

PATVIRTINTA

Šiaulių dailės mokyklos direktoriaus 2024 m.  
sausio 30 d. įsakymu Nr. V-15

## ŠIAULIŲ DAILĖS MOKYKLOS INFORMACINIŲ TECHNOLOGIJŲ (IT) SAUGUMO TVARKOS APRAŠAS

### I SKYRIUS BENDROSIOS NUOSTATOS

1. Informacinių technologijų (IT) saugumo tvarkos aprašo (toliau – Aprašas) tikslas – užtikrinti tinkamą ir efektyvų informacijos saugumo valdymą Šiaulių dailės mokykloje (toliau – Mokykla) ir išvengti veiklos sutrikdymo bei žalos atsiradimo dėl informacijos konfidencialumo, vientisumo bei prieinamumo pažeidimų.

2. Aprašas parengtas vadovaujantis Valstybinės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio aprašo ir Valstybinės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ su visais pakeitimais ir papildymais, Europos Sąjungos ir Lietuvos Respublikos teisės aktais, reglamentuojančiais Informacijos saugumą ir asmens duomenų tvarkymą, įskaitant Bendrąjį duomenų apsaugos reglamentą (ES) 2016/679, 2019 m. gruodžio 18 d. Valstybinės duomenų apsaugos inspekcijos gairėmis „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“, 2020 m. lapkričio 26 d. Lietuvos banko valdybos nutarimu Nr. 03-174 „Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašo patvirtinimo“ su visais pakeitimais ir papildymais.

3. Informacijos saugumo valdymas Mokykloje yra svarstomas ir tikslinamas pagal organizacinę struktūrą, funkcijas ir atsakomybę, veiklos strategiją ir tikslus, pajėgumus ir išteklius, informacijos sistemas ir procesus.

4. Aprašas galioja visiems Mokyklos darbuotojams.

### II SKYRIUS PAGRINDINĖS SAŲOKOS IR TERMINAI

5. Atsakingi asmenys – tai už Mokyklos informacinių technologijų (IT) sistemų priežiūrą Mokyklos direktoriaus įsakymu paskirti darbuotojai, kurie yra atsakingi už jų pareigybės aprašymuose nurodytas funkcijas.

6. Informacinė sistema – duomenų surinkimo, apdorojimo, perdavimo ir naudojimo sistema.

7. Kompiuterinė įranga – kompiuterių technikos fizinių priemonių visuma, t. y. mechaniniai, magnetiniai, elektriniai, elektroniniai įrenginiai ir įtaisai. Kompiuterinei įrangai priskiriama ne tik kompiuteris, bet ir visi išoriniai įrenginiai bei ryšio priemonės: monitorius, klaviatūra, pelė, spausdintuvas, garsiakalbiai, maitinimo įtaisas, kabeliai, jungtys ir pan.

8. Konfidencialumas – užtikrinimas, kad informacija būtų prieinama tik įgaliotiems asmenims, turintiems prieigos prie informacinių sistemų teises.

9. Prieinamumas – užtikrinimas, kad įgaliotieji vartotojai, kai būtina, turėtų prieigą prie informacinių ir bendrų išteklių.

10. Vientisumas – informacijos ir apdorojimo metodų tikslumo ir išbaigtumo užtikrinimas.

11. Vartotojas – kompiuterizuotos darbo vietos priemonės naudojantis darbuotojas ar įgaliotas trečiasis asmuo, nevykdantis jokių specialių informacijos apdorojimo sistemų priežiūros darbų.

12. Išorinė duomenų laikmena – visos nešiojamos kompiuterinės laikmenos (t.y. nešiojamieji kompiuteriai, nešiojami kietieji diskai, CD, DVD, USB atmintinės ir pan.).

### **III SKYRIUS KOMPIUTERINĖS ĮRANGOS APSAUGA**

13. Kompiuterinės įrangos įsigijimas ir instaliavimas:

13.1. pagrindiniai kompiuterinės įrangos įsigijimai turi būti vykdomi pagal patvirtintas įsigijimo procedūras;

13.2. kompiuterinės įrangos instaliavimas gali būti vykdomas tik įgaliotų asmenų ir atitikti šios kompiuterinės įrangos įsigijimo dokumentuose nustatytus reikalavimus, įrangos instaliavimo tvarką bei procedūras.

14. Reikalavimai nepertraukiamam elektros maitinimui, spausdintuvams:

14.1. Mokyklos sistemos (t.y. stacionarių kompiuterių veikimas) ar jų komponentai turi būti aprūpinti nepertraukiamo maitinimo šaltiniais;

14.2. spausdinant slaptą informaciją į tinklo spausdintuvą, būtina užtikrinti informacijos saugumą spausdinimo metu ir po jo. Atspausdinti dokumentai su slapta informacija negali būti palikti spausdintuve, spausdinęs darbuotojas turi juos iš karto paimiti.

15. Reikalavimai eksploatacinėms medžiagoms:

15.1. naudotis išimamais įrašomais informacijos nešėjais (magnetiniais diskeliais, kompaktiniais diskais, atminties kortelėmis ir t.t.) gali tik darbuotojai, kuriems pagal jų pareigybės aprašymus suteikiama prieiga prie Mokyklos tvarkomų asmens duomenų;

15.2. visos nešiojamos kompiuterinės laikmenos turi būti saugomos, naudojamos, perduodamos ir naikinamos atsižvelgiant į jose laikomos informacijos pobūdį;

15.3. naikinant nešiojamas kompiuterines laikmenas, kuriose naudojami asmens duomenys, ir jų kategorijos turi būti sunaikinti taip, kad šių dokumentų nebūtų galima atkurti ar atpažinti jų turinio.

16. Kompiuterinės įrangos dokumentacija:

16.1. kompiuterinės įrangos dokumentacija turi būti savalaikiai atnaujinama, lengvai suprantama ir prieinama darbuotojams, atsakingiems už jos aptarnavimą ir priežiūrą;

16.2. visa Mokyklos kompiuterinė įranga turi būti inventorizuojama kartą per metus įgalioto darbuotojo.

17. Kiti kompiuterinės įrangos apsaugos klausimai:

17.1. nenaudojamos, nereikalingos kompiuterių įrangos šalinimas turi būti vykdomas įgaliotų darbuotojų, kurie turi užtikrinti informacijos apsaugos reikalavimų įvykdymą;

17.2. sugedus kompiuterinei įrangai, būtina nedelsiant informuoti atsakingus Mokyklos darbuotojus;

17.3. informacija kompiuteriuose, išmaniuosiuose telefonuose, planšetėse turi būti šifruojama, apsaugota nuo vagysčių, pametimo ar sugadinimo.

17.4. paliekant darbo vietą, Mokyklos darbuotojas privalo išsiregistruoti iš visų taikomųjų programų;

17.5. siekiant apsaugoti kompiuterį nuo jo neteisėto naudojimo ar informacijos nuskaitymo, visuose Mokyklos naudojamuose kompiuteriuose turi būti naudojamos automatinės ekrano užsklandos vartotojams kurį laiką (pvz., 15 minučių) nedirbant su kompiuteriu;

17.6. įrangą išnešti ar leisti ją išnešti iš Mokyklos patalpų gali tik Mokyklos direktoriaus įsakymu įgalioti Mokyklos darbuotojai. Šie darbuotojai visiškai atsako už išnešamą įrangos ir joje esančios informacijos apsaugą.

### **IV SKYRIUS PROGRAMINĖS ĮRANGOS APSAUGA**

18. Programinės įrangos įsigijimas ir instaliavimas:

18.1. Mokykloje gali būti naudojama tik licencijuota programinė įranga;

18.2. programinės įrangos diegimą ir atnaujinimą vykdo tik įgalioti ir kvalifikuoti specialistai;  
 18.3. diegiant informacines sistemas, būtina pakeisti gamintojo ir / ar tiekėjo nustatytus slaptažodžius.

19. Programinės įrangos priežiūra ir atnaujinimas:

19.1. programinės įrangos klaidos turi būti registruojamos. Apie pastebėtas klaidas turi būti informuojami organizacijos ar asmenys, atsakingi už programinės įrangos priežiūrą ir aptarnavimą;

19.2. programų taisymas ir diegimas avariniais atvejais galimas tik informuojant Mokyklos direktorių. Diegimas vykdomas pagal iš anksto paruoštas ir patikrintas pakeitimų procedūras;

19.3. realių duomenų naudojimas testavimui galimas tik tada, jei yra užtikrinamas reikalingas duomenų konfidencialumas ir integralumas;

19.4. vartotojai turi būti reikiamai apmokyti darbui su nauja sistema;

19.5. visos Mokyklos sistemos / programos turi būti išsamiai ir suprantamai dokumentuotos. Sistemos / programos negali būti diegiamos be reikiamos dokumentacijos.

## **V SKYRIUS INFORMACINIŲ SISTEMŲ APSAUGA**

20. Elektroninis paštas ir internetas:

20.1. failų siuntimas iš interneto turi būti ypatingai kontroliuojamas, kad būtų išvengta piktavališkų programų ar netinkamos informacijos gavimo;

20.2. slaptos ar konfidencialios informacijos siuntimas, jei įmanoma, turi būti vykdomas, siunčiant šifruotus elektroninius laiškus;

20.3. gaunami el. laišakai, laiškų turinys turi būti vartotojų peržiūrėti su ypatingu atsargumu. Draudžiama atidarinti laiškuose esančius failus, jei jie nėra patikrinti dėl virusų ir piktavališkų programų arba gauti nuo nežinomų asmenų;

20.4. Mokyklos darbuotojai, administruojantys interneto prieigą, turi užtikrinti, kad Mokyklos kompiuterinis tinklas būtų apsaugotas nuo piktavališkų įsiveržimų įdiegiant ugniasienę;

20.5. elektroninio pašto sistemai apsaugoti turėtų būti įdiegta nepageidautinų elektroninių laiškų (*angl.* spam) gavimą ir siuntimą kontroliuojanti sistema;

20.6. susirašinėjant darbo reikalais turi būti naudojamos tik oficialios Mokyklos elektroninio pašto dėžutės;

20.7. Mokykloje turi būti naudojamos priemonės, leidžiančios uždrausti ar apriboti darbuotojams naudoti tam tikras interneto sritis. Turėtų būti blokuojami nepageidaujamo turinio internetiniai puslapiai;

20.8. bevielio interneto tinklo prieigai (Wi-Fi) Mokyklos patalpose yra sukongfigūruotos stotelės, skirtos Mokyklos darbuotojams. Bevielis interneto tinklas apsaugotas slaptažodžiu, kurį suteikia ir keičia atsakingas darbuotojas.

21. Mobilus ryšio įrenginių naudojimas:

21.1. mobilus ryšio įrenginys Mokyklos darbuotojams suteikiamas tik darbo funkcijoms vykdyti;

21.2. jei mobilus ryšio įrenginyje naudojamas elektroninis paštas, privaloma apriboti priėjimą prie mobilus įrenginio naudojant ekrano užraktą;

21.3. slapta ar konfidenciali informacija negali būti perduodama mobiliaisiais įrenginiais, visiškai neįsitikinus dėl informacijos gavėjo autentiškumo ir jo teisės gauti informaciją;

21.4. slapta ar konfidenciali informacija negali būti įrašinėjama į auto-atsakiklius / balso pašto sistemas.

22. Duomenų valdymas ir kontrolė:

22.1. duomenų apdorojimas ar keitimas nestandartinėmis priemonėmis gali būti naudojamas tik išskirtiniais (avariniais) atvejais ir pagal šiems atvejams numatytas procedūras;

- 22.2. informaciją iš magnetinių diskelių, kompaktinių diskų ar kitų nešiojamų informacijos laikmenų nuskaityti gali tik atitinkamas teises turintys darbuotojai;
- 22.3. duomenų archyvavimas ar saugojimas turi būti vykdomas atsižvelgiant į teisinius, techninius reikalavimus bei Mokyklos vidinius veiklos dokumentus;
- 22.4. kompiuteriuose esantys laikini failai turi būti periodiškai šalinami.
23. Rezervinis kopijavimas, atstatymas, archyvavimas:
- 23.1. atsakingas darbuotojas turi užtikrinti, kad informacinių sistemų rezervinio kopijavimo ir atstatymo procedūros yra paruoštos, vykdomos ir veikia korektiškai;
- 23.2. svarbūs duomenys, dokumentai, esantys kompiuteriuose, turi būti periodiškai kopijuojami. Kompiuterio vartotojas atsakingas už vykdomo rezervinio kopijavimo reguliarumą;
- 23.3. atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis;
- 23.4. pilnos atsarginės duomenų kopijos daromos kas mėnesį.
24. Popierinių dokumentų valdymas:
- 24.1. dokumentų su svarbia informacija savininkai turi užtikrinti reikiamą informacijos apsaugą dokumentų transportavimo metu;
- 24.2. nereikalingos konfidencialių ar slaptų dokumentų kopijos turi būti sunaikintos dokumentų naikinimui pritaikytais smulkintuvais.
25. Apsauga nuo kenkėjiškų programų:
- 25.1. visuose Mokyklos kompiuteriuose turi veikti reguliariai atnaujinama antivirusinė programinė įranga;
- 25.2. kompiuterinio viruso, kirmino ar kitos piktavališkos programos patekimas į Mokyklos tinklą yra traktuojamas kaip labai pavojingas informacijos saugumo incidentas. Kiekvienu tokio incidento atveju turi būti nustatyti ir užkirsti piktavališkų programų patekimo į Mokyklos tinklą keliai, turi būti ištirtas visas toks incidentas.
26. Informacijos apsaugos incidentai:
- 26.1. išsami duomenų apsaugos pažeidimų valdymo tvarka pateikiama Mokyklos Bendrosiose asmens duomenų apsaugos taisyklėse;
- 26.2. įstatymuose numatytais atvejais apie informacijos saugumo incidentus turi būti informuojamos išorinės organizacijos. Tai gali atlikti tik Mokyklos direktoriaus įgalioti asmenys;
- 26.3. visi informacijos apsaugos incidentai turi būti registruojami;
- 26.4. informacija apie incidentus ir jų tyrimus yra konfidenciali.

## **VI SKYRIUS**

### **PRIEIGOS TEISIŲ SUTEIKIMO, PANAIKINIMO IR PAKEITIMO PROCEDŪRA**

27. Prieiga prie visų Mokyklos naudojamų informacinių sistemų, tinklų, duomenų bazių ar saugyklų internete yra draudžiama, išskyrus kai Mokyklos informacinių sistemų naudotojui yra aiškiai suteiktos prieigos teisės.
28. Prieiga darbuotojui prie konkrečios informacinės sistemos suteikiama remiantis „būtinumo žinoti“ principu. Prieiga prie Mokyklos informacinių sistemų nesuteikia darbuotojui teisių peržiūrėti ir naudoti visą informacinėse sistemose esančią informaciją.
29. Prieigos teisės suteikiamos ir darbuotojo paskyra informacinėse sistemose sukuriama naudojant šiuos asmens duomenis: vardą, pavardę, duomenis, jungiantis el. parašu arba el. bankininkyste. Naudojamų asmens duomenų apimtis atskirose Mokyklos naudojamose informacinėse sistemose gali skirtis.
30. Sprendimą dėl prieigos teisių suteikimo konkrečiam Mokyklos darbuotojui priima Mokyklos direktorius.
31. Prieigos prie Mokyklos sistemų slaptažodžiai, keičiami ir saugomi užtikrinant jų konfidencialumą, yra unikalūs iš ne mažiau kaip 7 simbolių (slaptažodyje turi būti didžioji raidė), nenaudojant asmeninio pobūdžio informacijos, keičiami susidarius tam tikroms aplinkybėms (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas

tretiesiems asmenims ir pan.) ir naudotojo pirmojo prisijungimo metu. Mokyklos darbuotojas prieigos prie asmens duomenų slaptažodžiais turi naudotis asmeniškai ir neatskleisti jų tretiesiems asmenims.

32. Darbuotojas turi teisę susipažinti su Mokyklos konfidencialia informacija tik tais atvejais, jeigu darbuotojui tokie įgaliojimai suteikti pagal darbo sutartį, pareigines instrukcijas ar tokius įgaliojimus konkrečiam darbuotojui suteikė Mokykla.

33. Mokyklos darbuotojai ar išoriniai paslaugų teikėjai, kuriems Mokykla suteikė prieigą prie Mokyklos naudojamų informacinių sistemų, privalo laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino vykdydami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas.

34. Atsakingas darbuotojas reguliariai, bet ne rečiau kaip kartą per 6 mėnesius, peržiūri suteiktas prieigos prie Mokyklos informacinių sistemų teises, ir, jei reikia, panaikina ar pakeičia suteiktas teises.

35. Prieigos teisės trečiosioms šalims (duomenų tvarkytojams) suteikiamos tik pasirašius sutartį, kurioje turi būti nustatytos duomenų tvarkymo sąlygos, nurodomos duomenų tvarkytojo taikomos techninės ir organizacinės duomenų saugumo priemonės, aptariami duomenų tvarkytojo atsakomybės ir kiti klausimai.

36. Pasibaigus darbo santykiams, darbuotojo prieigos teisės prie Mokyklos naudojamų informacinių sistemų nedelsiant panaikinamos. Darbuotojo tiesioginis vadovas privalo pranešti atsakingam darbuotojui apie prieigos teisių panaikinimą ne vėliau kaip paskutinę darbuotojo darbo dieną.

37. Prieigos teisės trečiosioms šalims panaikinamos nutraukus paslaugų sutartį ne vėliau kaip paskutinę paslaugų teikimo dieną.

38. Kiekvienas Mokyklos darbuotojas, užregistruotas Mokyklos naudojamose informacinėse sistemoje, yra priskiriamas darbuotojų grupei, pagal kurią nustatomos, kokios prieigos teisės suteikiamos konkrečiam darbuotojui.

## **VII SKYRIUS FIZINĖ APSAUGA**

39. Patalpų apsauga:

39.1. patalpos, kuriose yra kompiuteriai ir saugomi duomenys, turi būti apsaugotos nuo fizinio įsilaužimo, vagysčių, gaisro, potvynio ir kitų rizikų;

39.2. patalpos, kuriose yra kompiuteriai ir saugomi duomenys, turi atitikti keliamus aplinkos reikalavimus;

39.3. visos kompiuterių patalpos turi būti apsaugotos nuo neautorizuoto fizinio įėjimo. Priklausomai nuo patalpų svarbos turi būti naudojamos įvairaus sudėtingumo fizinės apsaugos technologijos.

40. Švaraus stalo politika:

40.1. dokumentai su slapta informacija ir išorinės duomenų laikmenos turi būti saugomi rakinamose spintose, stalčiuose tuo metu, kai nėra naudojami, ypatingai nedarbo valandomis;

40.2. slapta ar konfidenciali verslo informacija turi būti laikoma saugiai (pvz., seifuose arba rakinamose spintose), nepaliekama spausdintuvuose.

## **VIII SKYRIUS BAIGIAMOSIOS NUOSTATOS**

41. Šis Aprašas įsigalioja nuo jo patvirtinimo datos.

42. Už Aprašo įgyvendinimo kontrolę atsakingi Mokyklos direktoriaus įsakymu įgalioti asmenys – tai darbuotojai, kuriems pagal jų pareigybės aprašymus nustatytos tam tikros funkcijos.

43. Mokyklos darbuotojui pažeidus šiame Apraše numatytų reikalavimų nuostatas, gali būti laikoma jo darbo pareigų pažeidimu.

44. Šis Aprašas gali būti keičiamas, pildomas ir atnaujinamas. Aktuali Aprašo redakcija skelbiama Mokyklos internetinėje svetainėje [www.sdailesmokykla.lt](http://www.sdailesmokykla.lt).

---

SUDERINTA  
Šiaulių dailės mokyklos  
Duomenų apsaugos pareigūnė  
Justina Šabanaitė

2024-01-30