PATVIRTINTA
Visagino „Verdenės“ gimnazijos
direktoriaus 2025-02-11
įsakymu Nr. V-23

VISAGINO „VERDENĖS“ GIMNAZIJOS KIBERNETINIO SAUGUMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Visagino „Verdenės“ gimnazijos (toliau – gimnazija) kibernetinio saugumo tvarkos aprašas (toliau – aprašas) apibrėžia gimnazijos poziciją ir atsakomybę informacijos ir kibernetinio saugumo srityje, yra skirtas pateikti vieningus saugumo valdymo principus ir užtikrinti efektyvų gimnazijos informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.

2. Šis aprašas privalomas visiems gimnazijos darbuotojams, tiekėjams bei rangovams ir taikomas kiekviename gimnazijos veiklos procese, kur yra perduodama ar kitaip tvarkoma informacija ir valdomi procesai.

3. Pagrindinės apraše vartojamos sąvokos:

3.1. **informacija** – bet koks žinių elementas, pateiktas tinkama naudoti, saugoti, perduoti ar apdoroti 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. Kai tai tikslinga, papildomai gali būti įtraukti ir kiti kriterijai, tokie kaip atsakingumas, apskaita, autentiškumas / patikimumas, nepaneigiamumas ir privatumas;

3.3. **informacinė aplinka** – individai (naudotojai), organizacijos ir (arba) sistemos, kurios renka, apdoroja arba platina informaciją, taip pat ir pati informacija;

3.4. **informacinė sistema** – informacijos apdorojimo sistemos ir organizacijos išteklių (pačios informacijos, žmonių, techninių priemonių, finansų ir pan.) visuma, skirta informacijai apdoroti, formuoti (kurti), skleisti (siųsti ir gauti). Tai struktūrizuotas procesų ir procedūrų rinkinys, kuriame yra kaupiami duomenys, organizuojami ir perduodami vartotojui;

3.5. **informaciniai ištekliai** – informacija (duomenų bazės, duomenų rinkmenos, sutartys ir kiti dokumentai, mokymų medžiaga; programinė įranga, jos kūrimo priemonės; aparatinė įranga (duomenų laikmenos, kompiuterinė ir ryšių įranga); informacinių technologijų ir telekomunikacijų funkcionavimui reikalingos paslaugos; išorės šalių teikiamos paslaugos ir infrastruktūriniai ištekliai; darbuotojų kvalifikacija ir įgūdžiai;

3.6. **išorės šalys** – paslaugų teikėjai, partneriai, kiti asmenys, turintys ar galintys turėti prieigą prie gimnazijos informacinių išteklių;

3.7. **kibernetinė erdvė** – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija;

3.8. **kibernetinis saugumas** – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, kuriomis taip pat siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą;

3.9. **konfidencialumas** – užtikrinimas, kad bet kokia gimnazijos informacija yra pasiekiama tik įgaliotiems asmenims, kuriems ją yra būtina žinoti, ir jiems suteikta tokia prieiga. Konfidencialios informacijos pavyzdžiai: banko sąskaitų išrašai, darbuotojų ir mokinių asmeninė informacija ir kt.;

3.10. **vientisumas** – užtikrinimas, kad informacija ir duomenys yra teisingi, nėra atsitiktinai ar neteisėtai pakeisti ir sunaikinti. Duomenys dažniausiai suklastojami dėl kenkimo programinės įrangos ar neteisėto užvaldymo, techninės ar programinės įrangos gedimo;

3.11. **prieinamumas** – užtikrinimas, kad visada yra prieiga prie tam tikros informacijos, duomenų bazės ar kitų elektroninių paslaugų.

4. Kitos šiame apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme ir kituose teisės aktuose.

II SKYRIUS
ĮGYVENDINIMO TIKSLAI, PRINCIPAI IR ĮSIPAREIGOJIMAI

5. Aprašo įgyvendinimo tikslai:

5.1. užtikrinti saugią ir patikimą informacinę ir kibernetinę erdvę;

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

5.3. užtikrinti veiklos tęstinumą – elektroninių ryšių tinklų, informacinių procesų valdymo sistemų techninės bei programinės įrangos nepertraukiamą veiklą;

5.4. ieškoti naujų būdų ir priemonių, užtikrinančių saugumą, tačiau nemažinančių patogumo naudotojams;

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

6. Gimnazija, siekdama užtikrinti kibernetinį saugumą, nustato šiuos informacijos ir kibernetinio saugumo valdymo principus:

6.1. padidintas dėmesys informacijos ir kibernetinio saugumo kultūros vystymui ir palaikymui. Darbuotojai turi tinkamai suvokti informacijos ir jos saugumo svarbą, galimą neigiamą poveikį gimnazijos veiklai. Didinamas visų gimnazijos darbuotojų atsparumas kibernetinėms grėsmėms vykdant komunikaciją apie aktualias grėsmes ir priemones, leidžiančias išvengti incidentų;

6.2. užtikrinti atitiktį teisės aktuose nustatytiems informacijos ir kibernetinio saugumo reikalavimams, gimnazijos sutartiniams įsipareigojimams su trečiosiomis šalimis taikant rizikos vertinimu pagrįstas informacijos ir kibernetinio saugumo priemones;

6.3. sistemingas ir nuoseklus incidentų ir pažeidžiamumo valdymas. Valdant informacijos saugumo ir kibernetinius incidentus, užtikrinamas reikiamas reagavimas, suvaldymas ir mokymasis iš incidentų siekiant išvengti jų pasikartojimo ar pažeidžiamumo išnaudojimo.

7. Siekdama įgyvendinti nustatytus informacijos ir kibernetinio saugumo valdymo principus, gimnazija įsipareigoja:

7.1. laikytis visų kibernetinio ir informacijos saugumo įsipareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartyse ir prižiūrėti ir nuolat tobulinti informacijos saugumo valdymo sistemos efektyvumą;

7.2. skatinti ir propaguoti incidentų prevenciją užtikrinančias priemones bei vystyti gimnazijos darbuotojų informacijos saugumo kultūrą ir kibernetinį sąmoningumą;

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

III SKYRIUS
GIMNAZIJOS KIBERNETINIO SAUGUMO RIZIKOS TIPAI

8. Grėsmės internete: tai įvairūs tiesioginiai ir netiesioginiai išpuoliai, įsilaužimai, atakos. Internetinių grėsmių pavyzdžiai yra virusai, įsilaužimai, šlamšto el. laiškai, apgaulingos SMS žinutės.

9. Vidinės grėsmės: tai grėsmės kylančios dėl darbuotojų kaltės. Ji gali būti tyčinė arba atsitiktinė. Tai slaptažodžių atskleidimas, slaptos informacijos aptarimas su kolegomis, sąmoningas neskelbtinos informacijos atskleidimas.

10. Fizinės grėsmės: tai materialaus gimnazijos turto (kompiuterių, serverių, kitų įrenginių) pažeidimas arba vagystė. Fizinės grėsmės kyla dėl stichinių nelaimių, teroristinių išpuolių ar tyčinio fizinio turto sugadinimo arba vagystės.

RIZIKOS LYGIO NUSTATYMAS

Lygis	Tikimybės apibrėžimas	Pavyzdys
Aukštas	Grėsmės šaltinis yra labai motyvuotas ir pakankamai pajėgus, o kontrolės priemonės, kuriomis siekiama užkirsti kelią pažeidžiamumui, yra neveiksmingos	Neteisėtas kenkėjiškas informacijos atskleidimas, kenkimas ar sunaikinimas
Vidutinis	Grėsmės šaltinis yra motyvuotas arba pajėgus, tačiau kontrolės priemonės gali trukdyti sėkmingai pasinaudoti pažeidžiamumu	Netyčinės klaidos ir pažeidimai
Žemas	Grėsmės šaltiniui trūksta motyvacijos ar gebėjimų, o taikomos kontrolės priemonės gali užkirsti kelią pažeidžiamumui	IT sutrikimai dėl stichinių ar žmogaus sukeltų nelaimių

DAŽNIAUSIAI GALINČIOS PASITAIKYTI RIZIKOS IR JŲ LYGIS

Rizika	Rizikos lygis	Rekomendacijos
Darbuotojas paspaudė nuorodą į užkrėstą svetainę	Aukštas	Užvesti pelės žymeklį ant nuorodos ir patikrinti, ar adresas yra tikras, ar nėra gramatinių klaidų, pavadinimas yra logiškas
Darbuotojas atskleidė savo prisijungimo slaptažodį	Aukštas	Jei yra galimybė naudoti dviejų žingsnių autentifikavimą, nelaikyti slaptažodžiu atviru tekstu
Darbuotojas įdiegė kenksmingą programinę įrangą	Aukštas	Darbuotojams draudžiama savarankiškai diegti programas

Virusas pateko per atminties laikmeną	Aukštas	Nesinaudoti nepatikimomis laikmenomis, nuolat jas tikrinti su antivirusine programa
Iš vadovo gautas laiškas su neįprasta užduotimi	Aukštas	Patikrinti el. pašto dėžutės adresą, radus neatitikimų informuoti IT inžinierių
Virusas užkrėtė kompiuteryje esančius duomenys	Aukštas	Periodiškai daryti atsargines duomenų kopijas, saugoti duomenis bent dviejuose fiziškai atskirtose vietose
Interneto ryšio dingimas	Vidutinis	Informuoti IT inžinierių arba interneto tiekėją
Gimnazijos interneto svetainės nulaužimas	Vidutinis	Atlikti svetainės atnaujinimus, tikrinti SSL sertifikato galiojimą ir jį laiku pratęsti

IV SKYRIUS
KIBERNETINIO SAUGUMO RIZIKOS MAŽINIMO PRIEMONĖS GIMNAZIJOS LYGMENIU

11. Slaptažodžių politika. Įsitikinti, kad gimnazijoje yra laikomasi saugaus slaptažodžio kūrimo ir naudojimo principų.

12. Kelių žingsnių autentifikavimas. Jei yra galimybė, naudoti aukštesnio lygio apsaugos priemones, kad būtų saugiai naudojamasi savo svarbiausiomis paskyromis.

13. Antivirusinės programos. Apsaugoti gimnazijos kompiuterius ir kitus įrenginius nuo kenkimo programų ir užkrėstų dokumentų.

14. Atsarginės duomenų kopijos. Apsaugoti gimnazijos dokumentus nuo informacijos nutekėjimo, vagysčių ar kitų nelaimių.

15. Prieigos kontrolė. Atskirti ir žinoti, kokie darbuotojai gali pasiekti svarbią informaciją.

16. Išmokyti darbuotojai. Sumažinti žmogaus klaidų rizika šviečiant darbuotojus kibernetinio saugumo klausimais.

17. Automatiniai atnaujinimai. Įsitikinti, kad gimnazijos kompiuteriai turi įdiegtą naujausią programinę įrangą.

18. Darbo ir asmeninių įrenginių atskyrimas. Įsitikinti, kad darbuotojai saugiai naudojasi savo įrenginiais.

19. Ugniasienės. Sukurti saugią neutralią zoną tarp interneto ir gimnazijos.

20. Saugus bevielis tinklas. Tinkamai prižiūrėti maršrutizatorius, kad kenkėjai nepatektų į gimnazijos tinklą.

V SKYRIUS
KIBERNETINIO SAUGUMO RIZIKOS MAŽINIMO PRIEMONĖS DARBUOTOJO LYGMENIU

21. Gimnazijos įranga (kompiuteriai, planšetiniai kompiuteriai, spausdintuvai ir kt.) ir internetas gali būti naudojami tik ugdymo ar darbo tikslais.

22. Draudžiama lankytis svetainėse, kurios skatina smurtą, diskriminaciją, viešina pornografiją ar kenkėjiškas veiklas.

23. Neprijungti nežinomų USB atmintinių prie gimnazijos kompiuterių.

24. Draudžiama diegti neautorizuotą programinę įrangą ar atlikti esminius pakeitimus įrangos nustatymuose.

25. Nepalikti neužrakinto kompiuterio net trumpam palikus savo darbo vietą. Galima nustatyti automatinio užsirakinimo funkciją.

26. Saugoti ir teisingai tvarkyti prisijungimo duomenis. Niekam neatskleisti savo prisijungimo duomenų.

27. Neklijuoti ant ekranų ir nepalikti prisijungimo duomenų kitiems matomose vietose.

28. Nespausti ant nuorodų el. laiškuose, ypač gautuose iš nežinomų siuntėjų.

29. Neatskleisti pašaliniams jautrios asmeninės ar gimnazijos informacijos.

30. Baigus darbą uždaryti programų langus, išjungti kompiuterį. Nepalikti ant stalo dokumentų ir duomenų laikmenų.

31. Kibernetinių incidentų (pavyzdžiui, įsilaužimų, virusų, duomenų nutekėjimo) atveju nedelsiant informuoti gimnazijos direktorių ir IT inžinierių.

VI SKYRIUS

BAIGIAMOSIOS NUOSTATOS

32. Aprašas yra skelbiamas gimnazijos interneto svetainėje.

33. Gimnazijos IT inžinierius reguliariai tikrina sistemų saugumą ir rengia rekomendacijas, kaip sumažinti kibernetines grėsmes.

34. Šio aprašo nuostatos įgyvendinamos priimant gimnazijos vidaus teisės aktus, derančius su strateginiais tikslais, teisiniais reikalavimais, tarptautiniais informacijos saugumo standartais ir gerosiomis praktikomis.

_____