PATVIRTINTA
Biržų Vlado Jakubėno muzikos mokyklos
direktoriaus 2024 m. sausio 23 d.
įsakymu Nr. VK-8

BIRŽŲ VLADO JAKUBĖNO MUZIKOS MOKYKLOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Biržų Vlado Jakubėno muzikos mokyklos informacinės sistemos veiklos tęstinumo valdymo plane (toliau – Planas) reglamentuojamas Biržų Vlado Jakubėno muzikos mokyklos (toliau – Mokykla) ir Mokyklos informacinės sistemos (toliau – IS) veiklos tęstinumo užtikrinimas.

2. Šis Planas privalomas Mokyklos IS tvarkytojams, saugos įgaliotiniui, administratoriui ir IS naudotojams.

3. Plane vartojamos Lietuvos Respublikos kibernetinio saugumo įstatyme, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių apraše, Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (su visais pakeitimais), Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ (su visais pakeitimais) ir kituose teisės aktuose, reglamentuojančiuose saugų elektroninės informacijos tvarkymą apibrėžtos sąvokos.

4. Plano tikslas – užtikrinti Informacinių sistemų veiklos tęstinumą incidento metu, kilus pavojui Informacinių sistemų duomenims, techninės ir programinės įrangos funkcionavimui. Valdymo planas vykdomas, įvykus incidentui, kuris gali turėti įtakos Mokyklos veiklai.

5. Elektroninės informacijos saugos incidentas – įvykis ar veiksmas, kuris 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.

6. Saugos įgaliotinis, įtaręs neteisėtą veiklą, pažeidžiančią Mokyklos saugą, privalo imtis reikiamų priemonių, kad nebūtų pažeista elektroninės informacijos sauga, ir apie tai pranešti Mokyklos vadovybei.

7. Informacinių sistemų administratoriai informuoja Saugos įgaliotinį apie pastebėtus Informacinių sistemų veiklos sutrikimus, neveikiančias ar netinkamai veikiančias duomenų saugos užtikrinimo priemones, taip pat dalyvauja šalinant Informacinių sistemų veiklos sutrikimus.

8. Naudotojai, pastebėję Informacinių sistemų veiklos sutrikimus, neveikiančias ar netinkamai veikiančias duomenų saugos užtikrinimo priemones, turi nedelsdami apie tai pranešti administratoriui ir (ar) Saugos įgaliotiniui. Incidento atveju naudotojai neturi teisės savo iniciatyva imtis jokių atsakomųjų veiksmų.

9. Kilus incidentui, jo nustatymas, vertinimas, informavimas apie incidentą, kibernetinių

incidentų tyrimas ir incidento analizė, baigus incidentų tyrimą, vykdomi Nacionaliniame kibernetinių incidentų valdymo plane nustatyta tvarka, o Valdymo plano nuostatos taikomos tiek, kiek incidentų valdymo nereglamentuoja Nacionalinis kibernetinių incidentų valdymo planas.

10. Įvykus bet kokiam incidentui, pirmiausia užtikrinamas darbuotojų saugumas, po to stengiamasi išsaugoti Mokyklos Informacinių sistemų duomenų bazės kopijas bei techninius išteklius.

11. Saugos įgaliotinis atsako už Plano įgyvendinimo organizavimą ir kontrolę.

12. Naudotojai, kibernetinio saugumo vadovas ir informacinių sistemų administratorius yra atsakingi už Plano įgyvendinimą.

13. Kibernetinio incidento metu patirti nuostoliai padengiami teisės aktų nustatyta tvarka.

14. Informacinių sistemų veikla atkuriama vadovaujantis šiomis nuostatomis:

14.1. Informacinių sistemų veikla atkuriama pagal kiekvienos Informacinės sistemos atliekamų funkcijų prioritetus, stabdant visą neesminę veiklą;

14.2. naudotojai privalo užtikrinti, kad būtų vykdomi Informacinių sistemų saugos politikos įgyvendinamuosiuose dokumentuose nustatyti reikalavimai.

15. Kriterijai, pagal kuriuos nustatoma, kad Informacinių sistemų veikla yra atkurta:

15.1. Informacinių sistemų duomenys yra prieinami naudotojams;

15.2. tvarkant Informacinių sistemų duomenis užtikrinamas jų konfidencialumas ir vientisumas;

15.3. užtikrinta virtualių mašinų, tinklo įrangos ir darbo vietų kompiuterių techninės ir programinės įrangos veikla ir teikiamos kokybiškos paslaugos.

16. IS veiklos atkūrimas finansuojamas iš Mokyklos biudžeto ir kitų teisės aktuose nustatytų finansavimo šaltinių.

17. IS veikla laikoma atkurta, jeigu bent 90 proc. yra atkurtas sistemos prieinamumas autorizuotų informacinės sistemos naudotojų atžvilgiu.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

18. Elektroninės informacijos saugos incidentams valdyti ir veiklos atkūrimui organizuoti Mokyklos direktoriaus įsakymu tvirtinamos 2 grupės: IS veiklos tęstinumo valdymo grupė (toliau – Valdymo grupė) ir IS veiklos atkūrimo grupė (toliau – Atkūrimo grupė).

19. Valdymo grupės tikslai: tirti elektroninės informacijos saugos incidentus, ieškoti priemonių ir būdų sukeltiems padariniams ir žalai likviduoti, užtikrinti IS veiklos tęstinumą.

20. Valdymo grupę sudaro:

20.1. Valdymo grupės vadovas – Mokyklos direktorius;

20.2. Valdymo grupės vadovo pavaduotojas – Mokyklos direktoriaus pavaduotojas;

20.3. Valdymo grupės nariai:

20.3.1. IS saugos įgaliotinis;

20.3.2. vyriausioji buhalterė.

21. Valdymo grupės funkcijos, užtikrinant veiklos tęstinumą:

21.1. situacijos analizė, problemų (incidentų) nustatymas;

21.2. sprendimų IS veiklos tęstinumo valdymo klausimais priėmimas ir kontrolė;

21.3. bendravimas su teisėsaugos ir kitomis institucijomis, Mokyklos darbuotojų informavimas;

21.4. finansinių ir kitų išteklių, reikalingų IS veiklai atkurti, įvykus nenumatytai situacijai, nustatymas ir naudojimo kontrolė;

21.5. elektroninės informacijos fizinės saugos, įvykus elektroninės informacijos saugos incidentui, užtikrinimas;

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

21.7. bendravimas su kitų informacinių sistemų veiklos tęstinumo valdymo grupėmis, žiniasklaidos atstovais;

21.8. kitos Valdymo grupei pavestos funkcijos.

22. Veiklos atkūrimo grupę sudaro:

22.1. Veiklos atkūrimo grupės vadovas – IS saugos įgaliotinis;

22.2. Veiklos atkūrimo grupės narys – IS administratorius;

23. Veiksmai, įvykus esminiams pokyčiams informacinėje sistemoje:

23.1. IS ir jos duomenų atkūrimo organizavimas;

23.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

23.3. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

23.4. kompiuterinių darbo vietų veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

23.5. Valdymo grupės informavimas;

23.6. kitos Atkūrimo grupei pavestos funkcijos.

24. Valdymo grupė organizuoja susirinkimą kartą per metus arba įvykus esminiams pokyčiams. Atkūrimo grupė organizuoja susirinkimą įvykus elektroninės informacijos saugos incidentui.

25. Esant būtinybei ar įvykus incidentui, Valdymo grupė į susirinkimą gali pasikviesti ir Atkūrimo grupės vadovą bei narius.

26. Grupės tarpusavyje komunikuoja tiesiogiai, telefonu ar elektroniniu paštu.

27. Saugos įgaliotinis, atsižvelgdamas į Valdymo grupės atliktos incidento analizės rezultatus, įvertina incidentą vadovaudamasis Nacionalinio kibernetinių incidentų valdymo plano priede nustatytais kriterijais ir priskiria incidentui kategoriją. Jeigu nustatytas incidentas ir (ar) jo poveikis atitinka bent vieną iš kriterijų, nurodytų Nacionalinio kibernetinių incidentų valdymo plano priede, būdingų pavojingo kibernetinio incidento kategorijai, Saugos įgaliotinis incidentą priskiria didelio poveikio kibernetinio incidento kategorijai.

28. Numatytose atsarginėse patalpose, naudojamose IS veiklai atkurti, elektroninės informacijos saugos incidento atveju, turi būti:

28.1. parengta ir veikianti duomenų perdavimo tinklo prieiga;

28.2. tiekiamas nepertraukiamas elektros maitinimas tarnybinėms stotims ir duomenų perdavimo tinklo įrangai;

28.3. įdiegtos įrangos kondicionavimo sistemos, užtikrinančios reikiamą patalpų temperatūrą ir drėgnumą;

28.4. rakinamos durys.

29. IS atkuriama pagal šiame plane numatytą IS atkūrimo prioritetą (l priedas), planas pateiktas (5 priede).

30. IS saugos įgaliotinio, IS administratoriaus, IS naudotojų, kitų asmenų įgaliojimai ir veiksmai išdėstyti informacinės sistemos veiklos tęstinumo detaliajame plane (2 priedas).

31. Elektroninės informacijos saugos incidentų, įvykusių IS, tyrimas Administracijoje vyksta pagal nustatytą tvarką (3 priedas).

32. Elektroninės informacijos saugos incidento metu sunaikinta ar sugadinta įranga įsigyjama viešųjų pirkimų būdu.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

33. Informacinių technologijų įrangos sąrašas, minimali techninė įranga informacinių sistemų veiklai atkurti, minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos užtikrinti Mokyklos poreikius atitinkančią IS veiklą elektroninės informacijos saugos incidento metu, specifikacija saugomi Mokykloje.

34. Biržų Vlado Jakubėno muzikos mokyklos (Kęstučio g. 6, Biržai) patalpų ir aukštų techniniai brėžiniai saugomi Mokykloje.

35. Kompiuterių tinklo fizinio ir loginio sujungimo schemos, techninės ir programinės įrangos priežiūros sutarčių sąrašas, minimaliam IS funkcionalumo atkūrimui būtinos įrangos

specifikacija, duomenų atkūrimui reikalingos darbuotojų kompetencijos aprašas saugomi Mokykloje.

36. Kadangi Mokykla naudojasi Savivaldybės administracijos serveriuose esančiomis informacinėmis sistemomis, todėl informacinių sistemų atsarginės duomenų kopijos daromos ir saugomos tuose serveriuose.

37. Mokyklos darbuotojų sąrašas, kuriame nurodyti darbuotojų darbo telefonai, o Valdymo grupės ir Atkūrimo grupės narių – mobiliojo ir namų telefono numeriai ir gyvenamosios vietos adresai, saugomas Mokykloje.

38. Veiklos tęstinumo vykdymui reikalingos informacijos rengimą ir atnaujinimą organizuoja saugos įgaliotinis.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

39. IS saugos įgaliotinis organizuoja Mokyklos darbuotojų supažindinimą su šiuo planu.

40. Plano veiksmingumas turi būti išbandomas kartą per metus. Bandymo metu Atkūrimo grupė išanalizuoja galimą (sumodeliuotą) nenumatytą situaciją, numato galimus jos sprendimų būdus (4 priedas).

41. Saugos įgaliotinis per 15 darbo dienų po Valdymo plano veiksmingumo bandymo parengia Valdymo plano veiksmingumo bandymo metu pastebėtų trūkumų ataskaitą ir priemonių planą pastebėtiems trūkumams pašalinti.

42. Valdymo plano veiksmingumo bandymo metu pastebėti trūkumai šalinami vadovaujantis veiksmingumo, operatyvumo ir ekonomiškumo principais.

43. Kibernetinių incidentų valdymo patirtis nuolat vertinama, išmoktos pamokos fiksuojamos ataskaitose ir pagal jas Valdymo planas tobulinamas.

_____

Biržų Vlado Jakubėno muzikos mokyklos
informacinės sistemos veiklos tęstinumo
valdymo plano
1 priedas

INFORMACINIŲ SISTEMŲ ATKŪRIMO PRIORITETAI IR ATSAKOMYBĖ

Eil. Nr.	**Aprašymas**	**Atsakingas už atkūrimą**
1.	Kompiuterių tinklo veikimo atkūrimo organizavimas	IS administratorius
2.	Elektroninis paštas	IS administratorius
3.	Dokumentų valdymo IS „AVILYS“	IS administratorius
4.	Buhalterinės apskaitos IS „LABBIS“	IS administratorius
5.	Viešųjų pirkimų IS „EcoCost“	IS administratorius
6.	Interneto svetainės http://www.muzikosmokykla.puslapiai.lt turinio valdymo IS	IS administratorius

_____

Biržų Vlado Jakubėno muzikos mokyklos
informacinės sistemos veiklos tęstinumo
valdymo plano
2 priedas

BIRŽŲ VLADO JAKUBĖNO MUZIKOS MOKYKLOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO DETALUSIS PLANAS

Pavojaus rūšys	**Pirmaeiliai veiksmai**	**Pasekmės likvidavimo veiksmai**	**Pasekmės likvidavimo atsakingi vykdytojai**
1. Gamtos veiksniai	1.1. Nenumatytos situacijos pasekmės įvertinimas	1.1.1. nenumatytos situacijos metu padarytos žalos įvertinimas	IS saugos įgaliotinis
		1.1.2. padarytą žalą likviduojančių darbuotojų instruktavimas	IS saugos įgaliotinis
		1.1.3. nenumatytos situacijos metu padarytos žalos likvidavimas	IS administratorius
2. Gaisro keliamas pavojus	2.1. Priešgaisrinės gelbėjimo tarnybos informavimas 2.2. Gaisro gesinimas ankstyvoje stadijoje	2.1.1. įvykio vietos lokalizavimas, jei yra rekomendacija	IS saugos įgaliotinis
		2.1.2. galimybių evakuoti darbuotojus nagrinėjimas, jei yra rekomendacija	IS saugos įgaliotinis
		2.1.3. darbuotojų informavimas apie evakavimą, jei yra rekomendacija	IS saugos įgaliotinis
		2.1.4. darbuotojų informavimas apie saugų darbą pavojaus zonoje	IS saugos įgaliotinis
		2.1.5. nenumatytos situacijos metu padarytos žalos įvertinimas	IS saugos įgaliotinis
		2.1.6. padarytą žalą likviduojančių darbuotojų instruktavimas	IS saugos įgaliotinis
		2.1.7. nenumatytos situacijos metu padarytos žalos likvidavimas	IS administratorius
3. Elektros energijos tiekimo sutrikimai	3.1. Energijos tiekimo sutrikimo priežasčių nustatymas	3.1.1. rekomendacijų iš energijos tiekimo tarnybos gavimas	IS administratorius
		3.1.2. žalą likviduojančių darbuotojų instruktavimas	IS saugos įgaliotinis
		3.1.3. padarytos žalos likvidavimas	IS administratorius
4. Šilumos energijos tiekimo sutrikimai	4.1. Kreipimasis į šilumos energijos paslaugų tiekėją dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių	4.1.1. šilumos energijos paslaugų teikėjo rekomendacijų gavimas	IS administratorius

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Pasekmės likvidavimo atsakingi vykdytojai
		4.1.2. darbuotojų informavimas apie rekomendacijas	IS saugos įgaliotinis
	4.2. Sutrikimo šalinimo prognozės skelbimas	4.2.1. padarytos žalos įvertinimas	IS saugos įgaliotinis
		4.2.2. padarytos žalos likvidavimas	IS administratorius
5. Ryšio sutrikimas komunikacijų tinkle	5.1. Ryšio sutrikimo priežasčių nustatymas	5.1.1. ryšio paslaugos teikėjo rekomendacijų gavimas	IS administratorius
	5.2. Sutrikimo šalinimo prognozės skelbimas	5.2.1. sutrikimo likvidavimas	IS administratorius
6. Įsilaužimas į vidinį kompiuterių tinklą	6.1. Pranešimas apie įvykį teisėsaugos tarnybai	6.1.1. teisėsaugos tarnybos nurodymų vykdymas	IS saugos įgaliotinis, IS administratorius, IS naudotojai
		6.1.2. nenumatytos situacijos pasekmės likvidavimas	IS administratorius
7. Pagrindinių tarnybinių stočių sugadinimas ir/arba praradimas	7.1. Pranešimas apie įvykį teisėsaugos tarnybai	7.1.1.teisėsaugos tarnybos nurodymų vykdymas	IS saugos įgaliotinis, IS administratorius, IS naudotojai
		7.1.2. nenumatytos situacijos pasekmės likvidavimas	IS administratorius
		7.1.3. padarytą žalą likviduojančių darbuotojų instruktavimas	IS saugos įgaliotinis
		7.1.4. padarytos žalos įvertinimas	IS saugos įgaliotinis
		7.1.5. žalos padarinių likvidavimas	IS administratorius
8. Vagystė iš duomenų bazės ar jos fizinis sunaikinimas, atskleidimas	8.1. Pranešimas apie įvykį teisėsaugos tarnybai	8.1.1. teisėsaugos tarnybos nurodymų vykdymas	IS saugos įgaliotinis, IS administratorius, IS naudotojai
		8.1.2. padarytos žalos įvertinimas	IS saugos įgaliotinis
		8.1.3. atkūrimas duomenų iš kopijų	IS administratorius
9. Programinės įrangos sugadinimas, praradimas	9.1. Pranešimas apie įvykį teisėsaugos tarnybai	9.1.1. teisėsaugos tarnybos nurodymų vykdymas	IS saugos įgaliotinis, IS administratorius, IS naudotojai
		9.1.2. nenumatytos situacijos metu padarytos žalos įvertinimas	IS administratorius
		9.1.3. žalą likviduojančių	IS saugos įgaliotinis

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmės likvidavimo veiksmai	Pasekmės likvidavimo atsakingi vykdytojai
		darbuotojų instruktavimas	
		9.1.4. padarytos žalos likvidavimas	IS administratorius
10. Vagystė	10.1. Pranešimas apie įvykį teisėsaugos tarnybai	10.1.1. teisėsaugos tarnybos nurodymų vykdymas	IS saugos įgaliotinis, IS administratorius, IS naudotojai
		10.1.2. vagystės metu padarytos žalos įvertinimas	Vyriausioji buhalterė, Informacinių technologijų specialistas
		10.1.3. vagystės padarinių likvidavimas	Informacinių technologijų specialistas
11. Pavojingas (įtartinas) radinys	11.1. Pranešimas apie įvykį teisėsaugos tarnybai	11.1.1. teisėsaugos tarnybos nurodymų vykdymas	IS saugos įgaliotinis, IS administratorius, IS naudotojai
12. Įvykis susijęs su teroristine veikla	12.1. Pranešimas apie įvykį teisėsaugos tarnybai	12.1.1. teisėsaugos tarnybos nurodymų vykdymas	IS saugos įgaliotinis, IS administratorius, IS naudotojai

_____

Biržų Vlado Jakubėno muzikos mokyklos
informacinės sistemos veiklos tęstinumo
valdymo plano
3 priedas

BIRŽŲ VLADO JAKUBĖNO MUZIKOS MOKYKLOS INFORMACINĖS SISTEMOS SAUGOS INCIDENTŲ TYRIMO TVARKA

1. Elektroninės informacijos saugos incidentas – įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie IS galimybę, sutrikdyti ar pakeisti IS veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti (pvz. duomenų neatitikimas ar pažeidimas, atsiradę konkretūs nesklandumai, ekrano pranešimai, neįprastas funkcionavimas, paslaugų, įrangos ar priemonių netektis, sistemos sutrikimai arba persikrovimai, žmogiškosios klaidos, fizinio saugumo pažeidimas, nesankcionuoti sistemos pakeitimai, nesankcionuota prieiga, saugos politikos neatitikimas ir kt.).
2. IS naudotojai privalo nedelsdami žodžiu ar raštu pranešti apie elektroninės informacijos saugos incidentą informatikos specialistui.
3. Elektroninės informacijos saugos incidento atveju IS naudotojai neturi teisės imtis jokių atsakomųjų veiksmų.
4. Informatikos specialistas nedelsdamas turi imtis atsakomųjų veiksmų, reikalingų elektroninės informacijos saugos incidentui stabdyti.
5. Informacinių sistemų saugos įgaliotinis teikia IS valdytojui tarnybinį pranešimą apie saugos incidentą.
6. Informacinių sistemų saugos įgaliotinis pagal galimybes surenka visą su saugos incidentu susijusią informaciją ir ją dokumentuoja, saugos incidentus ir informacinės sistemos atkuriamuosius darbus po informacijos saugos incidento registruoja saugos incidentų žurnale.
7. Informacinių sistemų saugos įgaliotinis privalo informuoti pranešusį apie incidentą asmenį apie pašalintus nesklandumus.
8. Informacijos saugumo incidentui peržengus Mokyklos ribas, Mokyklos darbuotojai privalo derinti atsakomuosius veiksmus ir pagal situaciją keistis informacija apie incidentus su paslaugų teikėjais ar kitomis institucijomis.
9. IS naudotojų drausminės procedūros atliekamos vadovaujantis Tarnybinių nuobaudų skyrimo valstybės tarnautojams taisyklėmis, Darbo kodeksu.

_____

Biržų Vlado Jakubėno muzikos mokyklos
informacinės sistemos veiklos tęstinumo
valdymo plano
4 priedas

INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO IŠBANDYMO ATASKAITA

(Grupės susitikimo data ir dokumento numeris)
Nenumatytos situacijos bandyme dalyvavo grupės nariai:
1. _____
2. _____
3. _____
(...) _____
Nenumatytos situacijos scenarijus:
_____
_____
_____

Informacinės sistemos, kurias paveikia nenumatyta situacija:
_____
_____
_____
Nenumatytos situacijos pašalinimo eiga:
_____
_____
_____

Rasti nenumatytų situacijų valdymo plano trūkumai:
_____
_____
_____

Pasiūlymai keisti arba papildyti nenumatytų situacijų valdymo planą:
_____
_____
_____

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

Biržų Vlado Jakubėno muzikos mokyklos
informacinės sistemos veiklos tęstinumo
valdymo plano
5 priedas

INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO PLANAS

Elektroninės informacijos saugos incidentas	Veiklos atkūrimo veiksmai	Atsakingi vykdytojai
5. Telekomunikacijų ir kitų ryšio tinklų sutrikimai	5.1. Telekomunikacijų ir kitų ryšio tinklų sutrikimų priežasčių nustatymas. Vykdymo terminas – 1 val.	Informacinių sistemų administratorius
	5.2. Kreipimasis į telekomunikacijų ir kitų ryšio tinklų paslaugų teikimo tarnybą dėl sutrikimo trukmės ir pašalinimo galimybių. Vykdymo terminas – 10 min.	Informacinių sistemų administratorius
	5.3. Darbuotojų informavimas. Vykdymo terminas – 10 min.	Informacinių sistemų administratorius
	5.4. Elektroninės informacijos saugos incidento padarinių įvertinimas, priemonių plano padarytai žalai likviduoti sudarymas ir įgyvendinimas. Vykdymo terminas – 24 val.	Saugos įgaliotinis, informacinių sistemų administratorius
6. Kompiuterių tinklo įrangos sugadinimas	6.1. Kompiuterių tinklo įrangos sugadinimo priežasčių nustatymas. Vykdymo terminas – 1 val.	Informacinių sistemų administratorius
	6.2. Kreipimasis į įrangos tiekėjus dėl įrangos remonto arba naujos įrangos įsigijimo. Vykdymo terminas – 10 min.	Informacinių sistemų administratorius
	6.3. Darbuotojų informavimas. Vykdymo terminas – 10 minučių.	Informacinių sistemų administratorius
	6.4. Elektroninės informacijos saugos incidento padarinių įvertinimas, priemonių plano padarytai žalai likviduoti sudarymas ir įgyvendinimas. Vykdymo terminas – 24 val.	Saugos įgaliotinis, informacinių sistemų administratorius
7. Įsilaužimas į vidinį kompiuterių tinklą	7.1. Įsilaužimo būdo nustatymas. Vykdymo terminas – 1 val.	Informacinių sistemų administratorius
	7.2. Aptikto įsilaužimo užkardymas.	Informacinių sistemų administratorius

Elektroninės informacijos saugos incidentas	Veiklos atkūrimo veiksmai	Atsakingi vykdytojai
	Vykdymo terminas – 10 min.	
	7.3. Viso vidinio tinklo patikra ir papildomų saugumo trūkumų analizė. Vykdymo terminas – 48 val.	Saugos įgaliotinis, informacinių sistemų administratorius
8. Programinės įrangos sugadinimas, praradimas	8.1. Programinės įrangos sugadinimo priežasčių nustatymas. Vykdymo terminas – 2 val.	Informacinių sistemų administratorius
	8.2. Sugadintos ar prarastos programinės įrangos atkūrimas. Vykdymo terminas – 20 val.	Informacinių sistemų administratorius
	8.3. Darbuotojų informavimas. Vykdymo terminas – 10 min.	Informacinių sistemų administratorius
	8.4. Elektroninės informacijos saugos incidento padarinių įvertinimas, priemonių plano padarytai žalai likviduoti sudarymas ir įgyvendinimas. Vykdymo terminas – 24 val.	Saugos įgaliotinis, informacinių sistemų administratorius
* Apie kibernetinius incidentus Nacionalinis kibernetinio saugumo centras turi būti informuojamas užpildant pranešimo apie incidentą formą, esančią interneto svetainėje https://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“.		

_____

Biržų Vlado Jakubėno muzikos mokyklos
informacinės sistemos veiklos tęstinumo
valdymo plano
6 priedas

KIBERNETINIŲ INCIDENTŲ REGISTRAVIMO ŽURNALAS

Eil. Nr.	Elektroninės informacijos saugos incidentas						
	Požymio kodas*	**Elektroninės informacijos saugos incidento aprašymas**	**Pradžia (data, laikas)**	**Pabaiga (data, laikas)**	**Elektroninės informacijos saugos incidentą pašalinęs (-ę) darbuotojas (-ai) (vardas (-ai), pavardė (-ės), parašas (-ai))**	**Saugos įgaliotinis (vardas, pavardė, parašas)**	**Elektroninės informacijos saugos incidento poveikio mažinimo priemonės**
1.							
2.							
3.							
4.							
5.							

* Elektroninės informacijos saugos incidento požymio kodai:
1. nenugalima jėga; 2. gaisras; 3. elektros energijos tiekimo sutrikimai; 4. vandentiekio ir šildymo sistemų sutrikimai; 5. telekomunikacijų ir kitų ryšio tinklų sutrikimai; 6. kompiuterių tinklo įrangos sugadinimas; 7. įsilaužimas į vidinį kompiuterių tinklą; 8. programinės įrangos sugadinimas.

_____