PATVIRTINTA
VšĮ Raseinių psichikos sveikatos centro
direktoriaus 2021 m. gruodžio 27 d.
įsakymu Nr. V-39

VIEŠOSIOS ĮSTAIGOS RASEINIŲ PSICHIKOS SVEIKATOS CENTRO INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. BENDROSIOS NUOSTATOS

1. VšĮ Raseinių psichikos sveikatos centro (toliau – Įstaiga) valdomų ir tvarkomų informacinių sistemų (toliau - Informacinė sistema arba IS) veiklos tęstinumo valdymo planas (toliau – Valdymo planas) yra vykdomas įvykus elektroninės informacijos saugos incidentui, kibernetiniam incidentui kuris gali sudaryti neteisėto prisijungimo prie Informacinės sistemos galimybę, sutrikdyti Informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija.

2. Valdymo plano tikslas – nustatyti Informacijos saugos įgaliotinio, Informacinės sistemos administratoriaus, naudotojų ir kitų asmenų veiksmus, įvykus elektroninės informacijos saugos incidentui ar kibernetiniam incidentui.

3. Valdymo planas parengtas vadovaujantis teisės aktais apibrėžtais VšĮ Raseinių psichikos sveikatos centro informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių 2 punkte.

4. Valdymo planas parengtas Įstaigos patalpoms, esančioms Ligoninės g. 6, Raseiniuose, kuriose yra pagrindinė IS informacinių technologijų infrastruktūra, reikalinga IS veiklai.

5. Valdymo plane vartojamos sąvokos:

5.1. Elektroninės informacijos saugos incidentas – įvykis ar veiksmas, kurie gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti

5.2. Kitos Valdymo plane naudojamos sąvokos atitinka VšĮ Raseinių psichikos sveikatos centro informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse apibrėžtas sąvokas ir Valdymo plane 3 punkte nurodytuose teisės aktuose ir kituose saugos politiką reglamentuojančiuose teisės aktuose nustatytas sąvokas.

6. Valdymo planas įsigalioja jei pastebimas Elektroninės informacijos saugos incidentas, dėl kurio Įstaiga negali teikti elektroninių paslaugų daliai arba visiems naudotojams ir būtina atkurti įprastą IS veiklą. Plano nuostatos taip pat taikomos po stichinės nelaimės, avarijos ar kitų ekstremalių situacijų, kai būtina atkurti įprastą IS veiklą.

7. Įvykus kibernetiniam incidentui vadovaujamasi Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nutarimas), atsakingas - Informacijos saugos įgaliotinis.

8. Identifikavus kibernetinį incidentą, atliekamas incidento vertinimas pagal poveikį ir incidento priskyrimas vienai iš šių kategorijų: didelio, vidutinio ar nereikšmingo. Kriterijai, pagal kuriuos incidentas priskiriamas tam tikrai kategorijai, yra nurodyti Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Nutarimu.

9. Atsakingų asmenų įgaliojimai įvykus kibernetiniam ar Elektroninės informacijos saugos incidentui:

9.1. Informacijos saugos įgaliotiniai turi:

9.1.1. bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, kibernetinius ir (ar) elektroninės informacijos saugos incidentus, neteisėtas veikas, susijusias su

kibernetiniais ir (ar) elektroninės informacijos saugos incidentais Įmonės komponentuose,

9.1.2. koordinuoti kibernetinių ir Elektroninės informacijos saugos incidentų tyrimą.

9.2. Informacinės sistemos administratorius turi dalyvauti atliekant Veiklos atkūrimo grupės nurodytas funkcijas;

9.3. Naudotojai vykdo Veiklos tęstinumo valdymo grupės nurodymus.

10. Informacijos saugos įgaliotinis, atsakingas už kibernetinių incidentų tyrimą ir pranešimą apie kibernetinius incidentus kompetentingoms institucijoms: Nacionaliniam kibernetinio saugumo centrui, Lietuvos policijai.

11. Nustačius, kad kibernetinis incidentas sukėlė asmens duomenų pažeidimą ir, kad yra rizika fizinių asmenų teisėms ir laisvėms, duomenų apsaugos pareigūnas nedelsdamas ir, jei įmanoma, praėjus ne daugiau kaip per 72 valandoms nuo tada, kai buvo sužinota apie pažeidimą, turėtų pranešti apie tai Valstybinei duomenų apsaugos inspekcijai (detali pranešimo tvarką apibrėžta dokumente „VšĮ Raseinių psichikos sveikatos centro asmens duomenų saugumo pažeidimų nustatymo, sustabdymo ir pranešimi apie juos tvarka“).

12. Būdai, kuriais pranešama apie kibernetinį incidentą kompetentingoms institucijoms:

12.1. Nacionaliniam kibernetinio saugumo centrui pranešama užpildant specialią formą interneto svetainėje www.nksc.lt, rašant el. paštu cert@nksc.lt arba skambinant trumpuoju numeriu 1843;

12.2. Lietuvos policijai, užpildant specialią formą interneto svetainėje www.epolicija.lt arba skambinant numeriu 870060000.

13. Informacijos saugos incidento ar kibernetinio incidento metu patirti nuostoliai padengiami ir Informacinės sistemos veikla atkuriama Įmonės lėšomis.

14. Informacinės sistemos veikla laikoma atkurta, jeigu tenkinami šie kriterijai:

14.1. veikia visi Informacinės sistemos komponentai;

14.2. galimas Informacinės sistemos elektroninės informacijos atnaujinimas;

14.3. galimas Informacinės sistemos elektroninės informacijos išsaugojimas;

14.4. užtikrintas IS elektroninės informacijos vientisumas ir konfidencialumas;

14.5. galimas Informacinės sistemos prieinamumas visų autorizuotų informacinės sistemos naudotojų atžvilgiu.

II. ORGANIZACINĖS NUOSTATOS

15. Veiklos tęstinumui užtikrinti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui sudaromos Veiklos tęstinumo valdymo grupė ir Veiklos atkūrimo grupė. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės vadovai turi teisę į šių grupių veiklą pasitelkti kitus darbuotojus ar trečiosios šalies kompetentingus specialistus, jeigu tai būtina veiklai atkurti ir veiklos tęstinumui užtikrinti.

16. Veiklos tęstinumo valdymo grupės sudėtis:

16.1. Veiklos tęstinumo valdymo grupės vadovas: Įstaigos direktorius;

16.2. Veiklos tęstinumo valdymo grupės vadovo pavaduotojas: vyriausioji psichikos sveikatos slaugytoja;

16.3. Veiklos tęstinumo valdymo grupės nariai: duomenų apsaugos pareigūnas, IT specialistas, ūkio dalies vedėjas, už darbų saugą atsakingas asmuo.

17. Veiklos tęstinumo valdymo funkcijos:

17.1. situacijos analizė ir sprendimų veiklos tęstinumo valdymo klausimais priėmimas;

17.2. bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

17.3. bendravimas su teisėsaugos ir kitomis institucijomis, institucijų darbuotojais ir kitomis interesų grupėmis;

17.4. finansinių ir kitų išteklių, reikalingų Informacinės sistemos veiklai atkurti, įvykus

elektroninės informacijos saugos incidentui, naudojimo kontrolė;

17.5. Informacinės sistemos elektroninės informacijos fizinė sauga įvykus elektroninės informacijos saugos incidentui;

17.6. logistika (žmonių, daiktų, įrangos gabenimas ir organizavimas);

17.7. Informacinės sistemos veiklos atkūrimo priežiūra ir koordinavimas.

18. Veiklos atkūrimo grupės sudėtis:

18.1. Veiklos atkūrimo grupės vadovas: Įstaigos direktorius;

18.2.

18.3. Veiklos atkūrimo grupės vadovo pavaduotojas: vyriausioji psichikos sveikatos slaugytoja;

18.4. Veiklos atkūrimo grupės nariai: duomenų apsaugos pareigūnas, IT specialistas, ūkio dalies vedėjas.

19. Veiklos atkūrimo grupės funkcijos:

19.1. tarnybinių stočių veikimo atkūrimo organizavimas;

19.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

19.3. IS elektroninės informacijos atkūrimo organizavimas;

19.4. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

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

20. Personalinę Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės sudėtį tvirtina Įstaigos vadovas.

21. Veiklos tęstinumo valdymo grupės, Veiklos atkūrimo grupės veiklą organizuoja ir koordinuoja šių grupių vadovai.

22. Veiksmai, reikalingi IS veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, jų vykdymo eiliškumas, terminai ir atsakingi vykdytojai nurodyti Valdymo plano priede Nr. 1.

23. Atsarginėms patalpoms, naudojamoms IS veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, keliami šie reikalavimai:

23.1. turi atitikti priešgaisrinės saugos reikalavimus;

23.2. turi atitikti IS techninės įrangos gamintojų nustatytus reikalavimus įrangos darbo aplinkai (pavyzdžiui, tinkama oro temperatūra, oro drėgmė ir kita);

23.3. turi būti įrengtos langų, durų, IS techninės įrangos, kabelių fizinės apsaugos priemonės;

23.4. turi būti įrengta patalpų apsaugos signalizacija, kurios signalai turi būti persiunčiami patalpas saugančiai saugos tarnybai;

23.5. turi būti atskirtos nuo bendrojo naudojimo patalpų;

23.6. turi būti interneto ryšio prieiga;

23.7. turi būti įrengti nenutrūkstamą elektros tiekimą užtikrinantys maitinimo šaltiniai;

23.8. turi būti užtikrintas elektroninių ryšių tinklais perduodamos elektroninės informacijos vientisumas ir konfidencialumas;

23.9. turi būti įdiegtos kitos priemonės, atitinkančios pagrindinėms patalpoms keliamus reikalavimus.

24. Atsarginės patalpos, pritaikytos IS atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, yra kabineto Nr. 2 patalpos, esančios VšĮ Raseinių psichikos sveikatos centro antro aukšto patalpose. Veiklos tęstinumo valdymo grupė ir Veiklos atkūrimo grupė organizuoja bendrą susirinkimą, įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, nenumatytoms situacijoms arba įvykus esminiams organizaciniams IS ar jų komponentų pokyčiam.

25. Veiklos tęstinumo valdymo grupė, atlikusi situacijos analizę, informuoja Veiklos atkūrimo grupę apie priimtus sprendimus IS veiklos tęstinumo valdymo klausimais. Veiklos atkūrimo grupė, atsižvelgdama į priimtus sprendimus, organizuoja IS veiklos atkūrimą.

26. Veiklos tęstinumo valdymo ir Veiklos atkūrimo grupės tarpusavyje bendrauja žodžiu, telefonu ir elektroniniu paštu

III. APRAŠOMOSIOS NUOSTATOS

27. IS veiklos tęstinumui užtikrinti turi būti parengti ir saugomi šie dokumentai:

27.1. IS dokumentacija, kurioje nurodyta IS informacinių technologijų įranga ir jos parametrai, už ją atsakingi asmenys;

27.2. kiekvieno pastato, kuriame yra IS įranga, aukštų patalpų brėžiniai ir juose pažymėta:

27.2.1. tarnybinės stotys;

27.2.2. kompiuterių tinklo ir telefonų tinklo mazgai;

27.2.3. kompiuterių tinklo ir telefonų tinklo tiesimo tarp pastato aukštų vietos;

27.2.4. elektros įvedimo pastate vietos;

27.2.5. IS kompiuterių tinklo fizinio ir loginio sujungimo schemos;

27.3. kompiuterinės, techninės ir programinės įrangos sutarčių sąrašas;

27.4. elektroninės informacijos atsarginių kopijų darymo ir išbandymo tvarkos aprašas, kuriame turi būti nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

27.5. Veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, kuriais šiuos asmenis galima pasiekti bet kuriuo paros metu.

27.6. minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos Įmonės poreikius atitinkančiai IS veiklai užtikrinti, įvykus kibernetiniam ar elektroninės informacijos saugos incidentui ar nenumatytai situacijai, specifikacija; už šios įrangos priežiūrą atsakingų administratorių sąrašas ir minimalūs reikiamos kompetencijos ar žinių lygio reikalavimai IS veiklai atkurti nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą.

28. Už Veiksmų plano 27.1.–27.6. papunkčiuose nurodytų dokumentų parengimo organizavimą, saugojimą, nuolatinį atnaujinimą ir kompiuterinės, techninės ir programinės įrangos sutarčių vykdymo priežiūrą atsakingas Informacinės sistemos administratorius. Šiame punkte nurodyti dokumentai saugomi išspausdinti kabinete Nr. 7. Jeigu naudojama IS įranga (pagal nuomos, panaudos ar kitas sutartis) priklauso trečiajai šaliai ir yra jos patalpose, sutarties su trečiąja šalimi kopija turi būti saugoma kartu su šiame punkte nurodytais dokumentais.

29. Elektroninės informacijos saugos incidento ar kibernetinio incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga įsigyjama Lietuvos Respublikos viešųjų pirkimų įstatymo nustatyta tvarka.

30. Kad būtų užtikrintas patikimas Informacinės sistemos veikimas įvykus elektroninės informacijos saugos incidentui, naudojama rezervinė techninė įranga, kuri turi būti laikoma atsarginėje patalpoje, esančioje kitu adresu nei pagrindinė patalpa, kurioje laikoma pagrindinė Informacinės sistemos techninė įranga.

IV. VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

31. Valdymo plano veiksmingumas išbandomas ne rečiau kaip kartą per metus teorinių ir (ar) praktinių mokymų metu, modeliuojant kibernetinį ar elektroninės informacijos saugos incidentą. Valdymo plano veiksmingumo išbandymas gali būti planinis arba neplaninis. Plano veiksmingumo išbandymą organizuoja Informacijos saugos įgaliotinis.

32. Valdymo plano veiksmingumo išbandymo rezultatai turi būti naudojami Valdymo planui atnaujinti. Nustačius Valdymo plano veiksmingumo trūkumų, rengiama pastebėtų Valdymo plano veiksmingumo trūkumų šalinimo ataskaita. Už Valdymo plano veiksmingumo trūkumų šalinimo

ataskaitos parengimą atsakingas Informacijos saugos įgaliotinis.

33. Plano veiksmingumo išbandymo metu pastebėti Valdymo plano veiksmingumo trūkumai šalinami remiantis efektyvumo, ekonomiškumo, rezultatyvumo ir operatyvumo principais.

34. Veiklos tęstinumo valdymo procesams tobulinti turi būti nustatomi ir vertinami šie rodikliai:

34.1. IS neprieinamumas valandomis per metus;

34.2. IS veiklos atkūrimo, įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, trukmė.

VšĮ Raseinių psichikos sveikatos centro informacinės sistemos veiklos tęstinumo valdymo plano 1 priedas

VIEŠOSIOS ĮSTAIGOS RASEINIŲ PSICHIKOS SVEIKATOS CENTRO INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

1. VšĮ Raseinių psichikos sveikatos centro (toliau – Įstaigos) valdomos ir tvarkomo informacinės sistemos (toliau – IS arba Informacinė sistema) veiklos atkūrimo detaliajame plane (toliau – Detalusis planas) nurodomi veiksmai, reikalingi Įstaigos IS veiklai atkurti įvykus kibernetiniam ar elektroninės informacijos saugos incidentui, jų vykdymo eiliškumas, terminai ir atsakingi vykdytojai.

2. Įsigaliojus Įstaigos IS veiklos tęstinumo valdymo planui, Veiklos tęstinumo valdymo grupė informuoja IS naudotojus, kitus suinteresuotus asmenis apie IS veikimo sutrikimus. Informacija teikiama pagrindinio Įstaigos interneto svetainėje, IS taikomosiose programose, kitomis priemonėmis (pavyzdžiui, raštu, elektroniniu paštu ir panašiai).

3. Veiklos atkūrimo grupė informacinių sistemų veiklą atkuria pagal šiuos IS funkcijų prioritetus:

3.1. tarnybinių stočių veikimo atkūrimas:

3.1.1. duomenų bazės veikimo atkūrimas;

3.1.2. taikomųjų programų veikimo atkūrimas;

3.2. kompiuterių tinklo veikimo atkūrimas;

3.3. elektroninės informacijos atkūrimas;

3.4. taikomųjų programų veikimo atkūrimas;

3.5. interneto ryšio atkūrimas;

3.6. pagrindinio IS tvarkytojo kompiuterinių darbo vietų veikimo atkūrimas;

3.7. kitų IS tvarkytojų kompiuterinių darbo vietų veikimo atkūrimas.

4. IS veiklos atkūrimo veiksmai, atsižvelgiant į kibernetinio ar elektroninės informacijos saugos incidento tipą ir mastą, veiklos atkūrimo veiksmų pobūdį, turi būti atlikti per kuo trumpesnį terminą, kuris neturi būti ilgesnis kaip 8 valandos.

Situacija	**Veiklos atkūrimo veiksmai**	**Už veiklos atkūrimo veiksmus atsakingi asmenys**
1. Patalpų pažeidimas arba praradimas	1.1. personalo evakuacija;	Ūkio dalies vedėjas, už darbuotojų saugumą atsakingas asmuo
	1.2. avarinių tarnybų informavimas, atsižvelgiant į iškilusio pavojaus pobūdį;	Ūkio dalies vedėjas, už darbuotojų saugumą atsakingas asmuo
	1.3. žalos įvertinimas;	Veiklos tęstinumo valdymo grupė
	1.4. esant reikalui, darbo organizavimas atsarginėse patalpose;	Veiklos tęstinumo valdymo grupė
	1.5. pažeistų ryšio linijų ir sugadintos techninės įrangos atstatymo ir duomenų atkūrimo organizavimas;	Veiklos atkūrimo grupė
	1.6. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.	Veiklos tęstinumo valdymo grupė
2. Elektros tiekimo sutrikimai	2.1. elektros tiekimo sutrikimo masto ir kritiškumo įvertinimas;	Veiklos tęstinumo valdymo grupė
	2.2. kreipimasis į elektros energijos tiekimo bendrovę dėl sutrikimo pašalinimo trukmės prognozės;	Veiklos atkūrimo grupė
	2.3. vietinio elektros tinklo atstatymo	Veiklos atkūrimo grupė

Situacija	Veiklos atkūrimo veiksmai	Už veiklos atkūrimo veiksmus atsakingi asmenys
	organizavimas, jei buvo pažeistas Informacinės sistemos veiklą užtikrinantis elektros tinklas;	
	2.4. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.	Veiklos tęstinumo valdymo grupė
3. Ryšio sutrikimai	3.1. kritiškumo įvertinimas;	Veiklos atkūrimo grupė
	3.2. ryšio sutrikimo priežasties nustatymas;	Veiklos atkūrimo grupė
	3.3. kreipimasis į ryšio paslaugų tiekėją dėl sutrikimo pašalinimo trukmės prognozės;	Veiklos atkūrimo grupė
	3.4. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.	Veiklos tęstinumo valdymo grupė
4. Tarnybinių stočių sugadinimas ir (arba) praradimas	4.1. kritiškumo įvertinimas	Veiklos tęstinumo valdymo grupė
	4.2. vagystės arba vandalizmo atvejais teisėsaugos tarnybų informavimas ir jų nurodymų vykdymas	Veiklos tęstinumo valdymo grupė
	4.3. esamų techninės įrangos išteklių perskirstymas, siekiant kompensuoti praradimą;	Veiklos atkūrimo grupė
	4.4. iškilus reikalui, kreipimasis į techninės įrangos tiekėjus dėl sugadintos įrangos remonto ar dėl naujos techninės įrangos įsigijimo;	Veiklos atkūrimo grupė
	4.5. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.	Veiklos tęstinumo valdymo grupė
5. Programinės įrangos sugadinimas	5.1. kritiškumo įvertinimas	Veiklos atkūrimo grupė
	5.2. sugadintos programinės įrangos atstatymas iš kopijų	Veiklos atkūrimo grupė
	5.3. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje	Veiklos tęstinumo valdymo grupė
6. Duomenų sugadinimas, praradimas arba atskleidimas	6.1. kritiškumo įvertinimas	Veiklos tęstinumo valdymo grupė
	6.2. neteisėto duomenų sugadinimo arba atskleidimo atvejais teisėsaugos tarnybų informavimas ir jų nurodymų vykdymas	Veiklos tęstinumo valdymo grupė
	6.3. Informacinės sistemos veiklos sutrikimo dėl duomenų sugadinimo ar praradimo atvejais duomenų atstatymas iš kopijų	Veiklos atkūrimo grupė
	6.4. įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje	Veiklos tęstinumo valdymo grupė

VšĮ Raseinių psichikos sveikatos centro informacinės sistemos veiklos tęstinumo valdymo plano 2 priedas

(VšĮ Raseinių psichikos sveikatos centro informacinės sistemos elektroninės informacijos saugos incidentų registravimo žurnalo formos pavyzdys)

VšĮ RASEINIŲ PSICHIKOS SVEIKATOS CENTRO INFORMACINĖS SISTEMOS ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia 20 _ m. _____d.

Eil. Nr.	**Elektroninės informacijos saugos incidentas**						
	Informacinės sistemos tvarkymo įstaigos pavadinimas	**Požymio kodas**	**Įvykio aprašymas**	**Pradžia (metai, mėnuo, diena, valanda)**	**Pabaiga (metai, mėnuo, diena, valanda)**	**Pašalino (vardas, pavardė)**	**Informacinės sistemos saugos įgaliotinis (vardas, pavardė, parašas)**
1.							
2.							
3.							
4.							
5.							
6.							

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 atakos; 13 – dokumentų praradimas; 14 – duomenų iš duomenų teikėjų negavimas; 15 – dalinis Informacinės sistemos informacinės sistemos sutrikimas dėl neaiškių priežasčių; 16 – gamtos reiškiniai.

_____