PATVIRTINTA
Vilniaus automechanikos ir verslo mokyklos
direktoriaus
2022 m. spalio 5 d. įsakymu Nr. V1-194

VILNIAUS AUTOMECHANIKOS IR VERSLO MOKYKLOS INTERNETINIŲ IR INTRANETINIŲ TINKLŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. SKYRIUS
BENDROSIOS NUOSTATOS

1. Internetinių ir intranetinių tinklų (toliau – IT sistemos) veiklos tęstinumo valdymo planas (toliau – Valdymo planas) parengtas pagal Nacionalinį kibernetinių incidentų valdymo planą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“. Valdymo planas vykdomas įvykus elektroninės informacijos saugos incidentui, kuris gali sudaryti neteisėto prisijungimo prie Mokyklos IT galimybę, sutrikdyti ar pakeisti 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.

2. Valdymo plane vartojamos sąvokos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“,

3. Kibernetinių incidentų valdymas, tyrimas, šalinimas bei pranešimas apie kibernetinius incidentus yra atliekamas vadovaujantis Nacionaliniame kibernetinių incidentų valdymo plane nurodytomis procedūromis.

4. Valdymo planas įsigalioja, kai dėl rizikos veiksnių nurodytų Mokyklos IT veiklos atkūrimo detaliajame plane (toliau – veiklos atkūrimo planas) (1 priedas), įvyksta saugumo incidentas, dėl kurio sutrinka IT veiklos tęstinumas ir tampa aišku, kad atkurti IT veikimą per 8 val. nepavyksta.

5. Už valdymo plano įgyvendinimo organizavimą atsakingas mokyklos vadovas ir jo įgalioti asmenys.

6. Valdymo plane nurodytomis IT veiklos tęstinumo procedūromis yra siekiama šių tikslų:

6.1. paskelbus apie saugumo įvykį, sutrikdžiusį IT veiklą, per trumpiausią terminą atkurti IT ir jos posistemių veiklą;

6.2. sustabdyti veiklą, kuri nėra gyvybiškai svarbi, kol bus visiškai atkurtas pagrindinių IT ir jos posistemių veiklos tęstinumas;

6.3. sušvelninti bet kokio saugumo įvykio, nurodyto veiklos atkūrimo plane, poveikį, atliekant nurodytus veiksmus;

6.4. sumažinti nesusipratimų ir klaidingos informacijos kiekį, sudarant aiškų veiklos atkūrimo planą ir jame įvardinant atsakingus asmenis.

7. Kiekvienas naudotojas, pastebėjęs susidariusią situaciją, kuri kelia grėsmę IT veiklos tęstinumui, privalo:

7.1. Informuoti Mokyklos vadovą apie pastebėtą situaciją, keliančią grėsmę IT veiklos tęstinumui;

7.2. Rūpintis asmeniniu saugumu, vadovautis avarijos likvidavimo procedūromis, vykdyti pagalbos tarnybų nurodymus;

7.3. Teikti pagalbą kitiems naudotojams nerizikuodamas savo sveikata;

7.4. Tęsti veiklą, kiek tai įmanoma susidariusios situacijos sąlygomis;

7.5. Pagal kompetenciją užtikrinti informacijos saugumą ir kokybę;

7.6. Vykdyti visus mokyklos IT inžinieriaus nurodymus;

7.7. Išsaugoti IT veiklai gyvybiškai svarbius duomenis, kad IT veiklos tęstinumas vėliau gelėtų būti atkurtas.

8. Kriterijai, pagal kuriuos nustatoma, kad IT veikla atkurta:

8.1. Veikia visa IT darbui reikalinga infrastruktūra;

8.2. Naudotojams prieinamos ir be kritinių klaidų veikia visos IT funkcijos;

8.3. Atnaujinami IT duomenys;

8.4. Išsaugomi atnaujinti IT duomenys;

8.5. Daromos IT duomenų atsarginės kopijos.

II. SKYRIUS
ORGANIZACINĖS NUOSTATOS

9. Mokyklos IT veikos tęstinumo valdymo grupės ir veiklos atkūrimo grupės nariai skiriami Mokyklos direktoriaus įsakymu.

10. Valdymo grupės funkcijos:

10.1. analizuoti kompiuterių tinklo saugos incidentus ir priimti sprendimus sistemos veiklos tęstinumo valdymo klausimais;

10.2. bendrauti su IT naudotojais;

10.3. bendrauti su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

10.4. bendrauti su teisėsaugos ir kitomis institucijomis, kitomis interesų grupėmis;

10.5. bendrauti su susijusių informacinių sistemų veiklos tęstinumo valdymo grupėmis;

10.6. finansinių ir kitų išteklių, reikalingų IT veiklai atkurti, įvykus IT elektroninės informacijos saugos incidentui, naudojimo kontrolė;

10.7. IT elektroninės informacijos fizinės saugos užtikrinimo kontrolę, įvykus IT elektroninės informacijos saugos incidentui;

10.8. Logistikos organizavimas (žmonių, daiktų, įrangos gabenimo organizavimas ir jų gabenimas);

10.9. IT veiklos atkūrimo priežiūra ir koordinavimas.

10.10. Vykdyti informacinių technologijų saugos atitikties vertinimą neriečiau kai kas 3 metus, atlikus vertinimą, rengti ataskaitas.

11. Atkūrimo grupės funkcijos:

11.1. organizuoti kompiuterių tinklo veikimo atkūrimą;

11.2. organizuoti sistemos elektroninės informacijos atkūrimą;

11.3. organizuoti taikomųjų programų tinkamo veikimo atkūrimą;

11.4. organizuoti darbo kompiuterių veikimo atkūrimą ir prijungimą prie kompiuterių tinklo;

11.5. vykdyti kitas Veiklos atkūrimo grupei pavestas funkcijas.

12. Įvykus IT elektroninės informacijos saugos incidentui patalpose, kuriose yra saugoma IS techninė ir programinė įranga atliekami šie IT veiklos atkūrimo veiksmai:

12.1. IT inžinierius apie IT elektroninės informacijos saugos incidentą nedelsdamas informuoja Mokyklos direktorių.

12.2. IT inžinierius atkuria IT techninės ir programinės įrangos veikimą, elektroninių ryšių tinklo veiklą, IS duomenis, IT techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir apie tai nedelsdamas informuoja Mokyklos direktorių.

13. IT inžinierius informuoja Mokyklos direktorių apie IT įvykusius kibernetinius incidentus, dėl kurių kilo arba galėjo kilti grėsmė Mokyklos IT duomenims, IT techninės ir programinės įrangos funkcionavimui, ir kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, jų galimas priežastis, veiksmus, kurių imasi ir (arba) planuojama imtis šalinant šiuos incidentus, bei pasekmes.

III. SKYRIUS
APRAŠOMOSIOS NUOSTATOS

14. Veiklos tęstinumo vykdymui užtikrinti naudojama detali ir aktuali informacija:

14.1. informaciją apie IT techninę ir programinė įrangą ir jos parametrus, aprašytus IT specifikacijose, saugo IT inžinierius;

14.2. patalpų brėžinius ir šiose patalpose esančios įrangos bei komunikacijų sąrašą saugo Mokyklos direktoriaus pavaduotojas infrastruktūrai;

14.3. telekomunikacijų tinklo fizinio sujungimo schemas saugo Mokyklos direktoriaus pavaduotojas infrastruktūrai;

14.4. programinės įrangos laikmenos ir laikmenos su atsarginėmis duomenų kopijomis saugomos mokyklos serverinėje. Už atsarginių kopijų saugojimą atsako mokyklos IT inžinierius.

14.5. mokyklos darbuotojų sąrašai, kuriuose nurodyti darbuotojų darbo telefonai, saugo personalo specialistas.

14.6. veiklos tęstinumo valdymo grupės ir Veiklos atkūrimo grupės narių sąrašas su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu, yra pas mokyklos sekretorę.

IV. SKYRIUS
VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

15. Valdymo plano veiksmingumas turi būti išbandomas ne rečiau kaip kartą per 3 metus.

16. Bandymo metu Veiklos tęstinumo valdymo grupė išanalizuoja galimą (sumodeliuotą) elektroninės informacijos saugos incidentą, numato galimus jo valdymo būdus ir sprendimus.

17. Išbandžius Valdymo plano veiksmingumą, valdymo grupės vadovas turi parengti Valdymo plano veiksmingumo išbandymo ataskaitą, kurioje yra apibendrinami atliktų bandymų rezultatai, akcentuojami pastebėti IT trūkumai ir pasiūlomos šių trūkumų šalinimo priemonės.

18. Parengtą ataskaitą (2 priedas) valdymo grupės vadovas pateikia Mokyklos direktoriui.

19. Valdymo plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

_____

IT sistemos veiklos tęstinumo
valdymo plano
1 priedas

INFORMACINĖS SISTEMOS VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Eil. Nr.	Įvykis, sukeliantis elektroninės	Pasekmės likvidavimo veiksmai	Atsakingi vykdytojai
1.	Gautas pranešimas apie IT saugos incidentą	❖ Pranešama mokyklos direktoriui, jo pavaduotojui infrastruktūrai. ❖ Pranešama Veiklos tęstinumo valdymo grupei. ❖ Surenkama informacija apie neveikiančias arba apgadintas IT, patalpas arba patirtą kitokią žalą.	IT inžinierius
		❖ Skelbiama ekstremalioji situacija	Mokyklos direktorius
		❖ Prireikus parengiami ir išplatinami informaciniai pranešimai darbuotojams (informaciniame pranešime turi būti pateikiamos rekomendacijos, kaip elgtis esant ekstremaliajai situacijai)	Veiklos tęstinumo valdymo grupė
		❖ Reikalui esant, informuojamos teisėsaugos institucijos	
2.	Nustatyta IT padaryta žala	❖ Parengiamas priemonių planas kilusiam pavojui užkirsti. ❖ Sudaroma Veiklos atkūrimo grupė. Atsižvelgiant į IT pažeidimus (į paskirtą grupę gali būti įtraukti ir kiti asmenys)	Veiklos tęstinumo valdymo grupė
3.	Nustatytas patalpų pažeidimas, stichinė nelaimė, gaisras ir pan. Nustatytas pavojus	❖ Darbuotojų ir mokinių evakavimas iš Mokyklos patalpų ❖ Pranešimas atitinkamoms tarnyboms	Darbuotojas, atsakingas už žmonių evakavimą mokykloje
4.	Pagrindinės kompiuterinės įrangos praradimas, nepakenkiant patalpų	❖ Parengiamas priemonių planas kilusiam pavojui užkirsti	Veiklos atkūrimo grupė
5.	Nustatytas IT techninės, programinės įrangos ir (arba) duomenų praradimas	❖ Parengiama atkūrimui būtina minimali techninė ir programinė įranga. ❖ Atkuriama techninės, programinės įrangos veikla. ❖ Atkuriami prarasti duomenys	IT inžinierius

6.	Nustatytas ryšio linijų sutrikimas, dėl kurio nustoja funkcionuoti IT	❖ Nustatomos ryšio sutrikimo priežastys. Šalinami ryšio sutrikimai. ❖ Ryšio paslaugų tiekėjas u-klausomas dėl įvykusio sutrikimo pašalinimo trukmės prognozės. ❖ Aktyvuojama rezervinė ryšio priemonė.	IT inžinierius
		❖ Pranešama atitinkamų tarnybų atsakingiems asmenims ir duomenų gavėjams	Veiklos tęstinumo valdymo grupė
7.	Sistemos veiklos sutrikdymas dėl kibernetinių atakų	❖ Nutraukti paslaugų teikimą sistemos naudotojams ir informuoti juos apie veiklos sutrikimus. ❖ Nustatyti trikdžių šaltinį	Veiklos atkūrimo grupė
		❖ Pranešti elektroninių ryšių ir informacijos saugumo incidentų tyrimo tarnyboms, suteikiant reikiamą informaciją apie įvykį.	Veiklos tęstinumo valdymo grupė
		❖ Patikrinti, ar neprarasti arba nesugadinti sistemos duomenys ❖ Pašalinti trikdžius, atkurti sistemos	Veiklos atkūrimo grupė
8.	Priežastys, kurios sukėlė ekstremaliąją situaciją, išnyksta ar yra pašalinamos, arba atkuriamas minimalus funkcionalumas	❖ Atšaukiama ekstremali situacija	Mokyklos direktorius
		❖ Užpildoma IT veiklos tęstinumo valdymo eigos ataskaita (2 priedas)	Veiklos tęstinumo valdymo grupė
		❖ Apie atšauktą ekstremalią situaciją, reikalui esant, pranešama interesų grupėms	Veiklos atkūrimo grupė

_____

IT sistemos veiklos
tęstinumo valdymo plano
2 priedas

IT SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO IŠBANDYMO ATASKAITA

_____
(veiklos tęstinumo valdymo grupės susitikimo data. Dokumento Nr.)

Veiklos tęstinumo valdymo plano išbandyme dalyvavo veiklos tęstinumo valdymo plano grupės nariai:

1. _____
2. _____
3. _____

Ekstremaliosios situacijos apibudinimas:

_____
_____
_____

Informacinės sistemos, kurias paveikė ekstremalioji situacija:

_____
_____

Ekstremaliosios situacijos valdymo eiga:

_____
_____

Rasti veiklos tęstinumo valdymo plano trūkumai:

_____
_____
_____

Pasiūlymai keisti arba papildyti veiklos tęstinumo valdymo planą:

_____
_____
_____

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)

_____
(vardas, pavardė) (parašas)

_____