PATVIRTINTA
Druskininkų „Ryto“ gimnazijos
direktoriaus 2026 m. kovo 18 d.
įsakymu Nr. VE1-114

DRUSKININKŲ „RYTO“ GIMNAZIJOS KIBERNETINIO SAUGUMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Druskininkų „Ryto“ gimnazijos (toliau – Gimnazija) kibernetinio saugumo aprašas (toliau – Aprašas) apibrėžia įstaigos poziciją ir atsakomybę informacijos ir kibernetinio saugumo srityje. Aprašas skirtas pateikti vieningus saugumo valdymo principus bei užtikrinti efektyvų Gimnazijos informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.

2. Aprašas parengtas vadovaujantis Lietuvos Respublikos Kibernetinio saugumo įstatymu ir privalomas visiems darbuotojams, tiekėjams bei rangovams. Taikomas kiekviename Gimnazijos veiklos procese, kur yra valdoma, perduodama ar kitaip tvarkoma ir valdoma informacija ir procesai.

3. Pagrindinės šiame Apraše vartojamos sąvokos:

3.1. Informacija – bet koks žinių elementas, pateiktas tinkamai 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, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą;

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

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.

II SKYRIUS
ĮGYVENDINIMO TIKSLAI, PRICINPAI IR ĮSIPAREIGOJIMAI

4. Aprašo tikslai:

4.1. užtikrinti saugią ir patikimą informacinę ir kibernetinę erdvę;

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

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

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

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

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

5.1. 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;

5.2. 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;

5.3. 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 pažeidžiamumų išnaudojimo.

6. Siekdama įgyvendinti nustatytus informacijos ir kibernetinio saugumo valdymo principus, Gimnazija įsipareigoja:

6.1. 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;

6.2. skatinti ir propaguoti incidentų prevenciją užtikrinančias priemones bei vystyti Gimnazijos darbuotojų informacijos saugumo kultūrą ir kibernetinę higieną (sąmoningumą);

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

III SKYRIUS
GIMNAZIJOS KIBERNETINIO SAUGUMO RIZIKOS TIPAI

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

8. 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.

9. 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.

10. 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.

11. Dažniausiai galinčios pasitaikyti rizikos ir jų lygis.

Rizika	**Rizikos lygis**	**Rekomendacijos**
Darbuotojas paspaudė nuorodą į užkrėstą svetainę.	Aukštas	Užvesti pelės žymeklį ant nuorodas ir patikrinti ar adresas yra tikras, ar nėra gramatinių klaidų, pavadinimas yra logiškas. Tikrinti svetainės adreso tikrumą svetainėje https://www.urlvoid.com/
Darbuotojas atskleidė savo prisijungimo slaptažodį.	Aukštas	Jei yra galimybė naudoti dviejų žingsnių autentifikavimą, nelaikyti slaptažodžių atviru tekstu. Pranešti informacinių technologijų sistemų administratoriui, kad užblokuotų prieigą prie paskyros (jei yra galimybė).
Darbuotojas įdiegė kenksmingą programinę įrangą.	Aukštas	Darbuotojams draudžiama savarankiškai diegti programas. Informuoti informacinių technologijų sistemų administratorių.
Virusas pateko per atminties laikmeną.	Aukštas	Nesinaudoti nepatikimomis laikmenomis, nuolat jas tikrinti su antivirusinę programa. Netikrinti ir juo labiau nenaudoti išorinių laikmenų, kurias randate pamestas arba paliktas.
Iš vadovo gautas laiškas su neįprasta užduotimi.	Aukštas	Patikrinti el. pašto dėžutės adresą, radus neatitikimų informuoti informacinių technologijų sistemų administratorių.
Virusas užkrėtė kompiuteryje esančius duomenys.	Aukštas	Iškart informuoti informacinių technologijų sistemų administratorių. Išjungti interneto ryšį. Neatidarinėti jokios jautrios informacijos, ypatingai kur reikalaujama suvesti prisijungimo duomenis. Periodiškai daryti atsargines duomenų kopijas, saugoti duomenis bent dviejuose fiziškai atskirtuose vietose (kompiuteris, debesis).
Interneto ryšio dingimas.	Vidutinis	Informuoti informacinių technologijų sistemų administratorių arba interneto tiekėją.
Mokyklos interneto svetainės nulaužimas.	Vidutinis	Atlikti svetainės atnaujinimus, tikrinti SSL sertifikato galiojimą ir jį laiku pratęsti. Daryti WEB serverių atnaujinimus. Tikrinti internetinio puslapio pažeidžiamumus su diagnostikos įrankiais – klaidas taisyti.

IV SKYRIUS
GIMNAZIJOS KIBERNETINIO SAUGUMO RIZIKOS MAŽINIMO PRIEMONĖS

12. Informacinių technologijų sistemų administratorius (toliau – IT administratorius) yra atsakingas už mokyklos IT infrastruktūros priežiūrą, saugumą ir funkcionalumą.

13. IT administratorius:

13.1. užtikrina, kad Gimnazijos interneto tinklas būtų apsaugotas ugniasiene, būtų naudojama licencijuota antivirusinė programinė įranga, naudojamos šifravimo technologijos;

13.2. reguliariai atlieka IT technikos (kompiuterių ir kt. įrangos), sistemų ir infrastruktūros atnaujinimus ir sistemos patikrinimus;

13.3. užtikrina, kad visi Gimnazijos įrenginiai būtų apsaugoti slaptažodžiais arba biometriniais užraktais;

13.4. užtikrinti, kad Gimnazijos darbuotojų ir mokinių asmens duomenys būtų laikomi tik apsaugotose serverių ar debesų platformose, laikantis BDAR nuostatų;

13.5. reguliariai tikrina prieigos teises ir apriboja jas pagal darbuotojų vaidmenis (jei tokios sistemos naudojamos);

13.6. nuolat stebi tinklo ir sistemų pokyčius, įskaitant įrangos atnaujinimus, programinės įrangos pakeitimus ir incidentų valdymą, kad būtų galima aptikti ir išspręsti galimas grėsmes (pvz., neautorizuotą prieigą).

14. Prieiga prie mokyklos IT sistemų suteikiama tik autorizuotiems naudotojams.

15. Kiekvienas bendruomenės narys privalo turėti asmeninį prisijungimo vardą ir stiprų slaptažodį.

16. Slaptažodžiai turi būti pakeisti po kibernetinio incidento.

17. Prieiga prie svarbios informacijos ribojama pagal naudotojo teises ir pareigas.

18. Gimnazijoje darbuotojai gali naudoti gimnazijos IT įrangą, internetą tik ugdymo ar darbo tikslais.

19. Slaptažodžiai ir prieigos kontrolė. Darbuotojai privalo:

19.1. susikurti tik stiprius, unikalius slaptažodžius: naudoti didžiąsias ir mažąsias raides, skaičius, specialiuosius simbolius, slaptažodį turi sudaryti ne mažiau kaip 12 simbolių.

19.2. saugoti savo slaptažodžius, neatskleisti savo slaptažodžio kitiems ir niekam neleiskite naudotis savo prisijungimo prie sistemų vardu;

19.3. reguliariai keisti slaptažodžius: bent du kartus per metus arba dažniau, jei įtaria, kad slaptažodis galėjo būti atskleistas;

19.4. kur įmanoma, naudoti dviejų faktorių autentifikaciją.

20. Informacijos saugumas. Darbuotojai privalo:

20.1. saugoti savo įrenginius, naudoti antivirusinę programinę įrangą, reguliariai atnaujinti operacinę sistemą ir programas;

20.2. apsaugoti savo duomenis, reguliariai daryti duomenų atsargines kopijas į asmenines debesų saugyklas arba išorines laikmenas;

20.3. neatidarinėti įtartinų el. laiškų, ypač tų, kuriuose prašoma pateikti asmeninius duomenis arba spustelėti nuorodas;

20.4. nesidalinti slapta informacija, nesidalinti konfidencialia informacija, pvz., mokinių duomenimis per nesaugius kanalus;

20.5. mokinių ir darbuotojų asmens duomenis laikyti tik gimnazijos paskyrose ir įrenginiuose, laikydamiesi BDAR (Bendrojo duomenų apsaugos reglamento) nuostatų, o ne asmeniniuose kompiuteriuose ar telefonuose;

20.6. nepalikti neužrakinto kompiuterio net trumpam palikus savo darbo vietą;

20.7. baigus darbą, atsijungti nuo visų paskyrų ir išjungti įrangą.

21. Darbuotojui draudžiama:

21.1. mokinių ir darbuotojų duomenis saugoti laikmenose, kurios nėra apsaugotos slaptažodžiais ar šifravimu;

21.2. palikti prisijungimo duomenis kitiems matomose vietose;

21.3. bandyti prisijungti prie kitų asmenų paskyrų ar neleistinai keisti duomenis;

21.4. lankytis svetainėse, kuriose pateikiama pornografinė, smurtinė, terorizmą bei kitokią nusikalstamą veiklą skatinanti informacija ar kurios susijusios diskriminuojančiu, nepadoriu, įžeidžiančiu, skatinančiu neapykantą ar kitu nepageidaujamu turiniu, taip pat platinti tokią informaciją;

21.5. talpinti interneto komentarus, pasiūlymus, bei kitus duomenis, susijusius su diskriminuojančiu, nepadoriu, įžeidžiančiu, kurstančiu neapykantą ar kitu nepageidaujamu turiniu;

21.6. savavališkai ar savarankiškai keisti jam priskirtos įrangos konfigūraciją, šalinti įrangos gedimus;

21.7. prijungti nežinomas USB atmintines ar kitus įrenginius prie Gimnazijos kompiuterių;

21.8. priskirtoje įrangoje naudoti, diegti nelicencijuotą programinę įrangą;

21.9. leisti naudoti jam priskirtą įrangą pašaliniams asmenims;

21.10. išnešti įrangą iš gimnazijos teritorijos nesuderinus su savo tiesioginiu vadovu. Šis draudimas netaikomas IT administratoriui.

22. Pastebėjus IT technikos gedimus, kibernetines patyčias, įtartiną veiklą ar kt. saugumo problemas privaloma:

22.1. nedelsiant informuoti IT administratorių ar tiesioginį vadovą;

22.2. saugoti įrodymus. Jei įmanoma, apie įvykį surinkti visą informaciją, kuri galėtų padėti ištirti incidentą.

23. Darbuotojai turi reguliariai dalyvauti mokymuose, kad būtų atnaujintos žinios apie naujausias kibernetines grėsmes ir apsaugos priemones.

V SKYRIUS
KIBERNETINIO SAUGUMO IR IT ĮRANGOS NAUDOJIMO TAISYKLĖS MOKINIAMS

24. Gimnazijoje mokiniai naudoja gimnazijos IT įrangą ir internetą tik mokymosi tikslais. Draudžiama diegti ir žaisti žaidimus, naudoti kompiuterius kitiems asmeniniams reikalams.

25. Asmeninė apsauga:

25.1. nesidalinkite savo slaptažodžiais nei su draugais, nei su mokytojais;

25.2. naudokite sudėtingus slaptažodžius Gimnazijos paskyrose (kombinuokite raides, skaičius, simbolius);

25.3. atsijunkite nuo paskyrų, kai baigiate naudotis Gimnazijos kompiuteriu ar kitu įrenginiu.

26. Elgesys internete:

26.1. naršykite tik mokytojų nurodytose arba mokymuisi skirtose svetainėse;

26.2. nesiųskite įžeidžiančių ar nepagarbių žinučių klasės draugams, mokytojams ar kitiems bendruomenės nariams;

26.3. nekurkite ir nesidalykite netinkamu turiniu socialiniuose tinkluose;

26.4. nesidalinkite nuotraukomis, kurios gali būti panaudotos prieš jus;

26.5. nepamirškite, kad ne viskas, ką matote internete, yra tiesa;

27. Atsargumas naudojantis gimnazijos IT įranga:

27.1. nesisiųskite failų ar programų be mokytojo leidimo;

27.2. jei pastebite įtartiną pranešimą ar kenkėjišką turinį, nedelsdami informuokite mokytoją.

28. Privatumo užtikrinimas:

28.1. neskelbkite savo asmeninių duomenų (pvz., adreso, telefono numerio) socialiniuose tinkluose ar svetainėse;

28.2. nekelkite mokyklos įvykių ar pamokų nuotraukų į socialinius tinklus bei kitas dalijimosi turiniu interneto platformas be mokytojo arba mokyklos administracijos leidimo.

29. Saugus naršymas internete:

29.1. būkite atsargūs su el. paštu. Neatidarinėkite laiškų nuo nepažįstamų siuntėjų ir nespauskite nuorodų, jei nesate tikri, kad jos saugios;

29.2. atsisiųskite programas tik iš patikimų šaltinių. Venkite siųstis programas iš neaiškių svetainių.

30. Kibernetinės patyčios:

30.1. elkitės gražiai, etiškai, būkite tolerantiški ir mandagūs, nepatirkite ir neprovokuokite kibernetinių patyčių;

30.2. jei patiriate kibernetines patyčias, kreipkitės pagalbos: pasakykite mokytojui, socialiniam pedagogui, tėvams arba Gimnazijos vadovams;

30.3. nesidalinkite smurtiniu turiniu. Jei matote, kad kažkas patiria kibernetines patyčias, praneškite apie tai mokytojui, socialiniam pedagogui, tėvams arba Gimnazijos vadovams.

VI SKYRIUS
KIBERNETINIŲ INCIDENTŲ VALDYMAS

31. Kibernetinių incidentų (pavyzdžiui, įsilaužimų, virusų, duomenų nutekėjimo) atveju, nedelsiant turi būti informuojami Gimnazijos vadovai ir IT administratorius.

32. Incidentų valdymo procedūros:

32.1. incidento identifikavimas ir grėsmės izoliavimas;

32.2. paveiktų sistemų ir duomenų atkūrimas naudojant atsargines kopijas;

32.3. suinteresuotų šalių, įstaigų ar asmenų informavimas apie incidentą (jei būtina pranešti kibernetinio saugumo centrui apie įvykdyta incidentą arba ataką);

32.4. ataskaitos apie incidentą parengimas ir prevencinių priemonių įgyvendinimas, kad incidentai nesikartotų.

33. Kiekvienas bendruomenės narys privalo laikytis Gimnazijos nustatytų procedūrų ir operatyviai bendradarbiauti valdant incidentus.

34. IT administratorius reguliariai tikrina sistemų saugumą, kad sumažinti kibernetines grėsmes.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

35. Atsakomybė:

35.1. kiekvienas Gimnazijos bendruomenės narys yra atsakingas už šio Aprašo nuostatų laikymąsi;

35.2. pedagogai užtikrina ugdymo proceso metu mokinių saugų elgesį internete ir atsakingą kompiuterinės technikos naudojimą;

35.3. darbuotojams ir mokiniams, pažeidusiems taisykles, taikomos drausminės priemonės, įskaitant prieigos prie Gimnazijos IT įrangos ar tinklo ribojimas;

35.4. apie taisyklių pažeidimus informuojami Gimnazijos vadovai, mokinio tėvai (globėjai, rūpintojai);

35.5. bet kokia tyčinė įrangos ar tinklo žala gali lemti drausmines priemones, mokinio / mokinio tėvų (globėjų, rūpintojų) atsakomybę už sugadintą turtą.

36. Gimnazijos darbuotojai su Aprašu supažindinami DVS Kontora priemonėmis, metų eigoje naujai priimami darbuotojai su Aprašu susipažįsta Gimnazijos interneto svetainėje.

37. Mokinius ir mokinių tėvus (globėjus, rūpintojus) su mokinių kibernetinio saugumo taisyklėmis supažindina klasių auklėtojai.

38. Aprašas gali būti atnaujinamas ar keičiamas pasikeitus teisės aktams.
