PATVIRTINTA
Šiaulių Centro pradinės mokyklos
direktoriaus 2026 m. balandžio 7 d.
įsakymu Nr. V-28 (1.2.)

ŠIAULIŲ CENTRO PRADINĖS MOKYKLOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ IR INCIDENTŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šiaulių Centro pradinės mokyklos (toliau – Mokyklos) Asmens duomenų saugumo pažeidimų valdymo tvarkos aprašo (toliau – Aprašas) tikslas – nustatyti duomenų tvarkymo metu įvykusių asmens duomenų saugumo pažeidimų ir incidentų valdymo tvarką Mokykloje, užtikrinti, kad Mokyklos darbuotojai sugebėtų laiku nustatyti galimus pažeidimus bei žinotų, kokie veiksmai privalo būti atlikti.

2. Pagrindinės Apraše vartojamos sąvokos:

2.1. Asmens duomenų saugumo pažeidimas (neatitiktis) (toliau – Pažeidimas) – duomenų saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.

2.2. Informacijos saugumo incidentas – vienas ar daugiau nepageidaujamų ir netikėtų informacijos saugumo įvykių, turinčių didelę tikimybę pakenkti veiklai ir keliančių grėsmę informacijos saugumui.

2.3. Įgaliotas (-i) asmuo (-ys) – Mokyklos vadovo paskirtas darbuotojas (-ai), atsakingas (-i) už Pažeidimų fiksavimą, pašalinimą ir pranešimą priežiūros institucijai ir duomenų subjektams.

3. Tiriant galimus Pažeidimus ir teikiant pranešimus vadovaujamasi BDAR, ADTAĮ ir kitais teisės aktais, reglamentuojančiais šių procedūrų atlikimą.

4. Kitos aukščiau nenurodytos Apraše vartojamos sąvokos atitinka ADTAĮ ir BDAR vartojamas sąvokas.

II SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ NUSTATYMAS

5. Galimi šie Pažeidimai pagal pobūdį (tipą):

5.1. konfidencialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie jų suteikimas (pavyzdžiui, atskleisti duomenys ir jie tapo prieinami tretiesiems asmenims, suteikiant prieigą, tinkamai nešifruojant, kt.);

5.2. duomenų pasiekiamumo/prieinamumo – neleistinas arba netyčinis prieigos prie asmens duomenų praradimas arba asmens duomenų sunaikinimas (pavyzdžiui, prarasti duomenys ir neturima atsarginių kopijų);

5.3. duomenų vientisumo pažeidimas – neleistinas arba netyčinis asmens duomenų pakeitimas (pavyzdžiui, prarasti vaikų duomenys, turima tik dalis atsarginių kopijų, dėl ko neįmanoma „atkurti“ visos su vaiku bendravimo istorijos);

5.4. mišraus pobūdžio (tipo) pažeidimas – asmens duomenų konfidencialumo, prieinamumo ir vientisumo pažeidimas ar bet kurių aukščiau nurodytų pažeidimų derinys.

6. Pažeidimas gali įvykti dėl šių priežasčių:

6.1. vagystė (pvz., pavogti nešiojami/mobilūs įrenginiai, kuriuose saugomi asmens duomenys;

6.2. pavogtos neautomatiniu būdu susistemintos bylos, kuriose yra asmens duomenų ir kt.);

6.3. kibernetinė ataka (pvz., duomenų bazėje ar informacinėje sistemoje esantys asmens duomenys užšifruojami, naudojant išpirkos reikalaujančią programą; internete paskelbiami informacinių sistemų naudotojų vardai ir slaptažodžiai ir kt.);

6.4. neleistina (neautorizuota) prieiga prie asmens duomenų (pvz., įgaliojimų neturintys asmenys patenka į patalpas, kuriose saugomos bylos su asmens duomenimis; įgaliojimų neturintys asmenys prisijungia prie duomenų bazių ar informacinių sistemų ir kt.);

6.5. įrenginių ar programinės įrangos gedimas, saugos sistemos spragos (pvz., energijos tiekimo nutrūkimas, dėl kurio negalima prieiga prie asmens duomenų; programos kodo, kuriuo kontroliuojamas prieigos teisių suteikimas informacinių sistemų naudotojams, klaida ir kt.);

6.6. nenumatytos (force majeure) aplinkybės ir kitos priežastys (gaisras, vandens užliejimas, dėl kurių sugadinami arba prarandami asmens duomenys ir kt.).

7. Pažeidimas, galintis kelti pavojų asmenų teisėms, yra toks, dėl kurio, laiku nesiėmus tinkamų priemonių, fiziniai asmenys gali patirti diskriminaciją, gali būti pakenkta jų reputacijai, prarastas duomenų, kurie laikomi profesine paslaptimi, konfidencialumas ir kt.

III SKYRIUS
PRANEŠIMAS APIE GALIMĄ ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

7. Mokyklos darbuotojas, pastebėjęs, nustatęs, gavęs informaciją apie galimą Pažeidimą iš duomenų tvarkytojo ar kito šaltinio, privalo:

7.1. ne vėliau kaip per 2 darbo valandas nuo galimo Pažeidimo paaiškėjimo momento informuoti žodžiu, raštu ar elektroninėmis priemonėmis Mokyklos vadovo Įgaliotą asmenį;

7.2. užpildyti pranešimą apie asmens duomenų saugumo pažeidimą (toliau – Pranešimas) (*priedas 1*) ir ne vėliau kaip per 4 darbo valandas nuo galimo Pažeidimo paaiškėjimo momento perduoti jį Mokyklos vadovo Įgaliotam asmeniui;

7.3. jei įmanoma, imtis priemonių pašalinti galimą Pažeidimą ir imtis priemonių galimoms neigiamoms jo pasekmėms sumažinti.

IV SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMO TYRIMAS IR PAŠALINIMAS

8. Mokyklos vadovo Įgaliotas asmuo, gavęs Pranešimą apie Pažeidimą, privalo:

8.1. Įvertinti ir atlikti 2.3 punkte numatytas funkcijas ne vėliau kaip per 24 valandas nuo Pranešimo gavimo momento;

8.2. konsultuotis su atitinkamomis savivaldybės tarnybomis;

8.3. jei Pažeidimas yra susijęs su elektroninės informacijos saugos incidentu, pasitelkti Mokyklos ar duomenų tvarkytojų IT, paslaugų tiekėjo specialistus;

8.4. įvertinti, kokių skubių ir tinkamų priemonių būtina imtis, kad būtų pašalintas Pažeidimas;

8.5. nustatyti, ar apie Pažeidimą būtina pranešti VDAI, kitoms tarnyboms;

8.6. nustatyti, ar apie Pažeidimą būtina pranešti duomenų subjektams.

9. Atliekant Pažeidimo tyrimą ir siekiant nustatyti, ar Pažeidimas iš tikrųjų įvyko, esamos situacijos įrodymai privalo būti fiksuojami dokumentuose ir užtikrinamas jų atsekamumas.

10. Pažeidimo tyrimo metu darbuotojai ir duomenų tvarkytojas privalo operatyviai teikti Mokyklos vadovo Įgaliotam asmeniui visą jo paprašytą su Pažeidimu susijusią informaciją ir dokumentus.

11. Vertinant rizikos lygį, atsižvelgiama į konkrečias pažeidimo aplinkybes, pavojaus duomenų subjektų teisėms ir laisvėms atsiradimo tikimybę ir rimtumą. Rizikos lygis vertinamas atsižvelgiant į šiuos kriterijus:

11.1. saugumo pažeidimo pobūdis (konfidencialumo, vientisumo ar prieinamumo pažeidimas) – nustatomas saugumo pažeidimo pobūdis: nuo padaryto pažeidimo pobūdžio gali priklausyti pavojaus duomenų subjektams dydis;

11.2. asmens duomenų pobūdis, jautrumas ir kiekis – nustatomas asmens duomenų, kurių saugumas buvo pažeistas, pobūdis, jautrumas ir jų kiekis: kuo jautresni asmens duomenys ir kuo didesnis jų kiekis, tuo didesnis žalos pavojus;

11.3. galimybė identifikuoti fizinį asmenį – įvertinama, ar neįgaliotiems asmenims, kuriems tapo prieinami asmens duomenys, bus lengva nustatyti konkrečių asmenų tapatybę arba susieti tuos duomenis su kita informacija (pvz., tinkamai užšifruoti asmens duomenys nebus suprantami neįgaliotiems asmenims, todėl pažeidimas padarys mažesnį poveikį duomenų subjektams);

11.4. fizinio asmens specifiniai ypatumai – nustatomi fizinių asmenų, kurių asmens duomenims kilo pavojus, specifiniai ypatumai: kuo asmenys yra labiau pažeidžiami (pvz., vaikai, negalią turintys asmenys), tuo didesnį poveikį pažeidimas gali jiems padaryti;

11.5. nukentėjusių duomenų subjektų skaičius – nustatomas nukentėjusių asmenų skaičius: kuo daugiau yra asmenų, kuriems pažeidimas turi poveikio, tuo didesnis žalos pavojus;

11.6. pasekmės, sukeltos fiziniams asmenims – įvertinamos visos galimos pažeidimo pasekmės bei jų rimtumas; taip pat atsižvelgiama į pasekmių ilgalaikiškumą: jei pažeidimo pasekmės yra ilgalaikės, tai poveikis fiziniams asmenims bus didesnis.

12. Įvertinus riziką nustatomas vienas iš trijų rizikos tikimybių lygių – maža, vidutinė ar didelė rizikos tikimybė.

13. Ataskaita yra pateikiama Mokyklos vadovui ir duomenų tvarkytojo vadovui, jei tai susiję su duomenų tvarkytojo atliekamais asmens duomenų tvarkymo veiksmais.

14. Atsižvelgdamas į Ataskaitą, Mokyklos vadovas, jei reikia, tvirtina priemonių planą, kuriame numatomas būtinų techninių, organizacinių, administracinių ir kitų priemonių poreikis dėl Pažeidimo pašalinimo, paskiria atsakingus vykdytojus ir nustato priemonių įgyvendinimo terminus.

15. Sprendžiant Pažeidimo pašalinimo klausimą bei tvirtinant priemonių planą, pirmiausia būtina atlikti veiksmus, siekiant apriboti ar sustabdyti saugumo incidentą. Priklausomai nuo konkrečių Pažeidimo aplinkybių, turėtų būti atlikti tokie veiksmai, kaip: ištrinti asmens duomenis nuotoliniu būdu iš pamesto ar pavogto nešiojamo/mobilaus įrenginio (telefono, nešiojamo kompiuterio ir kt.); jei asmens duomenys per klaidą išsiunčiami ne tam adresatui, kuriam jie buvo skirti, kuo skubiau kreiptis į jį su prašymu ištrinti atsiųstus asmens duomenis be galimybės juos atkurti; pakeisti prisijungimo prie duomenų bazių ar informacinių sistemų vardus ir slaptažodžius, jeigu jie tapo žinomi tretiesiems asmenims; atkuriant prarastus ar sugadintus asmens duomenis, naudoti atsargines kopijas ir kt.

16. Siekiant apriboti ar sustabdyti Pažeidimą, būtina kiek įmanoma tiksliau surinkti duomenų ir įrodymų apie įvykusį saugumo incidentą (pvz., kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės ar informacinės sistemos, kam per klaidą išsiųsti asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su asmens duomenimis ir kt.).

17. Priemonių plane turi būti numatyti veiksmai, nukreipti ne vien į esamo Pažeidimo priežasties pašalinimą, pavojaus fizinių asmenų teisėms ir laisvėms sumažinimą ar pašalinimą, bet taip pat skirti neleisti pasikartoti Pažeidimui. Būtina atsižvelgti į trūkumus ir duomenų tvarkymo silpnąsias vietas, kurios buvo išnaudotos įvykdant Pažeidimą bei imtis priemonių tuos trūkumus pašalinti.

V SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ PRIEŽIŪROS INSTITUCIJAI

18. Tyrimo metu nustačius, kad Pažeidimas buvo Mokyklos vadovui priėmus sprendimą dėl Pranešimo priežiūros institucijai pateikimo būtinybės, Mokyklos vadovo Įgaliotas asmuo ne vėliau kaip per 72 val. nuo tada, kai tapo žinoma apie Pažeidimą, apie tai informuoti VDAI, išskyrus atvejus, kai Pažeidimas nekelia pavojaus fizinių asmenų teisėms ir laisvėms.

19. VDAI informuojama vadovaujantis Pranešimo apie asmens duomenų saugumo pažeidimą pateikimo Valstybinei duomenų apsaugos inspekcijai tvarkos aprašu (aktuali redakcija) (*priedas 2*).

20. Jeigu įvertinus riziką, abejojama, ar Pažeidimas kelia pavojų fizinių asmenų teisėms ir laisvėms, apie pažeidimą pranešama VDAI.

VII SKYRIUS
PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ DUOMENŲ SUBJEKTUI

21. Tyrimo metu nustačius, kad dėl Pažeidimo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, Mokyklos vadovo įgaliotas darbuotojas, jei įmanoma, praėjus ne daugiau kaip 72 valandoms nuo to laiko, kai buvo sužinota apie pažeidimą, praneša apie tai duomenų subjektui, kurio teisėms ir laisvėms gali kilti didelis pavojus.

22. Duomenų subjektas informuojamas tiesiogiai, t. y. siunčiant jam pranešimą paštu, elektroniniu paštu, trumpąja žinute (SMS) ar kitu būdu. Pranešimas duomenų subjektui siunčiamas atskirai nuo kitos siunčiamos informacijos.

23. Pagrindinis pranešimo duomenų subjektui tikslas – pateikti konkrečią informaciją apie tai, kokių veiksmų jis turėtų imtis, kad apsisaugotų nuo neigiamų pažeidimo pasekmių. Pranešime duomenų subjektui aiškia ir paprasta kalba pateikiama ši informacija:

23.1. asmens duomenų saugumo pažeidimo pobūdžio ir tikėtinų pažeidimo pasekmių aprašymas;

23.2. priemonių, kurių ėmėsi Mokykla, kad būtų pašalintas saugumo pažeidimas, įskaitant priemonių galimoms neigiamoms jo pasekmėms sumažinti aprašymas;

23.3. kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas, pavardė ir kontaktiniai duomenys;

23.4. kita reikšminga informacija, susijusi su pažeidimu, kuri, Mokyklos vadovo Įgalioto asmens manymu, turėtų būti pateikta duomenų subjektui, pvz., patarimai, rekomendacijos, kaip apsisaugoti nuo galimų neigiamų pažeidimo pasekmių.

24. Pranešimo apie Pažeidimą duomenų subjektams teikti nereikia jeigu:

24.1. Mo0kykla įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos asmens duomenims, kuriems pažeidimas turėjo poveikio, visų pirma tas priemones, kuriomis užtikrinama, kad asmeniui, neturinčiam leidimo susipažinti su duomenimis, jie būtų nesuprantami (pvz., asmens duomenų šifravimo priemonės);

24.2. iš karto po pažeidimo Mokykla ėmėsi priemonių, kuriomis užtikrinama, kad nekiltų didelis pavojus duomenų subjektų teisėms ir laisvėms;

24.3. tiesioginio pranešimo duomenų subjektui pateikimas pareikalautų neproporcingai didelių pastangų, pvz., jei jų kontaktiniai duomenys buvo prarasti dėl pažeidimo arba iš pradžių nebuvo žinomi. Tokiu atveju apie pažeidimą viešai paskelbiama Mokyklos interneto svetainėje, spaudoje, pasitelkiami ne vienas, o keli informavimo būdai arba taikomos panašios priemonės, kuriomis duomenų subjektai būtų efektyviai informuojami (pvz., vien tik pranešimas interneto svetainėje nėra efektyvi informavimo priemonė).

25. Jeigu įvertinus riziką, nustatoma, kad tuo metu apie Pažeidimą duomenų subjektams pranešti nereikia, po kurio laiko situacija gali pasikeisti, todėl Pažeidimas bei jo keliamas pavojus fizinių asmenų teisėms ir laisvėms turėtų būti vertinamas iš naujo (pvz., įvykdoma kibernetinė ataka, naudojant išpirkos reikalaujančią programą ir duomenų bazėje esantys asmens duomenys užšifruojami – jei atlikus tyrimą, paaiškėja, kad vienintelė išpirkos reikalaujančios programos užduotis buvo užšifruoti asmens duomenis ir jokio kito kenksmingo poveikio duomenų bazei nėra, apie saugumo pažeidimą reikės pranešti tik VDAI, tačiau jei vėliau paaiškėja, kad prarastas ne tik duomenų prieinamumas, bet ir konfidencialumas, saugumo pažeidimo keliamas pavojus bus vertinamas iš naujo bei sprendžiama, ar atsižvelgiant į tikėtinas saugumo pažeidimo pasekmes reikia apie jį pranešti duomenų subjektams).

26. Tam tikromis aplinkybėmis, kai tai yra pagrįsta, Mokykla pasitarusi su teisėsaugos institucijomis ir atsižvelgdama į teisėtus teisėsaugos interesus, gali atidėti asmenų, kuriems pažeidimas turi poveikio, informavimą apie saugumo pažeidimą iki to laiko, kai tai netrukdys saugumo pažeidimo tyrimams.

VII SKYRIUS
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ DOKUMENTAVIMAS

27. Visi Pažeidimai, nepriklausomai nuo to, ar apie juos buvo pranešta VDAI ir (ar) duomenų subjektui, ar tokie pažeidimai kelia riziką, registruojami Asmens duomenų saugumo pažeidimų registravimo žurnale (toliau – Žurnalas).

28. Informacija apie Pažeidimą į Žurnalą turi būti įvedama ne vėliau kaip per 5 darbo dienas nuo galimo pažeidimo paaiškėjimo momento. Kai pasikeičia Žurnale nurodyta informacija arba paaiškėja nauja informacija, Žurnale esanti informacija turi būti papildoma ir (ar) koreguojama.

29. Asmens duomenų saugumo pažeidimų registravimo žurnale nurodoma:

29.1. pažeidimo nustatymo aplinkybės (pažeidimo nustatymo data, laikas, vieta, subjektas, pranešęs apie pažeidimą);

29.2. pažeidimo aplinkybės (pažeidimo data, vieta, pažeidimo pobūdis, priežastys, asmens duomenų, kurių saugumas pažeistas, kategorijos ir apytikslis skaičius, duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos ir apytikslis skaičius);

29.3. tikėtinos pažeidimo pasekmės ir pavojus duomenų subjekto teisėms ir laisvėms;

29.4. priemonės, kurių buvo imtasi, kad būtų pašalintas pažeidimas, įskaitant priemones galimoms neigiamoms pažeidimo pasekmėms sumažinti;

29.5. informacija apie pranešimą VDAI apie asmens duomenų saugumo pažeidimą;

29.6. jei apie asmens duomenų saugumo pažeidimą nebuvo pranešta VDAI, nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta VDAI, nurodoma pranešimo data ir numeris, taip pat, ar pranešimas teikiamas etapais;

29.7. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti VDAI, nurodomos tokio vėlavimo priežastys;

29.8. informacija apie pranešimą duomenų subjektui (subjektams) apie asmens duomenų saugumo pažeidimą;

29.9. jei apie asmens duomenų saugumo pažeidimą nebuvo pranešta duomenų subjektui (subjektams), nurodomi tokio sprendimo motyvai; jei apie asmens duomenų saugumo pažeidimą buvo pranešta duomenų subjektui (subjektams), nurodoma pranešimo (pranešimų) data (datos) ir būdas (būdai);

29.10. jeigu apie asmens duomenų saugumo pažeidimą buvo vėluojama pranešti duomenų subjektui (subjektams), nurodomos tokio vėlavimo priežastys;

29.11. kita reikšminga informacija, susijusi su asmens duomenų saugumo pažeidimu.

30. Už Žurnalo pildymą ir saugojimą atsakingas Mokyklos vadovo Įgaliotas asmuo. Žurnalas gali būti popierinės arba elektroninės formos. Užpildytas Žurnalas saugomas 5 metus nuo paskutinio įrašo Žurnale padarymo dienos.

31. Žurnalas yra pateikiamas VDAI jai pareikalavus.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

32. Aprašas skirtas užtikrinti, kad Mokyklos darbuotojai sugebėtų laiku nustatyti galimus Pažeidimus bei suprastų, kokie veiksmai privalo būti atlikti valdant juos.

33. Aprašo privalo laikytis visi Mokyklos darbuotojai, kurie tvarko asmens duomenis arba eidami savo pareigas juos sužino.

34. Šio Aprašo rekomenduojama laikytis juridiniams asmenims, esantiems Mokyklos duomenų tvarkytojams, kuriems pagal BDAR 33 str. 2 d. yra nustatyta prievolė pranešti Mokyklai apie kiekvieną Pažeidimą.

35. Mokyklos darbuotojai ir duomenų tvarkytojai privalo išsaugoti esamos situacijos, susijusios su galimu Pažeidimu, įrodymus, kad vėliau naudojant technines ir organizacines priemones (pvz., duomenų srauto ir prisijungimų analizės įrankius ar kt.) galima būtų tirti Pažeidimą.

36. Mokyklos darbuotojai su šiuo Aprašu bei jo pakeitimais supažindinami Dokumentų valdymo sistemos priemonėmis.

37. Mokyklos darbuotojai, pažeidę šio Aprašo reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

38. Aprašo priedai, jeigu tokių yra, tampa neatsiejama šio Aprašo dalimi.

_____

Šiaulių Centro pradinės mokyklos
Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
priedas 1

PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

_____Nr. _____
(data, dokumento numeris)

_____
(miestas)

Informuoju apie asmens duomenų saugumo pažeidimą, pateikdamas turimą informaciją:

1. Asmens duomenų saugumo pažeidimo nustatymo data, laikas ir vieta:

2. Asmens duomenų saugumo pažeidimo padarymo data, laikas ir vieta:

3. Asmens duomenų saugumo pažeidimo esmė ir aplinkybės:

4. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (pvz., Mokyklos darbuotojai, asmenys, pateikę prašymus, skundus, asmenys ir kt.) ir apytikslis jų skaičius:

5. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-us):
☐ Asmens tapatybę patvirtinantys duomenys (vardas, pavardė, gimimo data, lytis ir kt.)

☐ Asmens identifikaciniai ar prisijungimo duomenys (asmens kodas, mokėtojo kodas, slaptažodžiai ir kt.)

☐ Asmens kontaktiniai duomenys (gyvenamosios vietos adresas, telefono numeris, elektroninio pašto adresas ir kt.)

☐ Specialių kategorijų asmens duomenys (duomenys, susiję su asmens sveikata, genetiniai duomenys, biometriniai duomenys, duomenys, susiję su asmens rasine ar etnine kilme, duomenys, susiję su asmens politinėmis pažiūromis, religiniais, filosofiniais įsitikinimais ar naryste profesinėse sąjungose, duomenys susiję su asmens lytiniu gyvenimu ir lytine orientacija ir kt.)

☐ Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas ☐ Kiti asmens duomenys (įrašyti):

6. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

7. Kokių veiksmų (priemonių) buvo imtasi sužinojus apie padarytą asmens duomenų saugumo pažeidimą (pvz., pakeisti prisijungimo prie informacinės sistemos slaptažodžiai, panaudotos atsarginės kopijos, siekiant atkurti prarastus ar sugadintus duomenis, atnaujinta programinė įranga, surinkti ne saugojimui skirtoje vietoje palikti dokumentai su asmens duomenimis ir kt.):

_____ _____ _____
(pareigos) (parašas) (vardas ir pavardė)

_____

Šiaulių Centro pradinės mokyklos
Asmens duomenų saugumo pažeidimų
valdymo tvarkos aprašo
priedas 2

PRANEŠIMAS APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMĄ

.....
(data) (rašto numeris)

1. Asmens duomenų saugumo pažeidimo apibūdinimas

1.1. Asmens duomenų saugumo pažeidimo data ir laikas:
Asmens duomenų saugumo pažeidimo:
Data _____Laikas _____

Asmens duomenų saugumo pažeidimo nustatymo:
Data _____Laikas _____

1.2. Asmens duomenų saugumo pažeidimo vieta (pažymėti tinkamą (-us):
 Informacinė sistema
 Duomenų bazė
 Tarnybinė stotis
 Internetinė svetainė
 Debesų kompiuterijos paslaugos
 Nešiojami / mobilūs įrenginiai
 Neautomatiniu būdu susistemintos bylos (archyvas)
 Kita _____

1.3. Asmens duomenų saugumo pažeidimo aplinkybės (pažymėti tinkamą (-us):
 Asmens duomenų konfidencialumo praradimas (neautorizuota prieiga ar atskleidimas)
 Asmens duomenų vientisumo praradimas (neautorizuotas asmens duomenų pakeitimas)
 Asmens duomenų prieinamumo praradimas (asmens duomenų praradimas, sunaikinimas)

1.4. Apytikslis duomenų subjektų, kurių asmens duomenų saugumas pažeistas, skaičius:

1.5. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, kategorijos (atskiriamos pagal jai būdingą požymį):

1.6. Asmens duomenų, kurių saugumas pažeistas, kategorijos (pažymėti tinkamą (-as):
 Asmens tapatybę patvirtinantys asmens duomenys (vardas, pavardė, amžius, gimimo data, lytis ir kt.):
 Specialių kategorijų asmens duomenys (duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, sveikatos duomenys, duomenys apie lytinį gyvenimą ir lytinę orientaciją):
 Duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas:
 Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai (pavyzdžiui, asmens kodas, mokėtojo kodas, slaptažodžiai):
 Kiti:
 Nežinomi (pranešimo teikimo metu)

1.7. Apytikslis asmens duomenų, kurių saugumas pažeistas, skaičius:

1.8. Kita duomenų valdytojo nuomone reikšminga informacija apie asmens duomenų saugumo pažeidimą:

2. Galimos asmens duomenų saugumo pažeidimo pasekmės

2.1. Konfidencialumo praradimo atveju:

 Asmens duomenų išplitimas labiau nei yra būtina ir duomenų subjekto kontrolės praradimas savo asmens duomenų atžvilgiu (pavyzdžiui, asmens duomenys išplito internete)

 Skirtingos informacijos susiejimas (pavyzdžiui, gyvenamosios vietos adreso susiejimas su asmens buvimo vieta realiu laiku)

 Galimas panaudojimas kitais, nei nustatytais ar neteisėtais tikslais (pavyzdžiui, komerciniais tikslais, asmens tapatybės pasisavinimo tikslu, informacijos panaudojimo prieš asmenį tikslu)

 Kita

2.2. Vientisumo praradimo atveju:

 Pakeitimas į neteisingus duomenis dėl ko asmuo gali netekti galimybės naudotis paslaugomis

 Pakeitimas į galiojančius duomenis, kad asmens duomenų tvarkymas būtų nukreiptas (pavyzdžiui, pavogta asmens tapatybė susiejant vieno asmens identifikuojančius duomenis su kito asmens biometriniais duomenimis)

 Kita

2.3. Duomenų prieinamumo praradimo atveju:

 Dėl asmens duomenų trūkumo negalima teikti paslaugų (pavyzdžiui, administracinių procesų sutrikdymas, dėl ko negalima prieiti, pavyzdžiui, prie asmens sveikatos istorijų ir teikti pacientams sveikatos paslaugų, arba įgyvendinti duomenų subjekto teises)

 Dėl klaidų asmens duomenų tvarkymo procesuose negalima teikti tinkamos paslaugos (pavyzdžiui, asmens sveikatos istorijoje neliko informacijos apie asmens alergijas, tam tikra informacija iš mokesčių deklaracijos išnyko, dėl ko negalima tinkamai apskaičiuoti mokesčių ir pan.)

 Kita

2.4. Kita:

3. Priemonės, kurių imtasi, siekiant pašalinti pažeidimą ar sumažinti jo pasekmes

3.1. Taikytos priemonės, siekiant sumažinti poveikį duomenų subjektams:

3.2. Taikytos priemonės, siekiant pašalinti asmens duomenų saugumo pažeidimą:

3.3. Taikytos priemonės, siekiant, kad pažeidimas nepasikartotų:

3.4. Kita:

4. Siūlomos priemonės sumažinti asmens duomenų saugumo pažeidimo pasekmėms

5. Duomenų subjektų informavimas apie asmens duomenų saugumo pažeidimą

5.1. Duomenys apie informavimo faktą:

 Taip, duomenų subjektai informuoti (nurodoma data) _____

 Ne, bet jie bus informuoti (nurodoma data)_____

 Ne

5.2. Duomenų subjektų, kurių asmens duomenų saugumas pažeistas, neinformavimo priežastys:

 Ne, nes nekyla didelis pavojus duomenų subjektų teisėms ir laisvėms (nurodoma kodėl)

 Ne, nes įgyvendintos tinkamos techninės ir organizacinės priemonės, užtikrinančios, kad asmeniui, neturinčiam leidimo susipažinti su asmens duomenimis, jie būtų nesuprantami (nurodomos kokios)

 Ne, nes tai pareikalautų neproporcingai daug pastangų ir apie tai viešai paskelbta (arba taikyta panaši priemonė) (nurodoma kada ir kur paskelbta informacija viešai arba jei taikyta kita priemonė, nurodoma kokia ir kada taikyta)

 Ne, nes dar neidentifikuoti duomenų subjektai, kurių asmens duomenų saugumas pažeistas

5.3. Informacija, kuri buvo pateikta duomenų subjektams (gali būti pridėtas pranešimo duomenų subjektui kopija):

5.4. Būdas, kokiu duomenų subjektai buvo informuoti:

 Paštu

 Elektroniniu paštu

 Kitu būdu

6. Asmuo, galintis suteikti daugiau informacijos apie asmens duomenų saugumo pažeidimą (duomenų apsaugos pareigūnas ar kitas kontaktinis asmuo)

6.1. Vardas ir pavardė

_____

6.2. Telefono ryšio numeris

_____

6.3. Elektroninio pašto adresas

_____

6.4. Pareigos

_____

6.5. Darbovietės pavadinimas ir adresas

_____

7. Pranešimo pateikimo Valstybinei duomenų apsaugos inspekcijai pateikimo vėlavimo priežastys

8. Kita reikšminga informacija

_____

(pareigos) (parašas) (vardas, pavardė)

_____