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

# VILNIAUS AUTOMECHANIKOS IR VERSLO MOKYKLOS INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKA

## I. SKYRIUS
## PASKIRTIS

1. Informacijos ir kibernetinio saugumo politika (toliau – Politika) yra skirta pateikti vieningus ir veiksmingus Vilniaus automechanikos ir verslo mokyklos (toliau – Mokykla) informacijos ir kibernetinio saugumo (toliau – Saugumo) valdymo principus, vadovų poziciją informacijos ir kibernetinio saugumo atžvilgiu bei užtikrinti efektyvų Mokyklos informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.

## II. SKYRIUS
## TAIKYMO SRITIS

2. Ši Politika privaloma visiems Mokyklos darbuotojams ir taikoma Mokyklos veiklos procese, kur yra valdoma, perduodama ar kitaip tvarkoma informacija.

## III. SKYRIUS
## NUORODOS

3. **Kibernetinio saugumo įstatymas** – nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, taip pat tarp institucinį bendradarbiavimą.

4. **Kibernetinio saugumo reikalavimai taikomi ypatingos svarbos informacinei infrastruktūrai** – nustato organizacinius ir techninius kibernetinio saugumo reikalavimus ypatingos svarbos informacinės infrastruktūros valdytojams ir viešojo administravimo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius.

## IV. SKYRIUS
## POLITIKOS ĮGYVENDINIMO TIKSLAI

5. Pagrindiniai informacijos ir kibernetinio saugumo Mokykloje užtikrinimo tikslai:

5.1. Užtikrinti saugią ir patikimą informacinę ir kibernetinę aplinką;

5.2. Užtikrinti informacijos saugumą: informacijos konfidencialumą, vientisumą ir prieinamumą;

5.3. Užtikrinti veiklos tęstinumą – elektroninių ryšių tinklų, informacinių ir pramoninių procesų valdymo sistemų techninės bei programinės įrangos nepertraukiamą veiklą, incidentų valdymą ir savalaikį veiklos atstatymą;

5.4. Užtikrinti ir valdyti atitikimą, informacijos ir kibernetinį saugumą bei asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimams.

## V. SKYRIUS
## PAGRINDINIAI PRINCIPAI / ĮSIPAREIGOJIMAI

6. Mokyklos informacinės ir kibernetinės aplinkos, verslo informacinių ir darbo procesų valdymo sistemų saugumas yra užtikrinamas bei valdomas naudojant vieningą saugumo sistemą, kurią sudaro teisinės, techninės, organizacinės bei švietimo (mokymo) priemonės, parenkamos siekiant valdyti riziką ir ją sumažinti iki vadovybei priimtino rizikos lygio.

7. Mokyklos vadovai, siekdami užtikrinti informacijos ir kibernetinį saugumą, nustato šiuos informacijos ir kibernetinio saugumo valdymo principus:

7.1. kibernetinės erdvės nediskriminavimo – teisės aktų nuostatos yra taikomos, o gėriai yra saugomi vienodai tiek fizinėje, tiek kibernetinėje erdvėje;

7.2. kibernetinio saugumo rizikos valdymo – taikomos kibernetinio saugumo priemonės turi užtikrinti kibernetinio saugumo subjektų reguliariai įvertinamos rizikos suvaldymą;

7.3. kibernetinio saugumo proporcingumo – taikomos teisinės, organizacinės ir techninės kibernetinio saugumo priemonės neturi apriboti kibernetinio saugumo subjektų veiklos kibernetinėje erdvėje labiau, negu tai būtina;

7.4. viešojo intereso viršenybės – taikomos kibernetinio saugumo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje;

7.5. standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo priemones, kibernetinio saugumo subjektai skatinami vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais ryšių ir informacinių sistemų kibernetinio saugumo standartais ir specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;

7.6. subsidiarumo – už ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakingi šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai. Srityse, kurios priklauso išimtinei kibernetinio saugumo subjektų kompetencijai, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijos veiksmų imasi tik tada, kai ryšių ir informacinių sistemų ir jomis teikiamų paslaugų kibernetinio saugumo negali užtikrinti šias sistemas valdantys ir paslaugas jomis teikiantys kibernetinio saugumo subjektai.

8. Siekdami įgyvendinti nustatytus informacijos ir kibernetinio saugumo valdymo principus, Mokyklos vadovai įsipareigoja:

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

8.2. skirti išteklius, būtinus nuolat planingai gerinti saugumą užtikrinančio personalo kvalifikaciją bei įgūdžius;

8.3. suteikti kompetencijas ir įgaliojimus kompetentingiems asmenims derinti bei tvirtinti su priskirtu saugumo valdymo procesu susijusius dokumentus;

8.4. laikytis visų informacijos saugos įpareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos respublikos teisės aktuose bei sutartyse;

8.5. sudaryti sąlygas mokyklos darbuotojams tobulinti žinias informacijos saugos srityje.

## VI. SKYRIUS
## POLITIKOS ĮGYVENDINIMAS IR KONTROLĖ

9. Šios Politikos įgyvendinimo, kontrolės, organizavimo bei užtikrinimo veiksmai ir atsakomybės aprašomos Mokyklos informacijos ir kibernetinio saugumo dokumentuose.

10. Informacijos ir kibernetinio saugumo kompetentingi asmenys 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 pasiūlymus dėl šios Politikos pakeitimų poreikio.

11. Visi mokyklos darbuotojai supažindinami su šia politika skelbiant ją mokyklos svetainėje.

_____.