PATVIRTINTA
Šilalės r. Kvėdarnos Kazimiero Jauniaus
gimnazijos direktoriaus
2023 m. gruodžio 13 d. įsakymu Nr. V1-119

ŠILALĖS R. KVĖDARNOS KAZIMIERO JAUNIAUS GIMNAZIJOS INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacijos ir kibernetinio saugumo politika (toliau – Politika) yra skirta pateikti vieningus ir veiksmingus Šilalės r. Kvėdarnos Kazimiero Jauniaus gimnazijos (toliau – Gimnazija) informacijos ir kibernetinio saugumo (toliau – Saugumo) valdymo reikalavimus, kuriais vadovaujantis turi būti užtikrintas tinkamas ir efektyvus informacijos ir kibernetinio saugumo valdymas, išvengta veiklos sutrikdymo bei žalos atsiradimo dėl informacijos konfidencialumo, vientisumo, prieinamumo pažeidimų bei kitų kibernetinių grėsmių.
2. Ši Politika privaloma visiems Gimnazijos darbuotojams, paslaugų tiekėjams ir taikoma Gimnazijos veiklos procesuose, kur yra užtikrinamas informacijos ir kibernetinis saugumas, valdoma ar tvarkoma informacija.

II SKYRIUS
POLITIKOS ĮGYVENDINIMO TIKSLAI

3.Pagrindiniai informacijos ir kibernetinio saugumo Gimnazijoje užtikrinimo tikslai:
3.1. Užtikrinti saugią ir patikimą informacinę ir kibernetinę aplinką;
3.2. Užtikrinti informacijos saugumą: informacijos konfidencialumą, vientisumą ir prieinamumą;
3.3. Užtikrinti veiklos tęstinumą – elektroninių ryšių tinklų, informacinių procesų valdymo sistemų techninės bei programinės įrangos nepertraukiamą veiklą, incidentų valdymą ir savalaikį veiklos atstatymą;
3.4. Užtikrinti ir valdyti atitikimą informacijos ir kibernetinį saugumą bei asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimams.

III SKYRIUS
PAGRINDINIAI PRINCIPAI

4. Gimnazijos informacinės ir kibernetinės aplinkos, informacinių ir darbo procesų valdymo sistemų saugumas yra užtikrinamas bei valdomas naudojant vieningą saugumo sistemą, kurią sudaro teisinės, techninės, organizacinės bei mokymo priemonės, parenkamos siekiant valdyti riziką ir ją sumažinti iki priimtino rizikos lygio.
5.Gimnazijos vadovai, siekdami užtikrinti informacijos ir kibernetinį saugumą, nustato šiuos informacijos ir kibernetinio saugumo valdymo principus:
5.1. kibernetinės erdvės nediskriminavimo – teisės aktų nuostatos yra taikomos, o gėriai yra saugomi vienodai tiek fizinėje, tiek kibernetinėje erdvėje;

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

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

5.4. 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;

5.5. 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;

5.6. 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.

6. Informacijos ir kibernetinio saugumo valdymo prioritetinės kryptys:

6.1.užtikrinti tinkamą ir efektyvų informacijos bei kibernetinio saugumo valdymą ir išvengti veiklos sutrikdymo dėl informacijos konfidencialumo, vientisumo bei prieinamumo pažeidimų;

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

6.3. užtikrinti atitiktį teisės aktuose nustatytiems kibernetinio ir informacijos saugumo reikalavimams;

6.4. įgyvendinti gerąją praktiką atitinkančias organizacines ir technines informacijos saugumo priemones;

6.5. užtikrinti valdomų informacinių sistemų veiklos tęstinumą;

6.6. užtikrinti efektyvų rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant suvaldyti riziką iki priimtino lygio;

6.7. sudaryti sąlygas Gimnazijos darbuotojams tobulinti žinias informacijos saugos srityje.

7. Bet koks informacijos saugumo normų pažeidimas laikomas informacijos saugumo incidentu, kuris gali daryti neigiamą įtaką Gimnazijos veiklos tęstinumui, sugadinti ir pakenkti Gimnazijos įvaizdžiui visuomenėje.

IV SKYRIUS
POLITIKOS ĮGYVENDINIMAS IR KONTROLĖ

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

9. Informacijos ir kibernetinio saugumo kompetentingi asmenys ne rečiau kaip kartą per 2 (dvejus) metus turi inicijuoti vidaus patikrinimą, siekdami nustatyti, ar ši Politika yra tinkamai įgyvendinama praktikoje, ir parengti bei pateikti pasiūlymus dėl šios Politikos pakeitimų poreikio.

10. Visi Gimnazijos darbuotojai supažindinami su šia Politika.