VILNIAUS PASLAUGŲ VERSLO PROFESINIO MOKYMO CENTRO DIREKTORIUS

ĮSAKYMAS DĖL VILNIAUS PASLAUGŲ VERSLO PROFESINIO MOKYMO CENTRO INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKOS PATVIRTINIMO

2025 m. gegužės 23 d. Nr. 1V-131
Vilnius

1. T v i r t i n u Vilniaus paslaugų verslo profesinio mokymo centro informacijos ir kibernetinio saugumo politiką (toliau vadinama – Politika) (pridedama).

2. Į p a r e i g o j u Technologijų skyriaus IT specialistą Giedrių Vaičiulį įkelti Politiką į Vilniaus paslaugų verslo profesinio mokymo centro interneto svetainę.

3. Į p a r e i g o j u mokytoją Jeleną Borisenko įkelti Politiką į Moodle sistemą.

4. N u r o d a u, kad šis įsakymas įsigalioja, kai jį elektroniniu parašu pasirašo Vilniaus paslaugų verslo profesinio mokymo centro direktorė Daiva Motiejūnaitė-Minkauskė, Darbuotojų saugos ir sveikatos valdymo sistemoje - ESAUGA.

Direktorė Daiva Motiejūnaitė-Minkauskė

PATVIRTINTA
Vilniaus paslaugų verslo profesinio
mokymo centro direktorės
2025-05-23 įsakymu Nr. 1V-131

VILNIAUS PASLAUGŲ VERSLO PROFESINIO MOKYMO CENTRO INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKA

I SKYRIUS

BENDROSIOS NUOSTATOS

1. Informacijos ir kibernetinio saugumo politika (toliau vadinama – politika) yra skirta pateikti vieningus ir veiksmingus Vilniaus paslaugų verslo profesinio mokymo centro (toliau vadinama – Centras) informacijos ir kibernetinio saugumo (toliau vadinama – Saugumo) valdymo principus, vadovų poziciją informacijos ir kibernetinio saugumo atžvilgiu bei užtikrinti efektyvų Centro informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.

2. Kibernetinio saugumo politikos tikslus, prioritetus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė, kibernetinio saugumo politika formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija, o kibernetinio saugumo politiką įgyvendina Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija ir kitos institucijos, kurių funkcijos yra susijusios su kibernetiniu saugumu.

3. Pagrindiniai teisės aktai, kuriais vadovaujantis Centre diegiamos organizacinės ir techninės duomenų saugumo priemonės: Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Baudžiamasis kodeksas, Lietuvos Respublikos Elektroninių ryšių įstatymas, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, Lietuvos Respublikos kibernetinio saugumo įstatymas, Administracinių nusižengimų kodeksas ir kt. teisės aktai.

4. Politikoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme ir kituose teisės aktuose, reguliuojančiuose kibernetinį saugumą.

II SKYRIUS

TAIKYMO SRITIS

5. Ši politika privaloma visiems Centro darbuotojams ir taikoma Centro veiklos procese, kur yra valdoma, perduodama ar kitaip tvarkoma informacija.

III SKYRIUS

POLITIKOS ĮGYVENDINIMO TIKSLAI

6. Pagrindiniai informacijos ir kibernetinio saugumo Centro užtikrinimo tikslai:

6.1.Užtikrinti saugią ir patikimą informacinę ir kibernetinę aplinką;

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

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

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

IV SKYRIUS

PAGRINDINIAI PRINCIPAI / ĮSIPAREIGOJIMAI

7. Centro 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.

8. Centras, siekdamas užtikrinti informacijos ir kibernetinį saugumą, nustato šiuos informacijos ir kibernetinio saugumo valdymo principus:

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

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

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

8.4. 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;

8.5. 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;

8.6. 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.

9. Siekdami įgyvendinti nustatytus informacijos ir kibernetinio saugumo valdymo principus, Centras įsipareigoja:

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

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

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

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

9.5. sudaryti sąlygas Centro darbuotojams tobulinti žinias informacijos saugos srityje.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

10. Šios politikos įgyvendinimo, kontrolės, organizavimo bei užtikrinimo veiksmai ir atsakomybės aprašomos Centro informacijos ir kibernetinio saugumo dokumentuose.

11. 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.

12. Visi Centro darbuotojai supažindinami su šia politika skelbiant ją Centro svetainėje.

_____.