PATVIRTINTA
Prezidento Valdo Adamkaus gimnazijos
Direktoriaus 2023 m. sausio 2 d.
įsak.Nr.VK-12

PREZIDENTO VALDO ADAMKAUS GIMNAZIJOS KIBERNETINIO SAUGUMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Prezidento Valdo Adamkaus gimnazijos (toliau – Gimnazija) Kibernetinio saugumo taisyklės (toliau – Taisyklės) apibrėžia, kaip Gimnazijos bendruomenė – mokiniai, mokytojai, pagalbos mokiniui specialistai, darbuotojai – turėtų elgtis naudojantis Gimnazijos kompiuteriais, tinklu ir kitais skaitmeniniais įrankiais. Šios Taisyklės yra būtinos, kad būtų užtikrintas saugus ir efektyvus skaitmeninės aplinkos naudojimas, apsaugota nuo kibernetinių atakų ir išvengta nepageidaujamų incidentų.

2. Taisyklės parengtos vadovaujantis Lietuvos Respublikos Kibernetinio saugumo įstatymu ir yra būtinos visai gimnazijos bendruomenei: mokytojams, kitiems darbuotojams ir mokiniams.

II. KIBERNETINIO SAUGUMO PRINCIPAI

3. Kibernetinis saugumas grindžiamas bendraisiais teisės principais, elektroninių ryšių veiklos reguliavimo principais ir šiais kibernetinio saugumo principais:

1) kibernetinės erdvės nediskriminavimo – įstatymų ir kitų teisės aktų nuostatos ir saugomi gėriai vienodai taikomi tiek fizinėje, tiek kibernetinėje erdvėje;

2) kibernetinio saugumo proporcingumo – taikomos kibernetinio saugumo užtikrinimo priemonės negali būti griežtesnės, negu būtina kibernetiniam saugumui užtikrinti, o taikomi teisiniai, organizaciniai ir techniniai kibernetinio saugumo reikalavimai neturi apriboti kibernetinio saugumo dalyvių veiklos kibernetinėje erdvėje labiau, negu tai būtina;

3) viešojo intereso viršenybės – naudojamos kibernetinio saugumo užtikrinimo priemonės pirmiausia turi užtikrinti visuomenės viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų teisių ar neproporcingai apriboti jų laisvės kibernetinėje erdvėje.

III. KIBERNETINIO SAUGUMO TAISYKLĖS MOKYTOJAMS IR PAGALBOS MOKINIUI SPECIALISTAMS IR KITIEMS DARBUOTOJAMS

4. Šios taisyklės mokytojams ir pagalbos mokiniui specialistams ir kitiems gimnazijos darbuotojams yra skirtos užtikrinti saugų ir efektyvų informacinių technologijų naudojimą Gimnazijoje. Kiekvienas darbuotojas yra atsakingas už šių taisyklių laikymąsi.

III.I. SLAPTAŽODŽIAI IR PRIEIGOS KONTROLĖ

4.1. Sukurkite stiprius, unikalius slaptažodžius: naudokite didžiąsias ir mažąsias raides, skaičius ir specialiuosius simbolius.

4.2. Saugokite savo slaptažodžius. Neatskleiskite savo slaptažodžio kitiems, net administratoriams.

4.3. Reguliariai keiskite slaptažodžius: bent du kartus per metus arba dažniau, jei įtariate, kad jūsų slaptažodis gali būti nutekęs.

4.4. Naudokite dviejų faktorių autentifikaciją. Jei ši funkcija yra prieinama, būtinai ją įjunkite.

4.5. Nelikite prisijungus prie savo paskyros. Visada atsijunkite nuo visų paskyrų, kai baigiate darbą.

III.II. INFORMACIJOS SAUGUMAS

4.6. Saugokite savo įrenginius. Naudokite antivirusinę programinę įrangą, reguliariai atnaujinkite operacinę sistemą ir programas.

4.7. Apsaugokite savo duomenis. Reguliariai atlikite duomenų atsargines kopijas.

4.8. Būkite atsargūs su elektroniniu paštu. Neatsidarykite įtartinų laiškų, ypač tų, kuriuose prašoma pateikti asmeninius duomenis arba spustelėti nuorodas.

4.9. Nesidalinkite slapta informacija. Venkite dalintis konfidencialia informacija, pvz., mokinių duomenimis, per nesaugius kanalus.

III.III. INTERNETO NAUDOJIMAS

4.10. Naudokite internetą tik mokymosi tikslais. Venkite asmeninių reikalų tvarkymo darbo metu.

4.11. Būkite atsargūs su socialiniais tinklais. Venkite skelbti informaciją, kuri galėtų būti panaudota prieš jus ar jūsų mokinius.

4.12. Saugokitės sukčių. Neatsakykite į žinutes, kuriose prašoma pinigų arba siūlomos lengvos uždarbio galimybės.

4.13. Naudokite tik oficialias gimnazijos rekomenduotas programas ir platformas.

4.14. Mokinių asmens duomenis laikykite tik gimnazijos paskyrose ir įrenginiuose, o ne asmeniniuose kompiuteriuose ar telefonuose.

4.15. Reguliariai atnaujinkite naudojamas programas ir operacinę sistemą.

4.16. Atsijunkite nuo gimnazijos sistemų baigę darbą.

III.IV. KIBERNETINĖS SAUGOS INCIDENTŲ PRANEŠIMAS

4.17. Praneškite apie įtartinus incidentus. Jei pastebėsite bet kokį įtartiną veikimą, nedelsdami praneškite IT administratoriui.

4.18. Saugokite įrodymus. Jei įmanoma, surinkite visą informaciją apie įvykį, kuri galėtų padėti ištirti incidentą.

4.19. Visada būkite atidūs ir įtarūs bet kokiems neįprastiems įvykiams.

III.V. MOKYMAS IR MOKYMASIS

4.20. Mokykite mokinius apie kibernetinį saugumą. Įtraukite kibernetinio saugumo temas į savo pamokas.

4.21. Būkite pavyzdys mokiniams. Demonstruokite saugų elgesį internete.

4.22. Prižiūrėkite, kaip mokiniai naudojasi mokyklos kompiuteriais ar internetu.

4.23. Informuokite mokinius apie saugų elgesį internete ir spręskite incidentus, susijusius su kibernetiniu saugumu.

4.24. Reguliariai dalyvaukite mokymuose, kad būtų atnaujintos žinios apie naujausias kibernetines grėsmes ir apsaugos priemones.

4.25. Bendradarbiaukite su IT administratoriais, kad būtų užtikrintas tinkamas informacinių sistemų saugumas.

III.VI. ĮRANGOS NAUDOJIMAS

4.26. Jei pastebite technines problemas ar įtartiną veiklą, informuokite informacinių technologijų administratorių.

IV. KIBERNETINIO SAUGUMO TAISYKLĖS MOKINIAMS

5. Šios taisyklės yra skirtos padėti saugiai naudotis internetu ir gimnazijos informacinėmis sistemomis. Laikydamasis jų, apsaugosi savo ir kitų duomenis bei išvengsi nemalonių situacijų.

IV.I. ASMENINĖ APSAUGA

5.1. Nesidalykite savo slaptažodžiais nei su draugais, nei su mokytojais.

5.2. Naudokite sudėtingus slaptažodžius mokyklos paskyrose (kombinuokite raides, skaičius, simbolius).

5.3. Bent du kartus per metus pasikeisk slaptažodžius. Galite tai daryti ir dažniau, jei įtariate, kad jūsų slaptažodis gali būti atskleistas.

5.4. Atsijunkite nuo paskyrų, kai baigiate naudotis gimnazijos kompiuteriu ar įrenginiu.

IV.II. ELGESYS INTERNETE

5.5. Naršykite tik mokytojų nurodytose arba mokymuisi skirtose svetainėse.

5.6. Nesiųskite įžeidžiančių ar nepagarbių žinučių klasės draugams, mokytojams ar kitiems bendruomenės nariams.

5.7. Nekurkite ir nesidalykite netinkamu turiniu socialiniuose tinkluose.

5.8. Nesidalinkite nuotraukomis, kurios gali būti panaudotos prieš jus.

5.9. Neįsijauskite į virtualią realybę ir nepamirškite, kad ne viskas, ką matote internete, yra tiesa.

IV.III. ATSARGUMAS NAUDOJANT GIMNAZIJOS ĮRANGĄ

5.10. Neatsisiųskite failų ar programų be mokytojo leidimo.

5.11. Jei pastebite įtartiną pranešimą ar kenkėjišką turinį, nedelsdami informuokite mokytoją.

IV.IV. PRIVATUMO UŽTIKRINIMAS

5.12. Nerodykite savo asmeninių duomenų (pvz., adreso, telefono numerio) socialiniuose tinkluose ar svetainėse.

5.13. Nekelkite mokyklos įvykių ar pamokų nuotraukų be gimnazijos administracijos leidimo.

IV.V. SAUGUS NARŠYMAS

5.14. Būkite atsargūs su el. Paštu. Neatsidarykite laiškų nuo nepažįstamų siuntėjų ir nespauskite nuorodų, jei nesate tikri, kad jos saugios.

5.15. Atsisiųskite programas tik iš patikimų šaltinių. Venkite parsisiųsti programų iš neaiškių svetainių.

5.16. Naudokite antivirusinę programą. Ji apsaugos tavo kompiuterį nuo virusų ir kitų kenkėjiškų programų.

IV.VI. KIBERPATYČIOS

5.17. Būkite geri kitiems. Nepatirkite ir neprovokuokite kiberpatyčių.

5.18. Jei patiriate kiberpatyčias, kreipkitės pagalbos: pasakykite mokytojui, tėvams arba patikimam suaugusiam asmeniui.

5.19. Nesidalinkite smurtiniu turiniu. Jei matote, kad kažkas patyrinėja kiberpatyčias, praneškite apie tai.

IV.VII. GIMNAZIJOS IŠTEKLIŲ NAUDOJIMAS

5.20. Naudokite gimnazijos kompiuterius tik mokymosi tikslais. Žaidimai ir asmeniniai reikalai turi palaukti.

5.21. Saugokite gimnazijos tinklą. Nesiųskite jokio kenksmingo turinio ir nebandykite įsilaužti į kitas paskyras.

IV.VIII. KIBERNETINIO SAUGUMO TAISYKLĖS ADMINISTRACIJAI

5.22. Gimnazijos administracijai galioja tos pačios kibernetinio saugumo taisyklės, kaip ir mokytojams ir pagalbos mokiniui specialistams, o taip pat:

IV.IX. ĮRANGOS IR TINKLO APSAUGA

5.23. Užtikrinkite, kad gimnazijos tinklas būtų apsaugotas slaptažodžiais ir ugniasiene.

5.24. Reguliariai tikrinkite ir atnaujinkite antivirusines programas visuose gimnazijos įrenginiuose.

IV.X. ASMENS DUOMENŲ APSAUGA

5.25. Asmens duomenis saugokite tik apsaugotose sistemose, laikydamiesi BDAR (Bendrojo duomenų apsaugos reglamento) nuostatų.

5.26. Mokinių ir mokytojų duomenų nesaugokite laikmenose, kurios nėra apsaugotos slaptažodžiais ar šifravimu.

V. KIBERNETINIO SAUGUMO TAISYKLĖS GIMNAZIJOS INFORMACINIŲ TECHNOLOGIJŲ SISTEMŲ ADMINISTRATORIUI

6. Informacinių technologijų sistemų administratorius specialistas yra atsakingas už gimnazijos skaitmeninės infrastruktūros priežiūrą, saugumą ir funkcionalumą. Žemiau pateikiamos taisyklės ir atsakomybės:

V.I. TINKLO IR ĮRANGOS SAUGUMAS

6.1. Užtikrinkite, kad Gimnazijos tinklas būtų apsaugotas ugniasiene ir naudojamos šifravimo technologijos.

6.2. Nuolat stebėkite tinklo veiklą, kad būtų galima aptikti ir išspręsti galimas grėsmes (pvz., neautorizuotą prieigą).

6.3. Sukonfigūruokite svečių „Wi-Fi“ tinklą, kuris būtų atskirtas nuo pagrindinio Gimnazijos tinklo.

6.4. Reguliariai atnaujinkite visų Gimnazijos įrenginių operacines sistemas ir programas.

6.5. Įdiekite patikimas antivirusines programas ir užtikrinkite jų reguliarią atnaujintį.

6.6. Užtikrinkite, kad visi Gimnazijos įrenginiai būtų apsaugoti slaptažodžiais arba biometriniais užraktais.

6.7. Užtikrinkite, kad Gimnazijos asmens duomenys būtų laikomi tik apsaugotose serverių ar debesų platformose, laikantis BDAR nuostatų.

6.8. Reguliariai tikrinkite prieigos teises ir apribokite jas pagal darbuotojų vaidmenis (pvz., mokiniai neturėtų prieigos prie mokytojų dokumentų).

6.9. Organizuokite reguliarią Gimnazijos duomenų atsarginių kopijų kūrimo tvarką (mažiausiai kartą per savaitę).

6.10. Laikykite atsargines kopijas saugioje ir šifruotoje vietoje, atskiroje nuo pagrindinių sistemų.

6.11. Užtikrinkite, kad visi įrenginiai būtų tinkamai veikiantys, valykite ir tikrinkite techninę įrangą.

V.II. PASKYRŲ KŪRIMAS IR VALDYMAS

6.12. Kurkite individualias paskyras mokytojams, mokiniams ir administracijos darbuotojams, užtikrindami, kad kiekviena paskyra turėtų tik būtiną prieigą.

6.13. Reguliariai peržiūrėkite ir pašalinkite nebenaudojamas paskyras, ypač pasikeitus darbuotojams.

6.14. Stebėkite tinklo ir sistemų pokyčius, įskaitant įrangos atnaujinimus, programinės įrangos pakeitimus ir incidentų valdymą.

V.III. SLAPTAŽODŽIŲ POLITIKA:

6.15. Nustatykite Gimnazijos slaptažodžių politiką (pvz., slaptažodžių ilgis, sudėtingumas, atnaujinimo periodiškumas).

6.16. Užtikrinkite, kad slaptažodžiai nebūtų saugomi neapsaugotuose tekstiniuose failuose.

V.IX. INCIDENTŲ VALDYMAS

6.17. Sudarykite planą, kaip reaguoti į kibernetinius incidentus (pvz., virusų aptikimą, įsilaužimus, duomenų nutekėjimą).

6.18. Vykdykite reguliarius incidentų valdymo mokymus ir simuliacijas.

V.X. SISTEMŲ AUDITAS:

6.19. Kas pusmetį direktoriaus pavaduotojui ūkio reikalams vykdyti, įrenginių ir programinės įrangos saugumo auditą.

6.20. Informacinių komunikacinių sistemų specialistui nuolat stebėti mokytojų ir kitų darbuotojų pranešimus TAMO dienyne apie sistemų gedimus ir nedelsiant reaguoti. Nustatyti, ar buvo bandymų prisijungti neautorizuotai, fiksuoti, jei tokie buvo nustatyti.

VI. BAIGIAMOSIOS NUOSTATOS

7. Kibernetinis saugumas yra nuolatinis mokymosi procesas. Sekite naujienas apie kibernetines grėsmes, dalyvaukite mokymuose ir dalinkitės savo žiniomis su kitais.

8. Kiekvienas gimnazijos bendruomenės narys yra atsakingas už šių taisyklių laikymąsi. Pažeidus šias taisykles, gali būti taikomos atitinkamos disciplininės priemonės.