos paslaugos; išorės šalių teikiamos ITT paslaugos ir infrastruktūriniai ištekliai; darbuotojų kvalifikacija ir įgūdžiai.

7. **Išorės šalys** – paslaugų teikėjai, partneriai, pacientai, kiti asmenys, turintys ar galintys turėti prieigą prie Įstaigos informacinių išteklių.

8. **Kibernetinė aplinka** – informacinių ir sveikatos procesų valdymo sistemų naudotojai, tinklai, įrenginiai, programinė įranga, perduodama arba saugoma informacija, paslaugos ir sistemos, kurios gali būti pasiekiamos elektroniniais ryšių tinklais tiesiogiai arba netiesiogiai.

9. **Kibernetinis saugumas** – reiškia Įstaigos gebėjimą kibernetinėje erdvėje apsaugoti Įstaigos elektroninį ryšių tinklą, informacinės ir sveikatos procesų valdymo sistemas bei jas apginti kibernetinių atakų atveju. Tai visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, juos aptikti, analizuoti ir reaguoti į juos bei įprastinei elektroninių ryšių tinklų, informacinių ir sveikatos procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.

10. **Konfidencialumas** – informacijos savybė, užtikrinanti jos prieinamumą tik tiems fiziniams ar juridiniams asmenims (naudotojams), kuriems tokia teisė suteikta.

11. **Prieinamumas** – informacijos savybė, garantuojanti informacijos ir jos prieigai būtinų išteklių prieinamumą sankcionuotam naudotojui reikiamu metu.

12. **Vientisumas** – informacijos savybė, nusakanti jos tikslumą ir pilnumo apsaugą bei užtikrinanti, kad informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

13. Visi aukščiau minėti principai yra svarbūs analizuojant grėsmes ir formuojant šią Politiką.

IV. TIKSLAI

14. Saugi ir patikima kibernetinė Įstaigos aplinka, užtikrinanti aukštą elektroninių ryšių tinklų, informacinių ir sveikatos procesų valdymo sistemų bei informacijos saugumo lygį – tai strategiškai svarbi ir būtina sėkmingos Įstaigos veiklos ir jos tolimesnės plėtros bei Įstaigos turto ir reputacijos išsaugojimo sąlyga.

15. Pagrindiniai informacijos ir kibernetinio saugumo užtikrinimo tikslai:

15.1. Užtikrinti saugią ir patikimą kibernetinę Įstaigos aplinką, atsižvelgiant į Įstaigos veiklos tikslus ir neviršijant Vadovybės valdomos bei prisiimamos rizikos lygio;

15.2. Užtikrinti Įstaigos informacijos saugumą – t.y. Įstaigos informacijos konfidencialumą, vientisumą ir prieinamumą;

15.3. Užtikrinti Įstaigos veiklos tęstinumą – t.y. elektroninių ryšių tinklų, informacinių ir sveikatos procesų valdymo sistemų techninės bei programinės įrangos nepertraukiamą veiklą, incidentų valdymą ir savalaikį veiklos atstatymą;

15.4. Ieškoti naujų būdų ir priemonių, užtikrinančių saugumą, tačiau nemažinančių patogumo naudotojams ir sistemas eksploatuojančiam techniniam personalui;
15.5. Užtikrinti ir valdyti atitikimą, informacijos ir kibernetinį saugumą bei asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimams.

V. PRINCIPAI

16. Įstaigos kibernetinės aplinkos, informacinių ir sveikatos procesų valdymo sistemų saugumas yra užtikrinamas bei valdomas kuriant ir tobulinant vieningą saugumo sistemą, kurią sudaro teisinės, techninės, organizacinės bei švietimo (mokymo) priemonės, parenkamos siekiant valdyti riziką ir ją sumažinti iki Įstaigos vadovybei priimtino rizikos lygio.

17. Įstaigos vadovybė, siekdama užtikrinti kibernetinį saugumą, nustato šiuos kibernetinio saugumo valdymo principus:

17.1. Procesinis požiūris – Saugumą užtikrinanti veikla Įstaigoje turi būti organizuojama vadovaujantis procesiniu požiūriu. kibernetinio saugumo valdymo sistemos procesų rezultatai turi būti matuojami ir periodiškai vertinami, siekiant užtikrinti nepertraukiamą procesų tobulinimą ir prisitaikymą prie besikeičiančios sveikatos apsaugos sistemų aplinkos;
17.2. Darna – kibernetinę saugą stiprinti sistemingai užtikrinant tolygų saugumo gerinimą visose Įstaigos veiklos srityse, nuosekliai diegiant gerąsias kibernetinio saugumo praktikas (SANS/CIS CSC20) ir nuolat identifikuojant bei stiprinant silpniausias saugumo sistemos grandis;
17.3. Standartizavimas – kibernetinio saugumo procedūros turi būti aiškiai reglamentuotos ir visiems žinomos, valdomos pagal nustatytą vieningą standartizuotą procesą. Diegiant ir tobulinant Saugumo procesus turi būti siekiama vadovautis informacijos saugumo valdymo sistemos standarto (ISO 27001) reikalavimais;
17.4. Prioritetizavimas – užtikrinant Saugumą informacinėse sistemose, saugos priemonės vertinamos sekančiais aspektais, išdėstant juos prioriteto tvarka: konfidencialumas, vientisumas, prieinamumas. Saugumas sveikatos procesų valdymo sistemose įgyvendinamas prioritetus nustatant sekančiai - prieinamumas, vientisumas ir konfidencialumas;
17.5. Klasifikavimas („Būtina žinoti“) – visa Įstaigos informacija turi būti suskirstyta pagal konfidencialumo lygius; visa nevieša informacija aiškiai pažymėta, o jos prieiga Įstaigos personalui ir trečioms šalims suteikiama tiktai griežtai vadovaujantis principu „būtina žinoti“;
17.6. Adekvatumas (saugumas prieš patogumą) – apribojimai ir Saugumą užtikrinančios techninės bei organizacinės priemonės diegiamos prioritetu imant Saugumą, tačiau neviršijant rizikai iki Įstaigos vadovybei priimtino lygio sumažinti būtinos ribos, ir užtikrinant galimybę autorizuotam Įstaigos personalui ir išorės šalims naudotis Įstaigos skaitmeninėmis paslaugomis;
17.7. Racionalumas – diegiami nauji įrankiai ir kitos techninės bei organizacinės priemonės, užtikrinančios Saugumą bei apsaugą nuo kibernetinių grėsmių ir pažeidžiamumų, turi atitikti saugomos informacijos vertę. Jas diegiant, vadovaujantis Darnos principu, įvertinami bei panaudojami turimi Įstaigos ištekliai ir kompetencijos;
17.8. Operatyvumas – užtikrinamas nuolatinis informacinės ir kibernetinės aplinkos stebėjimas ir efektyvus reagavimas į kibernetinius incidentus bei informacijos ir kibernetinio saugumo incidentų (krizių) valdymas;

17.9. Prevencija – didesnis dėmesys turi būti skiriamas prevencijai, o ne reagavimui į incidentus ir jų pasekmes.

18. Siekdama įgyvendinti nustatytus kibernetinio saugumo valdymo principus, Įstaigos vadovybė įsipareigoja:

18.1. Skatinti ir propaguoti incidentų prevenciją užtikrinančias priemones bei visuotinės kibernetinės higienos (sąmoningumo) ir Saugumo kultūrą;

18.2. Skirti išteklius, būtinus nuolat planingai gerinti Saugumą užtikrinančio personalo kvalifikaciją bei įgūdžius;

18.3. Suteikti kompetencijas ir įgaliojimus vadovams derinti bei tvirtinti su priskirtu Saugumo valdymo procesu susijusius dokumentus.

VI. KONTROLĖ

19. Šios Politikos įgyvendinimo, kontrolės, organizavimo bei užtikrinimo veiksmai ir atsakomybės aprašomos šioje Politikoje ir kituose Įstaigos lokaliuose teisės aktuose, susijusiuose su kibernetiniu saugumu ir (ar) asmens duomenų apsauga.

20. Įstaigos Politikos atitikties teisės aktų reikalavimams vertinimui ir pasiūlymų dėl Politikos tobulinimo teikimui vyriausiasis gydytojas sudaro Saugumo komisiją, kurios uždaviniai, funkcijos ir darbo organizavimo principai apibrėžti Saugumo komisijos darbo reglamente.

21. Kibernetinio saugumo įgaliotinis ne rečiau kaip kartą per 2 (dvejus) metus turi inicijuoti vidaus patikrinimą, siekdamas nustatyti ar šį Politika yra tinkamai įgyvendinama praktikoje, ir parengti bei pateikti Saugumo komisijai pasiūlymus dėl šios Politikos pakeitimų poreikio.

VII. MINIMALŪS KIBERNETINIO SAUGUMO REIKALAVIMAI

22. Priklausomai nuo prieigos ir darbo su informacinėmis sistemomis, informacija bei duomenų tinklais ypatybėmis gali būti taikomi papildomi techniniai ir organizaciniai reikalavimai nurodyti kituose LR teisės aktuose.

23. Nuotolinio darbo saugumo reikalavimai. Įvertinus galimas rizikas ir suteikiant Išorės šaliai galimybę dirbti nuotolinėje kompiuterizuotoje darbo vietoje priklausančioje Išorės šaliai bei suteikiant nuotolinę prieigą prie Įstaigos informacinių sistemų Bendrajame duomenų tinkle būtina:

23.1. Drausti nuotolinę prieigą jei nenaudojamas saugus VPN ryšys;

23.2. Įsitikinti, kad informacinės sistemos, kompiuterinė įranga ir duomenų tinklai, iš kurių jungiamasi per nuotolį, yra saugūs ir patikimi (atnaujinta operacinė sistema ir kita programinė įranga, įdiegta antivirusinė programinės įranga, įjungta ir sukonfigūruota ugniasienė ir t.t.);

23.3. Užtikrinti savalaikę ir reguliarią prieigos teisių kontrolę;

23.4. Vykdyti nuolatinį veiksmų stebėjimą ir kontrolę;

23.5. Užtikrinti Įstaigos konfidencialios ir neviešinamos informacijos apsaugą techninėmis priemonėmis;

23.6. Užtikrinti, kad nuotolinio prisijungimo ryšys būtų kontroliuojamas su iš anksto tarpusavyje suderintais tikslais;

23.7. Nuotolinio ryšio sujungimas ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „Būtina darbui“ bei turėtų sutartą galiojimo terminą.

24. Saugumo reikalavimai personalui:

24.1. Įstaiga turi vykdyti savo darbuotojų kibernetinio saugumo sąmoningumo ugdymą suteikiant technines, procedūrines ir saugios veiklos žinias;
24.2. Kiekvienas Įstaigoje dirbantis asmuo privalo būti atsakingo Įstaigos darbuotojo supažindintas su Įstaigoje galiojančia kibernetinio saugumo politika.

25. Bendrieji kibernetinio saugumo reikalavimai:
25.1. Įstaiga turi užtikrinti, kad bet kokia nauja technologija, įdiegta Įstaigoje, yra sankcionuota ir yra gautas Įstaigos direktoriaus leidimas ją naudoti, taip pat užtikrinti, kad šios technologijos sauga yra pakankama;
25.2. Informacinių sistemų naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone;
25.3. Suteikiant laikinus slaptažodžius Informacinių sistemų naudotojams ir administratoriams, šie slaptažodžiai turi būti unikalūs kiekvienam ištekliaus naudotojui ir perduodami saugiu būdu;
25.4. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo naudotojo vardo, jeigu Informacinių sistemų naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių Informacinių sistemų naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroniniu ryšių tinklu;
25.5. Visose Informacinėse sistemose, prieš pradedant jas eksploatuoti, Informacinių sistemų administratoriai privalo pakeisti standartinius (gamintojų) slaptažodžius į šiuos reikalavimus atitinkančius slaptažodžius;
25.6. Informacinių sistemų dalys, patvirtinančios Informacinių sistemų naudotojo tapatumą, turi drausti automatiškai išsaugoti slaptažodžius;
25.7. Informacinių sistemų naudotojams negali būti suteikiamos Informacinių sistemų administratoriaus teisės;
25.8. Kiekvienas Informacinių sistemų naudotojas ar administratorius turi būti unikaliai atpažįstamas;
25.9. Informacinėse sistemose turi būti išjungiamos visos nereikalingos gamyklinės naudotojų paskyros (tame tarpe svečio paskyra);
25.10. Viešai prieinamose kompiuterizuotose darbo vietose paskutinio naudotojo vardas neturi būti matomas prisijungimo metu;
25.11. Prieiga turi būti suteikiama vadovaujantis principu „Būtina darbui“;
25.12. Nuotolinė prieiga prie Informacinių sistemų su administratoriaus paskyra turi būti draudžiama;
25.13. Prisijungdamas nuotoline prieiga prie Informacinių sistemų naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone. ;
25.14. Bet kokia nesankcionuota nuotolinė prieiga prie Įstaigos informacinių sistemų ir duomenų ar įrangos turi būti draudžiama;
25.15. Nuotolinė prieiga prie Įstaigos informacinių sistemų ir duomenų tinklo iš viešųjų duomenų tinklų turi būti šifruojama taikant VPN technologiją;
25.16. Technologiniame duomenų tinkle informacinių išteklių (tarnybinių stočių, komutatorių, maršrutizatorių, ugniasienių ir pan.) administravimui turi būti naudojama atskira techninė įranga neturinti el. pašto paskyros, prieigos prie viešųjų duomenų tinklų ar naudojama darbui su konfidencialia informacija.
25.17. Įmanoma gauti duomenis ar išrašą iš informacinės sistemos (informacinių sistemų) apie tai, kad konkretus asmuo gali naudotis asmens duomenimis, kokią dieną ir kokiu laiku galima naudotis asmens duomenimis ir kokios procedūros atliekamos asmens duomenų atžvilgiu (*pvz., kai darbuotojas pakeičia arba panaikina asmens duomenis)*.

25.18. Serveris (-iai) yra Įstaigos patalpose.

25.19. Įstaigos informacinės sistemos, kuriose laikomi asmens duomenys, numato galimybę pateikti asmens duomenis apie duomenų subjektą *(pvz., duomenų subjektui paprašius pateikti jo asmens duomenų kopiją)*.

25.20. Įstaiga naudoja saugumo priemones asmens duomenims apsaugoti: VPN ryšys nuotolinei prieigai; Asmens duomenų saugojimas ar siuntimas šifruota forma; Saugus spausdintų dokumentų laikymas *(pvz., seifai, rakinamos spintelės, archyvo patalpos ir pan.)*; Saugus spausdintų dokumentų naikinimas *(pvz., specialios šiukšliadėžės seniems spausdintiems dokumentams, dokumentų naikiklių naudojimas ir pan.)*.

25.21. Įstaiga atlieka bandymus, siekdama aptikti asmens duomenų tvarkymo klaidas ar nustatyti pažeidimus *(pvz., ar darbuotojai gali naudotis tik asmens duomenimis, kuriais jiems leista naudotis, ir ar asmens duomenys, kurie turi būti ištrinami, iš tiesų yra ištrinami iš visų saugojimo vietų)*.

VIII. KIBERNETINIŲ INCIDENTŲ KATEGORIJOS, INFORMAVIMAS APIE KIBERNETINIUS INCIDENTUS IR KIBERNETINIŲ INCIDENTŲ TYRIMAS

26. Kibernetiniai incidentai skirstomi į keturias kategorijas:

26.1. Pavojingi kibernetiniai incidentai;

26.2. Didelio poveikio kibernetiniai incidentai;

26.3. Vidutinio poveikio kibernetiniai incidentai;

26.4. Nereikšmingo poveikio kibernetiniai incidentai.

27. Kriterijai, kuriais vadovaujantis Įstaigos kibernetiniai incidentai priskiriami Politikos 30 punkte nustatytoms kategorijoms, nustatyti Politikos priede.

28. Kibernetinius incidentus Politikos 29.2–30.4 papunkčiuose nustatytoms kategorijoms, atsižvelgdami į Politikos priede nustatytus kriterijus, priskiria Įstaigos, kurios ryšių ir informacinėse sistemose nustatyti kibernetiniai incidentai. Jeigu nustatytas kibernetinis incidentas ir (ar) jo poveikis atitinka bent vieną iš kriterijų, nurodytų Politikos priede, būdingų Politikos 29.1 papunktyje nustatytai pavojingo kibernetinio incidento kategorijai, Įstaiga kibernetinį incidentą priskiria 30.2 papunktyje nustatytai didelio poveikio kibernetinio incidento kategorijai.

29. Kibernetinius incidentus Politikos 30.1 papunktyje nustatytai pavojingo kibernetinio incidento kategorijai turi teisę priskirti tik Nacionalinis kibernetinio saugumo centras.

30. Įstaiga Nacionalinį kibernetinio saugumo centrą informuoja apie:

30.1. Didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per vieną valandą nuo jų nustatymo;

30.2. Vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per keturias valandas nuo jų nustatymo;

30.3. Nereikšmingo poveikio kibernetinius incidentus – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną teikiant apibendrintą informaciją apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo teikimo dienos, skaičių.

31. Nacionalinis kibernetinio saugumo centras informuojamas apie didelio ar vidutinio poveikio kibernetinius incidentus Įstaigos pranešimu, kuriame nurodoma:

31.1. Kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Politikos priede pateiktus kriterijus;

31.2. Trumpas kibernetinio incidento apibūdinimas;

31.3. Tikslus laikas, kada kibernetinis incidentas įvyko ir buvo nustatytas;

31.4. Kibernetinio incidento šalinimo tvarka (nurodant, ar tai prioritetas, ar ne);

31.5. Tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita.

32. Įstaiga imasi visų įmanomų priemonių, būtinų kibernetiniam incidentui suvaldyti ir įprastai ryšių ir informacinių sistemų veiklai atkurti.

33. Įstaiga tyrimo išvadoje turi aprašyti žinoma informaciją:

33.1. Kibernetinio incidento grupė (grupės), pogrupis (pogrupiai) ir poveikio kategorija, nustatyta pagal Politikos priede pateiktus kriterijus;

33.2. Ryšių ir informacinės sistemos, kurioje nustatytas kibernetinis incidentas, tipas (elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema, tarnybinė stotis ir panašiai);

33.3. Kibernetinio incidento veikimo trukmė;

33.4. Kibernetinio incidento šaltinis;

33.5. Kibernetinio incidento požymiai;

33.6. kibernetinio incidento veikimo metodas;

33.7. Galimos ir (ar) nustatytos kibernetinio incidento pasekmės;

33.8. Kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas;

33.9. Kibernetinio incidento būsena (aktyvus, pasyvus);

33.10. Priemonės, kuriomis kibernetinis incidentas nustatytas;

33.11. Galimos ir (ar) taikomos kibernetinio incidento valdymo priemonės.

34. Įstaiga, įvertinusi, kad negalės savarankiškai ištirti ar suvaldyti kibernetinio incidento per protingą terminą, ne vėliau kaip per dvidešimt keturias valandas nuo šių aplinkybių nustatymo kreipiasi pagalbos į Nacionalinį kibernetinio saugumo centrą.

35. Įstaiga po kibernetinio incidento suvaldymo ar pasibaigimo pagal kompetenciją atlieka jo analizę. Dėl kibernetinių incidentų, priskirtų nereikšmingo kibernetinio incidento kategorijai, kibernetinio incidento analizė neatliekama.

36. Įstaiga, kurios ryšių ir informacinėje sistemoje tirtas kibernetinis incidentas, išanalizavusi ir įvertinusi visą informaciją, susijusią su kibernetiniu incidentu, atliktus veiksmus ir panaudotas priemones:

IX. BAIGIAMOSIOS NUOSTATOS

37. Šios Politikos įgyvendinimo, kontrolės, organizavimo bei užtikrinimo veiksmai ir atsakomybės aprašomos šioje Politikoje ir kituose Įstaigos lokaliuose teisės aktuose, susijusiuose su kibernetiniu saugumu ir (ar) asmens duomenų apsauga.

38. Įstaigos Politikos atitikties teisės aktų reikalavimams vertinimui ir pasiūlymų dėl Politikos tobulinimo teikimui Įstaigos direktorius sudaro Saugumo komisiją, kurios uždaviniai, funkcijos ir darbo organizavimo principai apibrėžti Saugumo komisijos darbo reglamente.

39. Kibernetinio saugumo įgaliotinis ne rečiau kaip kartą per 2 (dvejus) metus turi inicijuoti vidaus patikrinimą, siekdamas nustatyti ar šį Politika yra tinkamai įgyvendinama praktikoje, ir parengti bei pateikti Saugumo komisijai pasiūlymus dėl šios Politikos pakeitimų poreikio.

_____

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

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) virsijamas maksimalus leistinas paslaugos	Paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
1.	Nepageidaujamų laiškų, klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content*, *spam*)	1.1. Nepageidaujami laiškai ir (ar) klaidinančios, žeidžiančios informacijos platinimas trikdo ryšių ir informacinės sistemos (toliau – RIS) veiklą ir (ar) teikiamas paslaugas	N				V					D					P		
		1.2. Nepageidaujamų laiškų ir (ar) klaidinančios, žeidžiančios informacijos platinimas	N																
2.	Kenkimo	2.1. Aptikta moderni kenkimo					V					D					P		

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
	programinė įranga (angl. *malicious software / code*) Programinė įranga ar jos dalis, kuri padeda neteisėtai prisijungti prie RIS, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jų veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją,	programinė įranga (angl. *advanced persistent threat, APT*)																	
		2.2. RIS aktyviai kontroliuojama įsibrovėlių (pavyzdžiui, „galinės durys“ (angl. *back door*), kompiuterizuotos darbo vietos ar tarnybinės stotys tampa „Botinklo“ (angl. *Botnet*) infrastruktūros dalimi					V					D					P		
		2.3. Kenkimo programinė įranga, trikdanti saugumo priemonių darbą					V					D					P		
		2.4. Kenkimo programinė	N				V												

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) visiškas maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
	panaikinti ar apriboti galimybę ja naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims	įranga, kurią aptinka saugumo priemonės per reguliarų patikrinimą ir (ar) kurią saugumo priemonės automatiškai blokuoja																	
		2.5. Kenkimo programinė įranga, platinama naudojant socialinės inžinerijos metodus	N				V					D					P		
3.	Informacijos rinkimas (angl.	3.1. RIS paketų / informacijos perėmimas					V					D					P		

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
	information gathering) Žvalgyba ar kita įtartina veikla (angl. *scanning, sniffing*), manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. *social*	3.2. RIS klastojimas, siekiant surinkti prisijungimo ar kitą svarbią informaciją, tiksliniai laiškai, kuriuose, pasinaudojant socialinės inžinerijos principais, siekiama išvilioti prisijungimo ir (ar) kitą svarbią informaciją, priversti atlikti norimus veiksmus (pvz., finansines operacijas)					V					D					P		
		3.3. Vykdoma perimetro priemonių žvalgyba (nebandant įsilaužti)	N				V												
		3.4. Naudojami socialinės	N				V												

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
	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	inžinerijos metodai, siekiant išvilioti prisijungimo prie RIS ir (ar) kitą svarbią informaciją																	
4.	Mėginimas įsilaužti	4.1. Išnaudojamas vienas ar					V					D					P		

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) visiškas maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
	(angl. *intrusion attempts*) Mėginimas įsilaužti arba sutrikdyti RIS veikimą išnaudojant žinomus pažeidžiamumus (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą	keli nežinomi (angl. *zero day*) pažeidžiamumai, siekiant tikslingai sutrikdyti konkrečią RIS																	
		4.2. Išnaudojamas vienas ar keli nežinomi (angl. *zero day*) pažeidžiamumai	N				V					D					P		
		4.3. Vidinė RIS žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita)					V					D					P		
		4.4. Išnaudojami žinomi ir viešai publikuoti	N				V												

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) visiškai maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
	įsilaužimo būdą (angl. *new attack signature*)	pažeidžiamumai arba atliekami bandymai prisijungti prie RIS parenkant slaptažodžius																	
5.	Įsilaužimas (angl. *intrusions*) Sėkmingas įsilaužimas ir (ar) neteisėtas RIS, taikomosios programinės įrangos ar paslaugos naudojimas (angl. *privileged account*	5.1. Veiksmai prieš RIS ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, RIS ar jos dalies pažeidimas, sutrikdantis RIS teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti RIS					V					D					P		

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
	compromise, unprivileged account compromise, application compromise)	naudotojų pasitikėjimą jais																	
		5.2. Gaunama neteisėta prieiga prie RIS, taikomosios programinės įrangos ar paslaugos					V					D					P		
6.	Paslaugų trikdymas, prieinamumo pažeidimai (angl. *availability*) Veiksmai, kuriais trikdoma RIS veikla, teikiamos paslaugos (angl.	6.1. Teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas					V					D					P		
		6.2. Teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų	N				V												

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
	DoS, DDoS), RIS ar jos dalies pažeidimas, sutrikdantis RIS ir (ar) jos teikiamas paslaugas (angl. *sabotage, outage*)	prieinamumui																	
		6.3. Aptinkamas paslaugos trikdymas, kuris neturi įtakos paslaugų teikimui	N				V												
7.	Informacijos turinio saugumo pažeidimai (angl. *information content security*) Neteisėta prieiga prie informacijos, neteisėtas	7.1. Neteisėta prieiga prie informacijos, galinčios turėti įtakos RIS veiklai ir (ar) teikiamoms paslaugoms					V					D					P		
		7.2. Neteisėta prieiga prie informacijos, neteisėtas informacijos keitimas	N				V					D					P		

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) visiškai maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
	informacijos keitimas (angl. *unauthorised access to information, unauthorised modification of information*)																		

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) virsijamas maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
8.	Neteisėta veikla, sukčiavimas (angl. *fraud*) Vagystė, apgavystė, neteisėtas išteklių (angl. *unauthorized use of resources*), nelegalios programinės įrangos ar autorių teisių (angl. *copyright*) naudojimas, tapatybės	8.1. Neteisėta įtaka RIS veiklai ir (ar) teikiamoms paslaugoms	N				V					D					P		

Eil. Nr.	Kibernetinio incidento grupės	Kibernetinio incidento poveikis / Kibernetinio incidento pogrupiai	Nereikšmingas (N) (bent vienas iš kriterijų)				Vidutinis (V) (du ar daugiau kriterijų)					Didelis (D) (du ar daugiau kriterijų)					Pavojingas (P) (bent vienas iš kriterijų)		
			RIS trikdoma < 1 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga teikiama, bet trikdoma	Nuostoliai < 250 000 Eur	RIS trikdoma ≥ 1 val., bet < 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius <	Paslauga trikdoma dalyje šalies teritorijos	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 250 000, bet < 500 000 Eur	RIS trikdoma ≥ 2 val.	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	Paslauga trikdoma visos šalies teritorijoje ir (ar) ≥ 1 ES šalyje	Pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas	Nuostoliai ≥ 500 000 Eur	RIS trikdoma ≥ 24 val. ir (ar) viršijamas maksimalus leistinas paslaugos	Paveikių paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥	prisiimtų įsipareigojimų vykdymas, sukeliamas (gali kilti) ekstremalus
	klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai																		
9.	Kita Incidentai, kurie neatitinka nė vienos iš nurodytų grupių aprašymų		N				V					D					P		