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

INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKA

I SKYRIUS
PASKIRTIS

1. Informacijos ir kibernetinio saugumo politika (toliau – Politika) yra skirta nustatyti Biržų Vlado Jakubėno muzikos mokyklos (toliau – Mokykla) informacijos ir kibernetinio saugumo valdymo principus bei efektyvias saugumo užtikrinimo kryptis siekiant suvaldyti kibernetinių grėsmių ir informacijos saugos rizikas bei Politikos atitikimą teisės aktams.

II SKYRIUS
TAIKYMO SRITIS

2. Ši Politika privaloma visiems Biržų Vlado Jakubėno muzikos mokyklos darbuotojams ir taikoma kiekviename veiklos procese, kuriame yra valdoma, perduodama ar kitaip tvarkoma informacija.

III SKYRIUS
PAGRINDINĖS SĄVOKOS

3. Politikoje vartojamos pagrindinės sąvokos:

3.1. **Informacija** – bet koks žinių elementas, pateiktas naudoti, saugoti, perduoti ar apdoroti tinkama forma. Informacija apima žodine, rašytine, audiovizualine, skaitmenine ar bet kokia kita forma išreikštus ir apibendrintus arba interpretuotus duomenis;

3.2. **Informacijos saugumas** – informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

3.3. **Informacinė aplinka** – asmenys, organizacijos ir sistemos, kurios renka, apdoroja arba platina informaciją.

3.4. **Informacine sistema** – programinės įrangos visuma valstybės ar savivaldybės institucijos ar įstaigos, kito viešojo administravimo subjekto, viešosios įstaigos ar valstybės valdomos įmonės veiklos procesams skaitmenizuoti, duomenims tvarkyti ir (ar) administracinėms ar viešosioms paslaugoms teikti elektroniniu būdu.

3.5. **Informaciniai ištekliai** – informacija (duomenų bazės, duomenų rinkmenos, sutartys ir kiti dokumentai); programinė įranga (taikomoji ir sisteminė programinė įranga); aparatinė įranga (duomenų laikmenos, organizacinė, kompiuterinė ir ryšių įranga); informacinių technologijų ir telekomunikacijų (toliau – ITT) funkcionavimui reikalingos paslaugos; išorės šalių teikiamos ITT paslaugos ir infrastruktūriniai ištekliai; darbuotojų kvalifikacija ir įgūdžiai.

3.6. **Kibernetine aplinka** – informacinių sistemų naudotojai, tinklai, įrenginiai, programinė įranga, perduodama arba saugoma informacija, paslaugos ir sistemos, kurios gali būti pasiekiamos elektroniniais ryšių tinklais tiesiogiai arba netiesiogiai.

3.7. **Kibernetinis incidentas** – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

3.8. **Kibernetinis saugumas** – reiškia gebėjimą kibernetinėje erdvėje apsaugoti elektroninį ryšių tinklą, informacines valdymo sistemas bei jas apginti kibernetinių atakų atveju. Tai visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, juos aptikti, analizuoti ir reaguoti į juos bei įprastinei elektroninių ryšių tinklų, informacinių ir pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.

3.9. **Konfidencialumas** – informacijos savybė, užtikrinanti jos prieinamumą tik tiems fiziniams ar juridiniams asmenims (naudotojams), kuriems tokia teisė suteikta;

3.10. **Prieinamumas** – informacijos savybė, garantuojanti informacijos ir jos prieigai būtinų išteklių prieinamumą sankcionuotam naudotojui reikiamu metu;

3.11. **Vientisumas** – informacijos savybė, nusakanti jos tikslumą ir pilnumo apsaugą bei užtikrinanti, kad informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

IV SKYRIUS
INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKOS UŽTIKRINIMO TIKSLAI, PRINCIPAI IR TAIKOMOS PRIEMONĖS

4. **Pagrindiniai informacijos ir kibernetinio saugumo užtikrinimo tikslai:**

4.1. Užtikrinti saugią ir patikimą informacinę ir kibernetinę aplinką;

4.2. Užtikrinti informacijos konfidencialumą, vientisumą ir prieinamumą;

4.3. Užtikrinti veiklos tęstinumą – t. y. elektroninių ryšių tinklų, informacinių ir veiklos procesų valdymo sistemų techninės bei programinės įrangos nepertraukiamą darbą, incidentų valdymą ir veiklos atstatymą;

4.4. Ieškoti naujų būdų ir priemonių, užtikrinančių saugumą;

4.5. Užtikrinti informacijos bei kibernetinį saugumą, asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimų vykdymą.

5. **Pagrindiniai informacijos ir kibernetinio saugumo principai:**

5.1. Darbuotojai turi tinkamai suvokti informacijos ir kibernetinio saugumo svarbą, galimą neigiamą poveikį Mokyklos veiklai, keliamų tikslų įgyvendinimui bei vadovautis gerąja praktika pagal šios Politikos 1 priedą. Nuolatos didinamas visų darbuotojų atsparumas kibernetinėms grėsmėms periodiškai organizuojant mokymus, nuolat informuojant apie aktualias grėsmes ir priemones, leidžiančias išvengti incidentų;

5.2. Svarbiausių veiklos procesų, informacijos ir kibernetinio saugumo grėsmių rizika vertinama periodiškai, bet ne rečiau kaip kartą per metus, taip pat atsiradus poreikiui (kuriant naujas ar keičiant esamas informacines sistemas ar veiklos procesus);

5.3. Užtikrinti atitiktį teisės aktuose nustatytiems informacijos ir kibernetinio saugumo reikalavimams, Mokyklos sutartiniams įsipareigojimams trečiosioms šalims, taikant rizikos vertinimu pagrįstas informacijos ir kibernetinio saugumo priemones;

5.4. Valdant informacijos saugumo ir kibernetinius incidentus, užtikrinamas reikiamas reagavimas, suvaldymas ir mokymasis iš incidentų, siekiant išvengti jų pasikartojimo ar pažeidžiamumų išnaudojimo.

6. **Taikomos priemonės:**

6.1. Žmonių saugumo priemonės. Darbuotojų kompetencijai keliami reikalavimai nustatyti darbuotojų pareigybių aprašymuose. Darbuotojų atsakomybės, įgaliojimai ir įsipareigojimai nustatyti procesų aprašuose, tvarkose bei instrukcijose;

6.2. Fizinės saugumo priemonės apima patalpų ir įrangos apsaugą nuo praradimo, sugadinimo ar vagystės. Gali būti vykdoma nuolatinė stebėsena vaizdo stebėjimo kameromis;

6.3. Techninės priemonės: techninės ir programinės įrangos saugus konfigūravimas, apsauga nuo nesaugios įrangos, išorinio įsilaužimo prevencija, pažeidžiamumų vertinimas, elektroninio pašto ir naršyklių apsauga, audito žurnalų stebėjimas ir analizė, duomenų atkūrimo galimybės ir kt.

V SKYRIUS
ĮSIPAREIGOJIMAI IR ATSAKOMYBĖS

7. Laikytis visų informacijos ir kibernetinio saugumo įsipareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartyse. Prižiūrėti ir nuolat tobulinti kibernetinio saugumo valdymo sistemos efektyvumą.

8. Skatinti ir propaguoti incidentų prevenciją užtikrinančias priemones (ne rečiau nei kartą per metus darbuotojams organizuoti informacinio ir kibernetinio saugumo mokymus, teikti nuolatines rekomendacijas informacinio ir kibernetinio saugumo klausimais) bei vystyti darbuotojų informacijos ir kibernetinio saugumo kultūrą bei kibernetinę higieną.

9. Užtikrinti efektyvų informacijos ir kibernetinio saugumo valdymo sistemos aprūpinimą reikiamais ištekliais, sudaryti sąlygas darbuotojams tobulinti žinias informacijos ir kibernetinio saugumo bei asmens duomenų saugumo srityse.

10. Bet koks informacijos ir kibernetinio saugumo normų pažeidimas laikomas kibernetinio saugumo incidentu, kuris gali daryti neigiamą įtaką veiklos tęstinumui.

11. Pastebėjus informacinių sistemų veiklos sutrikimą ar saugumo incidentą, kibernetinio saugumo spragą ar silpną vietą, nedelsiant pranešti Mokyklos informatikos specialistui.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

12. Šios Politikos įgyvendinimo, kontrolės, organizavimo bei užtikrinimo veiksmai ir atsakomybės aprašomos Mokyklos informacijos ir kibernetinio saugumo dokumentuose. Saugos įgaliotinis ne rečiau kaip 1 (vieną) kartą per metus turi inicijuoti vidaus patikrinimą, siekdamas nustatyti ar šį Politika yra tinkamai įgyvendinama praktikoje ir parengti bei pateikti pasiūlymus dėl šios Politikos pakeitimų poreikio.

_____

Biržų Vlado Jakubėno muzikos mokyklos
Informacijos ir kibernetinio saugumo politikos
1 priedas

Priemonės ir būdai, padedantys išvengti ar bent sumažinti kibernetines grėsmes ir rizikas

1. Rekomendacijos siekiant išvengti kibernetinių grėsmių:

• Nuolatos darykite atsargines dokumentų kopijas;
• Nespauskite neaiškių nuorodų ir neatidarykite įtartinų priedų elektroniniuose laiškuose;
• Programinę įrangą atnaujinkite pagal gamintojo siūlomas rekomendacijas;
• Naudokite antivirusines ar kitas programas, apsaugančias nuo kenksmingos programinės įrangos.

2. Rekomendacijos slaptažodžių sudarymui:

• Nenaudokite populiarių slaptažodžių.
Kibernetiniai įsilaužėliai, bandydami prisijungti prie paskyrų, pirmiausia išbando populiariausius slaptažodžius, pavyzdžiui: *qwerty*, *123456*, *password* ar kitus dažnai naudojamus variantus. Šie ir panašūs slaptažodžiai gali būti nulaužiami per kelias sekundes.

• Nenaudokite tų pačių slaptažodžių skirtingoms paskyroms.
Viena dažniausiai pasitaikančių ir lengvai išsprendžiamų saugumo spragų – slaptažodžių pakartotinis naudojimas. Piktavaliai neretai naudojasi slaptažodžių duomenų bazėmis iš prieš tai atliktų atakų, todėl, naudojant tą patį slaptažodį prisijungimui prie kitų paskyrų, visose šiose paskyrose padidėja pažeidžiamumo rizika.

• Slaptažodžio ilgis.
Slaptažodžio ilgis yra vienas svarbiausių saugumo faktorių.
Pavyzdžiui, užtenka mažiau nei vienos sekundės atspėti slaptažodį, jei ji sudaro tik keturi simboliai. Tuo tarpu, prireiks 10 metų, jei slaptažodis bus sudarytas iš ne mažiau kaip 10 simbolių. Specialūs simboliai (!@$%"'&*()=+[];:'",<.>/?) suteikia slaptažodžiui papildomą apsaugą.

• Slaptažodžio sudėtingumas.
Norint sukurti saugų slaptažodį, būtina įtraukti didžiąsias raides, skaičius ir simbolius (pvz. U2o^$4Ex!H). Reikėtų vengti įprastų ir mūsų aplinkoje pasitaikančių objektų: produktų pavadinimų (pvz. obuolys), vardų (pvz. jonas), pavardžių (pvz. jonaitis), naminių gyvūnėlių vardų (pvz. sargis), gimtadienių (pvz. 0716) ar vestuvių metinių datų. Siekiant sukurti lengvai atsimenamą slaptažodį, dažniausiai sukuriamas slaptažodis, kurį lengva ir nulaužti.

3. Rekomendacijos siekiant išvengti kibernetinių grėsmių naudojantis elektroniniu paštu.

Darbuotojas turi apsvarstyti, jei laiškas gautas netikėtai, kokia jo gavimo priežastis, ir atsakyti į šiuos klausimus:
• Ar siuntėjo vardas ir el. pašto adresas sutampa?
• Ar jie nekelia įtarimų?
• Ar laiškas skirtas jam?
• Ar laiško gramatika, naudojami logotipai, siuntėjo parašas nekelia įtarimo?
• Ar laiške skatinama skubiai atlikti tam tikrus veiksmus?
• Jei jūsų prašoma informacijos, apsvarstykite, kokia tai informacija. Ar tai jautri informacija (pvz. prisijungimo duomenys, asmens duomenys)?
• Ar nuoroda, kurią matote, yra logiška, suprantama ir nekelia įtarimo? Užvedę pelės rodyklę ant nuorodos, patikrinkite, koks nuorodos adresas, ar jis nekelia įtarimų.
• Ar priedų pavadinimai, logotipai, plėtiniai nekelia įtarimo?

Jei kyla įtarimas, jog gautas apgaulingas laiškas, reikia apie tai pranešti. Svarbu kurti aplinką, kurioje darbuotojai nebijotų pranešti apie padarytą klaidą.

4. Darbuotojo atmintinė kibernetinei higienai palaikyti:

• Neprijunkite nežinomų USB atmintinių prie Mokyklos kompiuterių.
• Nepalikite neužrakinto kompiuterio net trumpam palikę savo darbo vietą. Reikia įjungti automatinio kompiuterio užsirakinimo funkciją.
• Saugokite ir teisingai tvarkykite prisijungimo duomenis.
• Neklijuokite ant monitorių ir nepalikite prisijungimo duomenų kitiems matomose vietose.
• Niekam neatskleiskite savo prisijungimo duomenų.
• Nespauskite ant nuorodų el. laiškuose, ypač gautuose iš nežinomų siuntėjų.
• Neatskleiskite pašaliniams asmenims jautrios asmeninės ar Mokyklos informacijos.
• Baigę darbą, uždarykite programų langus, išjunkite kompiuterį. Nepalikite ant stalo dokumentų ir duomenų laikmenų.
• Įtarę, jog el. laiške kažką padaryti ar atskleisti prašantis bendradarbis ar vadovas gali būti ne tas, kuo dedasi, perskambinkite jam, pasitarkite su kitais bendradarbiais ar vadovu.

5. Siekiant apsaugoti jautrius duomenis, rekomenduojama:

• Nenaudoti asmeninio el. pašto paskyros darbo tikslams, kai yra siunčiama ar naudojama jautri informacija ar asmens duomenys.
• Riboti asmeninių įrenginių naudojimą vykdant su Mokyklos darbu susijusią veiklą.
• Nelaikyti jautrios su Mokyklos veikla susijusios informacijos asmeniniuose įrenginiuose (pvz. išmaniajame telefone ar USB atmintinėje) ar asmeninėse duomenų laikmenose internete (pvz. „Google Drive“, „Dropbox“ ar „OneDrive“).
• Uždrausti prie Mokyklos kompiuterių prijungti nežinomas USB laikmenas ar kitus išorinius įrenginius. Prijungus USB įrenginius, kartais prireikia tik 30 sekundžių, kad įsilaužėliai nustatytų kompiuterio prisijungimo duomenis, net jei šis yra užrakintas. Kompiuteris gali būti užkrėstas kenkėjiška programine įranga, pvz. tokia, kuri rinks informaciją ir teiks ją įsilaužėliams.
• Įpareigoti darbuotoją užtikrinti, jog būtų laikomasi Informacijos ir kibernetinio saugumo politikos reikalavimų.

_____