

PATVIRTINTA

Druskininkų savivaldybės Viečiūnų progimnazijos
direktoriaus 2026 m. vasario 26 d. įsakymu Nr. V1-17

DRUSKININKŲ SAVIVALDYBĖS VIEČIŪNŲ PROGIMNAZIJOS INFORMACIJOS IR KIBERNETINIO SAUGUMO TVARKOS APRAŠAS

I SKYRIUS BENDROSIOS NUOSTATOS

1. Druskininkų savivaldybės Viečiūnų progimnazijos informacijos ir kibernetinio saugumo tvarkos aprašas (toliau – Aprašas) apibrėžia Druskininkų savivaldybės Viečiūnų progimnazijos (toliau – Progimnazija) poziciją ir atsakomybę informacijos ir kibernetinio saugumo srityje. Aprašas yra skirtas pateikti vieningus saugumo valdymo principus bei užtikrinti efektyvų Progimnazijos informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.

2. Šis Aprašas privalomas visiems Progimnazijos darbuotojams, mokiniams, mokinių tėvams (globėjams, rūpintojams), tiekėjams bei rangovams. Aprašas taikomas kiekviename Progimnazijos veiklos procese, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, valdomi procesai.

3. Kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, šių institucijų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas, taip pat tarpinstitucinį bendradarbiavimą nustato Lietuvos Respublikos kibernetinio saugumo įstatymas.

4. Pagrindinės šio Aprašo sąvokos:

4.1. **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.

4.2. **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.

4.3. **Informacinė aplinka** – individai (naudotojai), organizacijos ir/arba sistemos, kurios renka, apdoroja arba platina informaciją. Taip pat, ir pati informacija.

4.4. **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.

4.5. **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.

4.6. **Išorės šalis** – paslaugų teikėjai, partneriai, kiti asmenys, turintys ar galintys turėti prieigą prie Gimnazijos informacinių išteklių.

4.7. **Kibernetinė erdvė** – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriamą ir (arba) jais perduodama elektroninė informacija.

4.8. **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.

4.9. **Konfidencialumas** – užtikrinimas, kad bet kokia Įstaigos informacija yra pasiekama tik įgaliojtiems asmenims, kuriems yra būtina žinoti, ir jiems suteikta tokia prieiga. Konfidencialios informacijos pavyzdžiai: banko sąskaitų išrašai, darbuotojų ir mokinių asmeninė informacija.

4.10. **Vientisumas** – užtikrinimas, kad informacija ir duomenys yra teisingi, nėra atsitiktinai ar neteisėtai pakeisti ir sunaikinti. Duomenys dažniausiai suklaidojami dėl kenkimo programinės įrangos ar neteisėto užvaldymo, techninės ar programinės įrangos gedimo.

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

II SKYRIUS ĮGYVENDINIMO TIKSLAI, PRINCIPAI IR ĮSIPAREIGOJIMAI

5. 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 tinklą, informacinių ir pramoninių 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. Progimnazija, siekdama užtikrinti informacijos ir 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 Progimnazijos veiklai. Didinamas visų Progimnazijos 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, Progimnazijos sutartiniais įsipareigojimams su trečiosiomis šalimis, taikant rizikos vertinimu pagrįstas informacijos ir kibernetinio saugumo priemones;

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

7. Siekdama įgyvendinti nustatytus informacijos ir kibernetinio saugumo valdymo principus, Progimnazija 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 Progimnazijos darbuotojų informacijos saugumo kultūrą ir kibernetinę higieną (sąmoningumą);

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

III SKYRIUS KIBERNETINIO SAUGUMO RIZIKOS VERTINIMAS

8. Kibernetinio saugumo rizikos vertinimas leidžia nustatyti rizikos grėsmes bei jų lygį Progimnazijoje. Vadovaujantis rizikos mažinimo priemonėmis galima sumažinti kibernetinių atakų skaičių arba jų poveikį Progimnazijai.

9. Už kibernetinio saugumo rizikos vertinimą ir priemonių plano joms mažinti parengimą atsakingas Progimnazijos direktoriaus įsakymu paskirtas Progimnazijos inžinierius programuotojas.

PIRMASIS SKIRSNIS

KIBERNETINIO SAUGUMO RIZIKOS TIPAI PROGIMNAZIJOJE

10. Kibernetinio saugumo rizikos tipai Progimnazijoje:

10.1. Grėsmės internete. Tai įvairūs tiesioginiai ir netiesioginiai išpuoliai, įsilaužimai, atakos. Internetinių grėsmių pavyzdžiai yra virusai, įsilaužimai, šlamšto el. laišakai, apgaulingos SMS žinutės;

10.2. 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;

10.3. Fizinės grėsmės. Tai materialaus Progimnazijos turto (kompiuterių, serverių, kitų įrenginių) pažeidimas arba vagystė. Fizinės grėsmės kyla dėl stichinių nelaimių, teroristinių išpuolių ar tyčinio fizinio turto sugadinimo arba vagystės.

ANTRASIS SKIRSNIS

KIBERNETINIO SAUGUMO RIZIKOS LYGIAI PROGIMNAZIJOJE

11. Kibernetinio saugumo rizikos lygiai Progimnazijoje:

Rizikos 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

12. Dažniausiai galinčios pasitaikyti rizikos ir jų lygis:

Rizika	Rizikos lygis	Rekomendacijos
Svarbios įrangos fizinis pažeidimas arba vagystė	Žemas	Įranga laikyti saugiai, rakiname kabinete su ribota pašalinių asmenų patekimo galimybe
Mokyklos interneto svetainės nulaužimas	Vidutinis	Atlikti svetainės atnaujinimus, tikrinti SSL sertifikato galiojimą ir jį laiku pratęsti
Interneto ryšio dingimas	Vidutinis	Informuoti Progimnazijos inžinierių programuotoją arba interneto tiekėją. Kol ryšis atkuriamas pasinaudoti mobiliojo telefono saitviete (hot-spot)
Iš vadovo gautas laiškas su neįprasta užduotimi	Aukštas	Patikrinti el. pašto dėžutės adresą, radus neatitikimų informuoti Progimnazijos inžinierių programuotoją
Virusas pateko per atminties laikmeną	Aukštas	Nesinaudoti nepatikimomis laikmenomis, nuolat jas tikrinti su antivirusine programa
Virusas užkrėtė kompiuteryje esančius duomenis	Aukštas	Periodiškai daryti atsargines duomenų kopijas, saugoti duomenis bent dviejuose fiziškai atskirtuose vietose

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
Darbuotojas atskleidė savo prisijungimo slaptažodį	Aukštas	Jei yra galimybė naudoti dviejų žingsnių autentifikavimą, nelaikyti slaptažodžių atviru tekstu, lengvai pasiekiamoje, matomoje vietoje
Darbuotojas įdiegė kenksmingą programinę įrangą	Aukštas	Darbuotojams draudžiama savarankiškai diegti programas

TREČIASIS SKIRSNIS

KIBERNETINIO SAUGUMO RIZIKOS MAŽINIMO PRIEMONĖS PROGIMNAZIJOS LYGMENIU

13. Kibernetinio saugumo rizikos mažinimo priemonės progimnazijos lygmeniu:

13.1. Slaptažodžių politika. Įsitikinti, kad Progimnazijoje yra laikomasi saugaus slaptažodžio kūrimo ir naudojimo principų. Visi Progimnazijos darbuotojai ir mokiniai turi naudoti saugius, sudėtingus slaptažodžius, kuriuos reikia reguliariai keisti;

13.2. Kelių žingsnių autentifikavimas. Jei yra galimybė, naudoti aukštesnio lygio apsaugos priemones, kad būtų saugiai naudojamas savo svarbiausiomis paskyromis;

13.3. Antivirusinės programos. Apsaugoti Progimnazijos kompiuterius ir kitus įrenginius nuo kenkimo programų ir užkrėstų dokumentų;

13.4. Atsarginės duomenų kopijos. Apsaugoti Progimnazijos dokumentus nuo informacijos nutekėjimo, vagysčių ar kitų nelaimių. Svarbi Progimnazijos informacija turi būti reguliariai kopijuojama į saugias laikmenas ar debesų saugyklas, kad būtų išvengta duomenų praradimo;

13.5. Prieigos kontrolė. Prieiga prie jautrios informacijos, tokios kaip mokinių pažymiai ar administraciniai dokumentai, turi būti suteikiama tik tiems darbuotojams, kuriems tai būtina pagal pareigas;

13.6. Apmokyti darbuotojai. Progimnazijoje turi būti organizuojami mokymai apie kibernetinį saugumą, siekiant sumažinti riziką dėl žmogiškųjų klaidų;

13.7. Automatiniai atnaujinimai. Įsitikinti, kad Progimnazijos kompiuteriai turi įdiegtą naujausią programinę įrangą;

13.8. Darbo ir asmeninių įrenginių atskyrimas. Darbuotojai turi naudoti Progimnazijos įrenginius tik darbo reikalam, o asmeninius – tik asmeniniams tikslams, laikantis saugumo reikalavimų;

13.9. Ugniasienės. Progimnazijos tinklas turi būti apsaugotas ugniasienėmis, kurios padeda apsisaugoti nuo išorinių kibernetinių grėsmių;

13.10. Saugus bevielis tinklas. Maršrutizatoriai turi būti tinkamai sukonfigūruoti ir apsaugoti, kad neautorizuoti naudotojai negalėtų prisijungti prie Progimnazijos tinklo;

13.11. Prisijungimas prie Progimnazijos informacinių sistemų nuotoliniu būdu turi vykti naudojant saugius duomenų perdavimo protokolus, tokius kaip VPN, HTTPS ar SSL.

KETVIRTASIS SKIRSNIS

KIBERNETINIO SAUGUMO RIZIKOS MAŽINIMO PRIEMONĖS DARBUOTOJO LYGMENIU

14. Kibernetinio saugumo rizikos mažinimo priemonės darbuotojo lygmeniu:

14.1. neprijungti nežinomų USB atmintinių prie Progimnazijos kompiuterių;

14.2. nepalikti neužrakinto kompiuterio net trumpam – naudoti automatinio užsirakinimo funkciją;

14.3. prisijungti prie sistemų tik naudojant savo asmeninį identifikatorių ir slaptažodį;

14.4. slaptažodžius laikyti saugiai – neklijuoti jų ant ekranų ir nepalikti matomose vietose;

- 14.5. niekam neatskleisti savo prisijungimo duomenų;
- 14.6. kilus abejonių dėl slaptažodžio saugumo, kreiptis į Progimnazijos inžinierių programuotoją;
- 14.7. nespausti nuorodų el. laiškuose, ypač gautuose iš nežinomų siuntėjų;
- 14.8. neatskleisti pašaliniam jautrios asmeninės ar Progimnazijos informacijos;
- 14.9. baigus darbą, užverti programų langus, išjungti kompiuterį, nepalikti dokumentų ar duomenų laikmenų ant stalo;
- 14.10. naudotis internetu, el. paštu ir kitais ištekliais tik tiesioginiam darbui;
- 14.11. nedaryti savavališkų pakeitimų kompiuterinėje technikoje ar programinėje įrangoje;
- 14.12. neįdiegti, nepapildyti ir neištrinti programinės įrangos be leidimo;
- 14.13. nenaudoti nepatvirtintos programinės įrangos iš informacinių laikmenų ar interneto;
- 14.14. neardyti kompiuterinės technikos ir nekeisti jos komplektacijos;
- 14.15. nesiųsti internetu, el. paštu ar kitais būdais garso, vaizdo ir kitų bylų, nesusijusių su tiesioginiu darbu.

IV SKYRIUS

BAIGIAMOSIOS NUOSTATOS

- 15. Aprašas tvirtinamas, keičiamas ar naikinamas Progimnazijos direktoriaus įsakymu.
 - 16. Aprašą rengia, reguliariai peržiūri ir atnauja Progimnazijos direktoriaus įsakymu paskirtas Progimnazijos inžinierius programuotojas.
 - 17. Aprašas yra skelbiamas Progimnazijos interneto svetainėje www.vieciunai.lt ir prieinamas visoms suinteresuotoms šalims.
 - 18. Šio Aprašo nuostatos įgyvendinamos priimant Progimnazijos vidaus teisės aktus, derančius su strateginiais tikslais, teisiniais reikalavimais, tarptautiniais informacijos saugumo standartais ir gerosiomis praktikomis.
-