PATVIRTINTA
Klaipėdos r. Slengių mokyklos-
daugiafunkcio centro direktoriaus
2026 m. rugsėjo 1 d. įsakymu Nr. V1-52A

KLAIPĖDOS R. SLENGIŲ MOKYKLOS-DAUGIAFUNKCIO CENTRO

INFORMACINIŲ TECHNOLOGIJŲ NAUDOJIMO TVARKOS APRAŠAS

I. BENDROSIOS NUOSTATOS

1.1. Paskirtis ir taikymo sritis

1. Informacinių technologijų (toliau – IT) naudojimo ir saugumo tvarkos aprašas (toliau – Tvarka) nustato Klaipėdos rajono Slengių mokyklos-daugiafunkcio centro (toliau – Centras) informacinių sistemų, kompiuterinės ir tinklo įrangos, duomenų laikmenų, programinės įrangos bei su jomis susijusios informacijos naudojimo, apsaugos ir valdymo principus.

2. Tvarkos tikslas – užtikrinti Centro tvarkomos informacijos (įskaitant mokinių, jų tėvų (globėjų, rūpintojų) bei darbuotojų asmens duomenis, ugdymo proceso, finansinę ir kitą veiklos informaciją) konfidencialumą, vientisumą ir prieinamumą, sumažinti informacijos saugumo incidentų riziką ir jų galimą žalą, taip pat sudaryti sąlygas greitai atkurti Centro veiklai svarbias IT sistemas įvykus sutrikimui.

3. Tvarka vieningai reglamentuoja šias sritis: informacijos saugumo politiką, turto valdymą ir informacijos klasifikavimą, prieigos teisių valdymą, tinklo (ryšių) saugumą, IT sistemų diegimą ir keitimų valdymą, atsarginį kopijavimą ir duomenų atstatymą, duomenų laikmenų naudojimą, kriptografijos priemonių naudojimą, techninių pažeidžiamumų valdymą, mobiliųjų įrenginių naudojimą, informacijos perdavimą, paslaugų teikėjų (tiekėjų) saugą, fizinę saugą, dirbtinio intelekto įrankių naudojimą, informacijos saugumo incidentų valdymą bei veiklos tęstinumo ir IT sistemų atstatymo planavimą.

4. Tvarka privaloma visiems Centro darbuotojams, taip pat mokiniams, jų tėvams (globėjams, rūpintojams) ir kitiems asmenims (paslaugų teikėjams, rangovams, praktikantams, savanoriams ir kt.), kurie naudojasi Centro IT ištekliais arba turi prieigą prie Centro valdomos informacijos ir informacinių sistemų – atitinkamai jiems taikytina apimtimi.

5. Tvarka taikoma visai Centro valdomai informacijai, nepriklausomai nuo jos formos (elektroninė ar popierinė) ir laikmenos, taip pat visai Centro naudojamai, nuomojamai ar valdomai IT infrastruktūrai (kompiuteriams, serveriams, tinklo įrangai, programinei įrangai, debesijos paslaugoms ir kt.).

1.2. Pagrindinės sąvokos

- Informacijos saugumas – informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

- Informacinis turtas – bet kokia Centrui reikšmingą vertę turinti informacija ar ją apdorojantys ištekliai (duomenų bazės, dokumentai, programinė įranga, techninė įranga).
- Naudotojas – Centro darbuotojas ar kitas asmuo, kuriam suteikta prieiga prie Centro informacinių sistemų ar informacijos.
- IT administratorius – Centro paskirtas darbuotojas arba paslaugų teikėjas (pagal sutartį), atsakingas už IT infrastruktūros priežiūrą, administravimą ir techninį saugumą.
- Informacijos saugos koordinatorius – Centro direktoriaus paskirtas asmuo (Centre šias funkcijas atlieka direktoriaus pavaduotojas ūkio reikalams), atsakingas už šios Tvarkos įgyvendinimo koordinavimą, informacijos saugumo incidentų valdymo organizavimą ir Tvarkos aktualumo priežiūrą.
- Duomenų apsaugos pareigūnas (DAP) – Centro paskirtas asmuo (darbuotojas arba paslaugų teikėjas pagal sutartį), atsakingas už asmens duomenų apsaugos reikalavimų (BDAR) laikymosi priežiūrą Centre. Kaip viešojo sektoriaus (viešojo administravimo) subjektui, Centrui DAP paskyrimas yra privalomas pagal BDAR 37 straipsnio 1 dalies a punktą.
- Informacijos saugumo incidentas – įvykis ar aplinkybė, kelianti grėsmę informacijos konfidencialumui, vientisumui ar prieinamumui (pvz., neteisėta prieiga, duomenų praradimas, kenkėjiškos programinės įrangos užkratas, IT sistemos gedimas ar išpuolis prieš ją).
- Kritinė informacinė sistema – IT sistema, kurios sutrikimas iš esmės sutrikdytų Centro veiklą (pvz., elektroninis dienynas, buhalterinės apskaitos sistema, Centro tinklas, mokinių registro sąsaja).
- Dirbtinio intelekto (DI) įrankis – programinė įranga ar paslauga (pvz., pokalbių robotas, teksto, vaizdo ar kito turinio generavimo priemonė), kuri, remiantis Reglamentu (ES) 2024/1689, atitinka dirbtinio intelekto sistemos apibrėžimą ir naudojama Centro veikloje.

1.3. Susiję teisės aktai

6. Tvarka parengta atsižvelgiant į:

- 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas, BDAR);
- Lietuvos Respublikos kibernetinio saugumo įstatymą ir jo įgyvendinamuosius teisės aktus, įskaitant Kibernetinio saugumo reikalavimų aprašą;
- Lietuvos standarto LST EN ISO/IEC 27001:2022 (informacijos saugumo, kibernetinio saugumo ir privatumo apsaugos valdymo sistemos) rekomendacijas ir gerąją praktiką;

- 2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentą (ES) 2024/1689, nustatantį suderintas dirbtinio intelekto taisykles (Dirbtinio intelekto aktas);
- Lietuvos Respublikos 2026–2035 m. nacionalines dirbtinio intelekto strategines gaires;
- kitus Centro veiklą reglamentuojančius vidaus teisės aktus (Centro nuostatus, darbo tvarkos taisykles, asmens duomenų tvarkymo taisykles ir kt.).

7. Kilus prieštaravimui tarp šios Tvarkos ir galiojančių teisės aktų, vadovaujamasi teisės aktų nuostatomis.

8. Informacijos saugos koordinatorius ne rečiau kaip kartą per metus patikrina, ar Centras yra (ar turėtų būti) įtrauktas į Nacionalinio kibernetinio saugumo centro (NKSC) administruojamą Kibernetinio saugumo subjektų registrą, ir, kilus abejonių dėl Centro statuso ar jam taikomų papildomų techninių bei organizacinių reikalavimų, kreipiasi į Centro savininko teises ir pareigas įgyvendinančią instituciją (Klaipėdos rajono savivaldybės administraciją) ir (ar) NKSC. Jei Centras būtų priskirtas prie reguliuojamų (esminių ar svarbių) subjektų, ši Tvarka turi būti papildyta specialiais Kibernetinio saugumo reikalavimų apraše nustatytais reikalavimais (įskaitant pranešimo apie reikšmingus incidentus NKSC per teisės aktuose nustatytus terminus tvarką).

II. INFORMACIJOS SAUGUMO POLITIKA IR VALDYMAS

2.1. Bendrieji principai

9. Centras įsipareigoja užtikrinti tinkamą informacijos saugumo lygį, atitinkantį jo veiklos pobūdį (ugdymo įstaiga, tvarkanti nepilnamečių ir darbuotojų asmens duomenis) ir jam taikomus teisinius reikalavimus. Informacijos saugumo kontrolės priemonės parenkamos ir taikomos atsižvelgiant į realią riziką ir Centro turimus išteklius – proporcingai grėsmėms, o ne formaliai.

10. Informacijos saugumo užtikrinimas yra visų Centro bendruomenės narių atsakomybė, ne tik IT administratoriaus. Kiekvienas naudotojas privalo laikytis šios Tvarkos ir nedelsdamas pranešti apie pastebėtus pažeidimus ar įtartinus įvykius.

11. Informacijos saugumo reikalavimai turi būti taikomi visame informacijos gyvavimo cikle: kuriant ar renkant informaciją, ją apdorojant, saugant, perduodant ir galiausiai sunaikinant.

2.2. Atsakomybės pasiskirstymas

Pareigos	Atsakomybės informacijos saugumo srityje
Direktorius	Tvirtina Tvarką ir jos pakeitimus; priima galutinius sprendimus dėl didelio masto incidentų ir veiklos tęstinumo plano aktyvavimo; skiria informacijos saugos koordinatorių ir duomenų apsaugos pareigūną (DAP

Pareigos	Atsakomybės informacijos saugumo srityje
	paskyrimas Centrui yra privalomas pagal BDAR 37 str. 1 d. a punktą).
Direktoriaus pavaduotojas ūkio reikalams (informacijos saugos koordinatorius)	Koordinuoja Tvarkos įgyvendinimą ir kasmetinę peržiūrą; organizuoja informacijos saugumo incidentų valdymą; prižiūri IT administratoriaus ir paslaugų teikėjų darbą saugumo klausimais; teikia direktoriui ataskaitas.
IT administratorius (darbuotojas arba paslaugų teikėjas)	Administruoja IT infrastruktūrą, naudotojų paskyras, atsargines kopijas, tinklo ir įrenginių saugumą; diegia atnaujinimus; techniškai sprendžia incidentus.
Duomenų apsaugos pareigūnas (DAP)	Konsultuoja asmens duomenų apsaugos (BDAR) klausimais, prižiūri, kaip laikomasi teisės aktų reikalavimų tvarkant asmens duomenis; kaip nepriklausomas asmuo, atsiskaito tiesiogiai direktoriui.
Darbuotojai, mokiniai, tėvai (globėjai)	Laikosi Tvarkos, saugo jiems suteiktas prieigos priemones ir įrenginius, nedelsdami praneša apie pastebėtus incidentus ar pažeidimus.

2.3. Nuolatinis tobulinimas ir peržiūra

12. Ši Tvarka peržiūrima ne rečiau kaip kartą per metus arba įvykus esminiams pasikeitimams (naujos IT sistemos diegimas, teisės aktų pasikeitimas, reikšmingas incidentas). Peržiūrą inicijuoja informacijos saugos koordinatorius, pakeitimus tvirtina direktorius.

13. Pastabos ir pasiūlymai dėl Tvarkos tobulinimo gali būti teikiami bet kuriuo metu informacijos saugos koordinatoriui.

III. INFORMACIJOS IR TURTO KLASIFIKAVIMO TVARKA

3.1. Tikslas

14. Šiuo skyriumi nustatomos konkrečios kontrolės priemonės, taikomos tam tikros klasifikacijos informacijai tvarkyti, siekiant užtikrinti, kad Centro informacinis turtas (dokumentai, duomenų bazės, elektroniniai failai, sutartys ir kt.) būtų tinkamai apsaugotas per visą jo gyvavimo ciklą.

15. Nevieša (neviešinama) informacija negali būti atskleista jokiam nesuinteresuotam asmeniui ar organizacijai nesaugiu būdu (popieriumi, faksu, telefonu, elektroniniu paštu ar žodžiu), o dalijimasis ja su trečiosiomis šalimis vyksta tik pagal suderintą tvarką ar sutartį. Neteisėtas atskleidimas laikomas darbo drausmės pažeidimu ir informuojama vadovaujantis XV skyriuje nustatyta incidentų valdymo tvarka.

3.2. Klasifikavimo lygiai

16. Centre naudojami keturi informacijos klasifikavimo lygiai:

Lygis	Pavadinimas	Pavyzdžiai Centro veikloje
0	Vieša	Viešai skelbiama informacija: Centro internetinio puslapio turinys, renginių skelbimai, viešieji pirkimai, ugdymo plano viešoji dalis.
1	Apsaugota (vidinė)	Darbuotojų pareigybių aprašymai, vidiniai tvarkų aprašai, pamokų tvarkaraščiai, susirinkimų protokolai, neskelbtina, bet nekonfidenciali korespondencija.
2	Ribota	Mokinių ir darbuotojų asmens duomenys (kontaktai, pažymiai, lankomumas), mokinių pasiekimų vertinimai, sutartys su tiekėjais, individualūs susitarimai.
3	Konfidenciali	Specialių kategorijų asmens duomenys (sveikatos, specialiųjų ugdymosi poreikių informacija), darbuotojų asmens bylos, atlyginimų duomenys, vidaus tyrimų medžiaga, incidentų tyrimo dokumentacija.

Pastaba: viešai skelbiamos (Centro interneto svetainėje, viešuosiuose registruose ar kitaip oficialiai paskelbtos) finansinės ir kitos ataskaitos priskiriamos 0 (Vieša) klasifikavimo lygiui; šio skyriaus reikalavimai konfidencialumui netaikomi toms jų dalims, kurios yra viešai skelbiamos.

17. Kiekvienam klasifikavimo lygiui taikomos šios bendrosios tvarkymo taisyklės:

Lygis	Apdorojimas / prieiga	Saugojimas	Perdavimas	Sunaikinimas
0 – Vieša	Be apribojimų, tačiau tik patvirtintomis priemonėmis (ne asmeniniais įrankiais internete).	Gali būti saugoma neapsaugotose vietose.	Gali būti siunčiama nešifruota.	Įprastu būdu, be specialių priemonių.
1 – Apsaugota	Prieiga suteikiama	Elektroninėse laikmenose – be	Rekomenduojamas failų šifravimas,	Popierius – susmulkinama

Lygis	Apdorojimas / prieiga	Saugojimas	Perdavimas	Sunaikinimas
	darbuotojams pagal poreikį; spausdiniai laikomi viešai nepasiekiamose vietose.	viešos prieigos, pageidautina užrakintoje patalpoje.	ypač el. laiškų prieduose.	s; elektroninės laikmenos – ištrinamos.
2 – Ribota	Griežta prieigos kontrolė (autorizuotas prisijungimas, fizinė apsauga); apdorojama tik patvirtintomis priemonėmis.	Užrakintoje patalpoje ar spintoje, ribojant prieigą; nustatyta raktų valdymo tvarka.	Šifravimas privalomas (failų priedams, laikmenoms); perdavimas registruojamas.	Popierius – sunaikinamas smulkintuvu taip, kad teksto atkurti nebūtų įmanoma; laikmenos – visiškai ištrinamos; sunaikinimą tikrina antras asmuo.
3 – Konfidencialu	Labai griežta prieigos kontrolė; prieiga tik įgaliotiems asmenims; negalima apdoroti nepatvirtintomis priemonėmis.	Nerekomenduojama saugoti išimamose laikmenose; jei būtina – tik šifruota, užrakintoje patalpoje.	Šifravimas privalomas; el. paštu siųsti nerekomenduojama; kopijos numeruojamos ir registruojamos.	Popierius – sunaikinamas smulkintuvu, užtikrinančiu, kad teksto atkurti nebūtų įmanoma; laikmenos – visiškai ištrinamos arba fiziškai sunaikinamos; būtinas antro asmens patvirtinimas.

18. Su 2 ir 3 lygio informacija susiję saugumo incidentai laikomi svarbiais ir apie juos nedelsiant pranešama informacijos saugos koordinatoriui, vadovaujantis XV skyriuje nustatyta tvarka.

3.3. Fizinio turto apskaita

19. Visa Centro IT ir kita reikšminga įranga registruojama turto apskaitos registre, nurodant turto numerį, modelį ar serijos numerį, atsakingą naudotoją ir įsigijimo datą.

Registrą tvarko IT administratorius kartu su direktoriaus pavaduotoju ūkio reikalams; registro duomenys derinami su centralizuotos apskaitos duomenimis.

IV. INFORMACINIŲ SISTEMŲ PRIEIGOS TEISIŲ VALDYMO TVARKA

4.1. Bendrieji principai

20. Prieigos teisės prie Centro informacinių sistemų suteikiamos vadovaujantis būtinumo žinoti ir mažiausių privilegijų principais – naudotojui suteikiama tik tokia prieiga, kokios reikia jo pareigoms atlikti.

4.2. Naujo naudotojo paskyros sukūrimas

21. Prašymą sukurti naują naudotojo paskyrą (naujam darbuotojui, mokiniui ar kitam asmeniui) IT administratoriui teikia tiesioginis vadovas (mokinių atveju – direktoriaus pavaduotojas ugdymui arba klasės mokytojas), nurodydamas: vardą, pavardę, pareigas ar mokinio klasę, reikalingas sistemas ir prieigos lygį, darbo (mokymosi) pradžios datą.

22. Prieigos prie jautrių ar riboto naudojimo sistemų (pvz., buhalterinės apskaitos, elektroninio dienyno administravimo) suteikiamos tik gavus tiesioginio vadovo arba informacijos saugos koordinatoriaus patvirtinimą.

23. Sukūrus paskyrą, naudotojui nustatomas pirminis slaptažodis, kurį jis privalo pasikeisti pirmo prisijungimo metu. Pirminis slaptažodis naudotojui perduodamas asmeniškai arba kitu saugiu būdu, patvirtinus naudotojo tapatybę; slaptažodis neturi būti siunčiamas trumpąja žinute ar nešifruotu el. laišku kartu su prisijungimo vardu.

4.3. Prieigos teisių keitimas

24. Pasikeitus darbuotojo pareigoms, klasei ar atsakomybėms, tiesioginis vadovas nedelsdamas informuoja IT administratorių dėl prieigos teisių pakoregavimo (naujų teisių suteikimo ir nebereikalingų – panaikinimo).

4.4. Paskyros panaikinimas ir blokavimas

25. Nutraukus darbo santykius ar mokymosi Centre, tiesioginis vadovas (personalą administruojantis darbuotojas) informuoja IT administratorių ne vėliau kaip paskutinę darbo (mokymosi) dieną, o skubotos atleidimo tvarkos atveju – nedelsiant.

26. IT administratorius nedelsdamas užblokuoja arba panaikina visas su naudotoju susijusias paskyras (įskaitant el. paštą, prieigą prie bendrų diskų, specializuotų sistemų). Prireikus, atgaunami visi naudotojui išduoti prieigos raktai ar kortelės.

27. Ne vėliau kaip paskutinę darbuotojo darbo dieną tiesioginis vadovas kartu su IT administratoriumi pasirūpina, kad būtų grąžinta visa darbuotojui perduota Centro IT įranga ir laikmenos (nešiojamas ar kitas kompiuteris, telefonas, planšetė, USB laikmenos ir kt.), o jose buvusi su darbu susijusi informacija, kurios reikia Centro veiklai, perduota tiesioginiam vadovui ar jo nurodytam asmeniui. Grąžinta įranga registruojama turto apskaitos registre (žr. 3.3 punktą).

4.5. Privilegijuotos (administratoriaus) prieigos teisės

28. Administratoriaus (privilegijuotos) teisės suteikiamos tik tiems asmenims, kuriems tai būtina pareigoms atlikti, ir naudojamos atskira, ne kasdiene naudotojo paskyra. Numatytojo administratoriaus slaptažodis niekam neatskleidžiamas ir keičiamas įdiegus sistemą.

4.6. Periodinė prieigos teisių peržiūra

29. IT administratorius kartu su informacijos saugos koordinatoriumi ne rečiau kaip kartą per metus atlieka pagrindinių informacinių sistemų naudotojų prieigos teisių peržiūrą, siekdami nustatyti: nebenaudojamas ar perteklines paskyras, netinkamai priskirtas teises, bendrai naudojamas (nepersonalizuotas) paskyras. Nustatyti neatitikimai ištaisomi ir užregistruojami.

4.7. Slaptažodžių politika ir kelių veiksnių autentifikavimas

30. Naudotojo slaptažodis turi būti pakankamai ilgas ir sudėtingas (rekomenduojama – ne trumpesnis kaip 12 ženklų arba ilgesnė slaptafrazė), unikalus kiekvienai sistemai ir laikomas paslaptyje. Naudotojui griežtai draudžiama atskleisti savo prisijungimo slaptažodį kitiems asmenims (įskaitant kitus darbuotojus, tiesioginį vadovą ar IT administratorių) ir naudotis kito asmens paskyra.

31. Kelių veiksnių autentifikavimas (MFA) privalomas naudotojams jungiantis prie: Centro darbuotojų el. pašto paskyrų, administratoriaus (privilegijuotų) paskyrų (žr. 4.5 punktą) ir nuotolinės prieigos prie Centro vidinių sistemų (žr. V skyrių). Kitoms sistemoms, kuriose tvarkoma 2 ar 3 klasifikavimo lygio informacija, kelių veiksnių autentifikavimas įjungiamas visais atvejais, kai tai techniškai palaiko naudojama sistema.

V. TINKLO IR RYŠIŲ SAUGUMO TVARKA

5.1. Tinklo projektavimo principai

32. Centro kompiuterių tinklas projektuojamas ir prižiūrimas atsižvelgiant į: juo perduodamos informacijos jautrumą, galimas grėsmes, reikiamą prieinamumo lygį bei iš kokių vietų tinklas bus pasiekiamas.

33. Kur įmanoma, taikomas kelių apsaugos lygių principas (pvz., tinklo ugniasienė papildoma atskirų serverių ar įrenginių apsauga), kad vieno komponento gedimas nekeltų pavojaus visam tinklui.

5.2. Tinklų atskyrimas

34. Centro tinklas logiškai (pvz., naudojant VLAN arba atskirus belaidžius tinklus) atskiriamas bent į šias dalis:

- administracinis tinklas – darbuotojų kompiuteriams, buhalterinei ir kitoms administravimo sistemoms;

- pedagoginis (ugdymo) tinklas – mokinių ir ugdymo proceso reikmėms naudojamiems įrenginiams;
- svečių belaidis tinklas – lankytojams ir kitiems asmenims, fiziškai ar logiškai atskirtas nuo vidinių tinklų.

35. Perimetras tarp Centro vidinio tinklo ir viešojo interneto apsaugomas ugniasiene, leidžiančia tik būtiną tinklo srautą.

5.3. Belaidžio ryšio sauga

36. Belaidžiai tinklai apsaugomi ne žemesnio nei WPA2 lygio šifravimu (rekomenduojama WPA3, kai palaikoma įrangos). Prieigos taškų administravimo slaptažodžiai visada pakeičiami iš gamintojo numatytųjų.

5.4. Nuotolinė prieiga

37. Nuotolinei prieigai prie Centro vidinių sistemų naudojamas šifruotas virtualus privatus tinklas (VPN) arba kitas lygiavertį saugumo lygį užtikrinantis būdas. Nuotolinė prieiga suteikiama tik konkrečiam poreikiui, o ne visiems naudotojams pagal numatytuosius nustatymus.

5.5. Stebėsena, pakeitimai ir incidentai

38. IT administratorius periodiškai stebi tinklo veikimą ir prieinamumą, o pastebėjęs neįprastą veiklą (pvz., įtartiną srautą, prievadų nuskaitymą) imasi priemonių ir prireikus inicijuoja incidento valdymo procedūrą (žr. XV skyrių).

39. Visi tinklo įrangos pakeitimai atliekami vadovaujantis VI skyriuje nustatyta pakeitimų valdymo tvarka ir registruojami, kad būtų išlaikytas aktualus tinklo vaizdas.

VI. IT SISTEMŲ DIEGIMO IR KEITIMŲ VALDYMO TVARKA

6.1. Naujų IT sistemų ir paslaugų įsigijimas

40. Centras daugumą naudojamų informacinių sistemų (elektroninis dienynas, buhalterinės apskaitos programa, mokyklos svetainė ir kt.) įsigyja arba nuomojasi iš išorės paslaugų teikėjų, o ne kuria pats. Todėl, renkantis naują IT sistemą ar paslaugą, būtina įvertinti:

- kokio pobūdžio ir kokio klasifikavimo lygio duomenys bus tvarkomi sistemoje (žr. III skyrių);
- ar tiekėjas užtikrina tinkamą duomenų apsaugą ir atitinka BDAR reikalavimus (jei tvarkomi asmens duomenys);
- kur ir kaip bus saugomos ir atkuriamos atsarginės duomenų kopijos;
- kaip bus valdomos naudotojų prieigos teisės naujoje sistemoje;
- sistemos palaikymo ir problemų sprendimo sąlygas.

41. Prieš pasirašant sutartį dėl naujos IT sistemos ar paslaugos, informacijos saugos koordinatorius kartu su IT administratoriumi įvertina saugumo reikalavimus ir, jei tvarkomi asmens duomenys, prireikus pasitelkia duomenų apsaugos pareigūną.

6.2. Pakeitimų valdymo procesas

42. Bet koks reikšmingas Centro IT infrastruktūros, sistemų konfigūracijos ar naudojamų paslaugų pakeitimas (nauja įranga, sistemos atnaujinimas, tinklo konfigūracijos keitimas) planuojamas ir įgyvendinamas šia tvarka:

1. pakeitimo poreikį nustato ir jį pagrindžia iniciatorius (darbuotojas, IT administratorius ar paslaugų teikėjas);
2. IT administratorius įvertina pakeitimo poveikį (įskaitant informacijos saugumui) ir reikalingus išteklius;
3. reikšmingiems pakeitimams pritarimą duoda informacijos saugos koordinatorius (esant poreikiui – direktorius);
4. pakeitimas, kai įmanoma, iš anksto išbandomas testinėje aplinkoje ar ne darbo/pamokų metu;
5. įgyvendinus pakeitimą, patikrinama, ar sistemos veikia tinkamai, o pakeitimas ir jo rezultatas užregistruojami.

43. Skubūs pakeitimai (būtini nedelsiant, siekiant išspręsti aukšto prioriteto incidentą ar problemą) gali būti įgyvendinami be išankstinio, viso proceso, tačiau apie juos kuo greičiau informuojamas informacijos saugos koordinatorius, o pakeitimas visais atvejais užregistruojamas.

44. Mažos rizikos, reguliariai atliekami standartiniai veiksmai (pvz., įprastas programinės įrangos atnaujinimas pagal tiekėjo grafiką) gali būti atliekami be atskiro kiekvieno karto derinimo, tačiau turi būti fiksuojami IT administratoriaus vedamame veiksmų žurnale.

VII. ATSARGINIO KOPIJAVIMO IR DUOMENŲ ATSTATYMO TVARKA

7.1. Atsarginių kopijų politika

45. Siekiant užtikrinti Centro veiklos tęstinumą įvykus techninei ar kitokiai klaidai, reguliariai daromos Centro informacijos atsarginės kopijos. Atsarginio kopijavimo apimtis, dažnumas ir saugojimo laikotarpis nustatomi pagal duomenų svarbą ir fiksuojami Atsarginių kopijų valdymo registre (forma – C priedas).

46. Kai atsarginį kopijavimą (dalinai ar visiškai) atlieka išorės paslaugų teikėjas (pvz., debesijos paslaugų ar naudojamos informacinės sistemos tiekėjas), su juo sudaromoje sutartyje turi būti aptarti šie klausimai:

- atsarginių kopijų apimtis, tvarkaraštis ir saugojimo vietos;

- kopijų saugojimo trukmė ir jų vientisumo užtikrinimas;
- atstatymo testavimo tvarka ir terminai, per kuriuos duomenys būtų atkurti įvykus incidentui;
- naudojamas šifravimo metodas.

47. Atsarginės kopijos, kai įmanoma, saugomos vietoje, pakankamai nutolusioje nuo pagrindinės duomenų saugojimo vietos, kad nelaimės atveju (gaisras, užliejimas ir pan.) nebūtų paveiktos abi kopijos vienu metu.

48. Ne rečiau kaip kartą per metus atliekamas bandomasis duomenų atstatymas iš atsarginės kopijos, siekiant patikrinti kopijų tinkamumą ir atstatymo proceso veikimą. Rezultatai užfiksuojami.

7.2. Duomenų atstatymo procedūra

49. Prašymą atstatyti duomenis iš atsarginės kopijos naudotojas teikia IT administratoriui, nurodydamas: kokius konkrečius failus ar aplankus reikia atkurti, iš kokios sistemos, nuo kada, ir ar atkurti duomenys turi būti perrašyti ant esamų.

50. Avarinį (skubų, didelio masto) duomenų atstatymą patvirtina informacijos saugos koordinatorius arba direktorius. Po atstatymo IT administratorius parengia trumpą ataskaitą apie atlikto atstatymo rezultatus.

VIII. DUOMENŲ LAIKMENŲ NAUDOJIMO TVARKA

8.1. Bendrieji reikalavimai

51. Išimamos duomenų laikmenos (USB atmintinės, atminties kortelės, išoriniai kietieji diskai, CD/DVD) naudojamos tik tiek, kiek tikrai būtina, ir tik oficialiais Centro veiklos tikslais. Kur įmanoma, teikiama pirmenybė saugesniems duomenų perdavimo būdams (pvz., el. paštu su šifravimu, bendriems saugotinos informacijos diskams su prieigos kontrole).

52. Draudžiama Centro duomenis, priskirtus 2 ar 3 klasifikavimo lygiui (žr. III skyrių), laikyti neužšifruotose išimamose laikmenose.

53. Duomenų perkėlimas dirbti iš namų asmeninėje (ne Centro) technikoje leidžiamas tik XI skyriuje („Mobiliųjų įrenginių naudojimo tvarka“) nustatyta tvarka gavus reikiamą leidimą ir taikant tinkamas apsaugos priemones (šifravimą); draudžiama daryti asmeniškai inicijuotas atsargines kopijas į Centrui nepriklausančią infrastruktūrą (pvz., asmeninę debesijos saugyklą).

8.2. Laikmenų išdavimas

54. Norintis gauti tarnybinę duomenų laikmeną naudotojas kreipiasi į IT administratorių, nurodydamas naudojimo tikslą. IT administratorius veda laikmenų apskaitos registrą (turto numeris, serijos numeris, paskirtas naudotojas, išdavimo data).

55. Jei laikmenoje bus saugoma 2 ar 3 lygio informacija, ji privalo būti užšifruota. Naudotojas atsako už laikmenos šifravimą ir slaptažodžio saugojimą; slaptažodis niekada nelaikomas kartu su laikmena.

8.3. Nežinomos kilmės laikmenos

56. Gavus ar radus nežinomos kilmės laikmeną, darbuotojui ar mokiniui draudžiama jungti ją prie savo ar Centro įrangos; laikmena nedelsiant perduodama IT administratoriui.

8.4. Saugus laikmenų sunaikinimas

57. Nebenaudojamos laikmenos (ar tos, kuriose buvo saugoma 2–3 lygio informacija) saugiai sunaikinamos taip, kad duomenų nebūtų galima atkurti (fizinis sunaikinimas arba patikimas ištrynimas), o sunaikinimas fiksuojamas laikmenų apskaitos registre. Sunaikinimą, kai laikmenoje buvo 2–3 lygio informacija, stebi ir patvirtina antras asmuo.

IX. KRIPTOGRAFIJOS PRIEMONIŲ NAUDOJIMO TVARKA

9.1. Kada naudojama kriptografija (šifravimas)

58. Kriptografijos (šifravimo) priemonės Centre paprastai taikomos apsaugant 2 (Ribota) ir 3 (Konfidenciali) klasifikavimo lygio informaciją, taip pat šiais atvejais:

- naudojant mobiliuosius įrenginius (nešiojamus kompiuterius, planšetes, išmaniuosius telefonus);
- naudojant išimamas duomenų laikmenas;
- perduodant neskelbtinus duomenis viešaisiais tinklais (pvz., internetu);
- naudojantis debesijos paslaugomis, nepriklausomai nuo jų tipo.

9.2. Rekomenduojami metodai

Situacija	Rekomenduojama technika	Pastabos
Duomenų saugojimas debesijoje	AES-256 šifravimas ramybės būsenoje	Šifravimo raktai neturėtų būti saugomi to paties tiekėjo, kuris saugo duomenis.
Duomenys interneto svetainėse / prisijungimo formose	TLS 1.2 ar naujesnė versija	Sertifikatai gaunami iš patikimo tiekėjo.
Duomenys išimamose laikmenose	Simetrinis AES-256 šifravimas	Taikoma, kai laikmenoje saugoma 2–3 lygio informacija.

Situacija	Rekomenduojama technika	Pastabos
Slaptažodžių saugojimas sistemose	Adaptyvios (lėtos), druską naudojančios slaptažodžių maišos funkcijos (Argon2id, bcrypt arba scrypt)	Bendrosios paskirties maišos funkcijos (pvz., SHA-2 šeimos) vienos pačios nėra tinkamos slaptažodžiams saugoti – jos per greitos ir nepakankamai atsparios sistemingam spėjimui (brute-force); taikytina, kai Centras pats administruoja sistemos naudotojų slaptažodžius.
Nuotolinis prisijungimas	VPN, naudojant TLS 1.2+ arba IPSec	Žr. taip pat V skyrių.

9.3. Raktų valdymas

59. Šifravimo raktai turi būti apsaugoti nuo modifikavimo, praradimo ar neteisėto atskleidimo. Kur šifravimo raktų valdymą atlieka debesijos paslaugų teikėjas, su juo aptariama rakto tipas, valdymo sistema ir procedūros raktų generavimui, saugojimui, atnaujinimui bei atšaukimui.

X. TECHNINIŲ PAŽEIDŽIAMUMŲ VALDYMO TVARKA

10.1. Pažeidžiamumų nustatymas

60. IT administratorius seka informaciją apie Centro naudojamos technikos ir programinės įrangos (operacinių sistemų, taikomųjų programų, tinklo įrangos) gamintojų skelbiamus saugumo pažeidžiamumus ir jiems skirtus pataisymus.

10.2. Atnaujinimų (pataisų) diegimas

61. Saugumo atnaujinimai diegiami kuo greičiau po jų paskelbimo, atsižvelgiant į sistemos kritiškumą ir galimą poveikį vartotojams. Kritinių sistemų atnaujinimai planuojami vadovaujantis VI skyriuje aprašyta pakeitimų valdymo tvarka, esant galimybei – atliekami ne pamokų metu.

10.3. Periodinis pažeidžiamumų vertinimas

62. Ne rečiau kaip kartą per metus atliekamas Centro IT infrastruktūros (bent jau iš interneto pasiekiamų paslaugų ir pagrindinių vidinio tinklo elementų) pažeidžiamumo įvertinimas – tai gali atlikti IT administratorius, kviestinis specialistas ar paslaugų teikėjas.

10.4. Apsaugos priemonės ir informuotumas

63. Nenaudojamos paslaugos ir prievadai serveriuose bei tinklo įrenginiuose išjungiami, siekiant sumažinti galimą atakos paviršių. Nustačius reikšmingus trūkumus, darbuotojai supažindinami su rizikomis ir rekomenduojamais atsargumo veiksmais.

XI. MOBILIŲJŲ ĮRENGINIŲ NAUDOJIMO TVARKA

11.1. Centro suteikti įrenginiai

64. Centro suteiktais mobiliaisiais įrenginiais (nešiojamais kompiuteriais, planšetėmis, telefonais) galima naudotis tik su darbo (ugdymo) funkcijomis susijusiais tikslais. Įrenginys turi būti apsaugotas ekrano užraktu (slaptažodžiu ar PIN kodu), o esant galimybei – ir viso disko šifravimu.

65. Įrenginius draudžiama palikti be priežiūros viešose vietose, dalintis su šeimos nariais ar naudoti asmeniniais tikslais. Praradus ar pavogus įrenginį, naudotojas privalo nedelsiant informuoti IT administratorių.

66. Prijungiant įrenginį prie Centro vidinio tinklo iš išorės, naudojamas VPN ar kitas saugus prisijungimo būdas (žr. V skyrių). Draudžiama jungtis prie nepatikimų viešųjų belaidžio interneto prieigos taškų su Centro įranga, kai apdorojama neskelbtina informacija.

11.2. Asmeninių įrenginių naudojimas ugdymo ir darbo tikslais (BYOD)

67. Asmeninių įrenginių naudojimas darbo ar ugdymo tikslais Centre yra ribojamas ir leidžiamas tik konkrečiais atvejais, kuriuos patvirtina direktorius arba jo įgaliotas asmuo, atsižvelgiant į tai, kokio jautrumo informacija bus pasiekiama.

68. Naudojant asmeninį įrenginį Centro veiklos duomenims pasiekti, jame turi būti įdiegta ir veikianti antivirusinė programa, laiku diegiami programinės įrangos atnaujinimai, o įrenginys turi turėti ekrano užraktą. 2–3 klasifikavimo lygio informacija asmeniniuose įrenginiuose nesaugoma.

69. Ugdymo procese naudojami asmeniniai mokinių mobilieji įrenginiai (telefonai ir kiti galiniai įrenginiai) reglamentuojami atskiru Centro direktoriaus patvirtintu Mokinių asmeninių mobiliųjų telefonų ir kitų galinių įrenginių naudojimo tvarkos aprašu; ši Tvarka tam neprieštarauja ir taikoma papildomai tais atvejais, kai tokie įrenginiai naudojami prieigai prie Centro informacinių sistemų.

XII. INFORMACIJOS PERDAVIMO VIDUJE IR IŠORINIAMS PARTNERIAMS TVARKA

12.1. Bendrieji principai

70. Informacija perduodama trečiosioms šalims (kitoms institucijoms, tiekėjams, tėvams (globėjams) ir kt.) tik esant aiškiam ir pagrįstam poreikiui, siekiant sumažinti jos praradimo ar neteisėto atskleidimo riziką.

71. Pagrindiniai Centro naudojami informacijos perdavimo būdai: oficiali elektroninė sistema/paštas (Centro naudojamas el. pašto ar dokumentų valdymo sprendimas), Centro naudojamas mokinių registro / dienyno sprendimas, prireikus – registruotas paštas ar kurjeris fizinėms laikmenoms.

12.2. Šifravimas, ženklinimas ir perdavimo tvarka

72. Perduodant 2 ir 3 klasifikavimo lygio informaciją, taikomas šifravimas (žr. IX skyrių). Kelių failų ar laikmenų perdavimo atveju kiekviena laikmena ar failas pažymimi juose esančios informacijos klasifikacija.

73. Prieš perduodant informaciją, patikrinami gavėjo duomenys (adresas, el. paštas), o po perdavimo siuntėjas įsitikina, kad gavėjas informaciją gavo ir prireikus sėkmingai iššifravo.

74. Naudojantis kurjerio ar registruoto pašto paslaugomis, siuntimo dokumentai saugomi kaip perdavimo įrodymas.

12.3. Incidentai perdavimo metu

75. Jei perduodama informacija prarandama ar sugadinama, siuntėjas nedelsdamas informuoja informacijos saugos koordinatorių ir toliau veikiama pagal XV skyriuje nustatytą incidentų valdymo tvarką.

XIII. PASLAUGŲ TEIKĖJŲ (TIEKĖJŲ) SAUGOS POLITIKA

13.1. Bendrosios nuostatos

76. Centro santykiai su IT ir kitomis paslaugas teikiančiomis trečiosiomis šalimis (tiekėjais, rangovais) grindžiami aiškiu informacijos saugumo reikalavimų supratimu ir atitinkamų nuostatų įtraukimu į sutartis.

77. Prieš pasirašant sutartį su nauju tiekėju, kuris turės prieigą prie Centro informacijos ar informacinių sistemų, įvertinama, kokias informacijos saugumo priemones taiko tiekėjas. Kai tiekėjas asmens duomenis tvarko Centro vardu, su juo privaloma sudaryti BDAR 28 straipsnį atitinkančią duomenų tvarkymo sutartį (arba įtraukti atitinkamas nuostatas į pagrindinę sutartį), nustatančią duomenų tvarkymo dalyką, trukmę, pobūdį ir tikslą, taip pat tiekėjo pareigas bei įsipareigojimus asmens duomenų apsaugos srityje.

13.2. Sutartiniai reikalavimai

78. Sutartyse su tiekėjais, kur taikytina, numatoma: tvarkomos informacijos klasifikacija ir apsaugos reikalavimai; Centro teisė patikrinti tiekėjo taikomas saugumo priemones; pranešimo apie saugumo incidentus tvarka ir terminai; atsakomybė už subrangovų veiksmus.

79. Naudojant debesijos paslaugas, papildomai įvertinama, kur fiziškai saugomi duomenys ir ar tai atitinka teisinius reikalavimus dėl asmens duomenų perdavimo.

13.3. Tiekėjų stebėsena

80. Svarbiausių (kritinių) IT paslaugų teikėjų (pvz., elektroninio dienyno, buhalterinės sistemos, interneto ryšio tiekėjo) veikla periodiškai peržiūrima – vertinama, ar paslaugos teikiamos pagal sutartį ir ar nekyla papildomų saugumo rizikų. Pastebėję reikšmingus trūkumus, informacijos saugos koordinatorius ir IT administratorius sprendžia dėl tolesnių veiksmų (pretenzijos, papildomų priemonių reikalavimo ar sutarties peržiūros).

XIV. FIZINĖS SAUGOS TVARKA

14.1. Saugios zonos

81. Serverinė (-s), IT įrangos spintos ir kitos patalpos, kuriose laikoma svarbi IT įranga ar neskelbtina informacija, laikomos saugiomis zonomis ir turi būti užrakinamos, kai jose nėra darbuotojų.

82. Prieigą prie saugių zonų raktų (kodų) turi tik tie darbuotojai, kuriems tai būtina pareigoms atlikti. Šių patalpų raktai (kodai) valdomi centralizuotai.

83. Pastato perimetro apsaugai naudojamos turimos priemonės (signalizacija, durų spynos, prireikus – vaizdo stebėjimas), atitinkančios Centre nustatytą fizinės saugos ir vidaus tvarkos lygį.

14.2. Popierinių dokumentų ir įrangos apsauga

84. 2–3 klasifikavimo lygio popieriniai dokumentai laikomi užrakinamose spintose ar seifuose. Darbo vietos, kuriose tvarkomi neskelbtini duomenys, išdėstomos taip, kad pašaliniai asmenys negalėtų jų matyti (švaraus stalo principas).

85. Bendro naudojimo kompiuterinė įranga (serveriai, tinklo įranga) laikoma vietose, mažinančiose aplinkos (karščio, drėgmės, dulkių) ir vagystės riziką; kritinės sistemos, kur įmanoma, apsaugomos nepertraukiamo maitinimo šaltiniu (UPS).

86. Visa IT įranga registruojama turto apskaitos registre (žr. 3.3 punktą) su unikaliu turto numeriu.

14.3. Įrangos gyvavimo ciklo valdymas

87. IT įrangos techninė priežiūra atliekama laikantis gamintojo rekomendacijų; priežiūros ir remonto darbų informacija registruojama.

88. Įranga, kurią ketinama naudoti pakartotinai, perduoti kitam asmeniui ar išmesti, prieš tai turi būti išvalyta – iš jos ištrinami ar sunaikinami visi duomenys ir programinė įranga, vadovaujantis VIII skyriuje nustatyta tvarka.

XV. INFORMACIJOS SAUGUMO INCIDENTŲ VALDYMO TVARKA

15.1. Tikslas ir taikymo sritis

89. Šiuo skyriumi nustatoma tvarka, kaip Centras reaguoja į įvykius, keliančius grėsmę informacijos saugumui – nuo pastebėjimo iki galutinio išsprendimo ir išvadų padarymo. Aprašyti veiksmai laikomi gairėmis; konkretūs veiksmai visais atvejais derinami prie realios situacijos.

15.2. Incidento nustatymas ir pirminis vertinimas

90. Bet kuris darbuotojas, mokinys ar kitas asmuo, pastebėjęs galimą informacijos saugumo incidentą (pvz., neteisėtą prieigą, duomenų nutekėjimą, kenkėjišką programinę įrangą, prarastą ar pavogtą įrenginį, IT sistemos gedimą dėl išpuolio), nedelsdamas apie tai praneša IT administratoriui arba informacijos saugos koordinatoriui.

91. Gavęs pranešimą, informacijos saugos koordinatorius kartu su IT administratoriumi atlieka pirminį incidento poveikio vertinimą: kokia informacija ir sistemos paveiktos, kada incidentas galėjo prasidėti, koks galimas poveikis Centro veiklai ir duomenų subjektams.

15.3. Reagavimo laikas

Incidento pobūdis	**Maksimalus laikas iki pirminio reagavimo**
Didelė tikimybė, kad informacija (įsk. asmens duomenys) prarasta ar atskleista	1 val.
Sutrikdyta ar nepasiekiama Centro veiklai kritinė IT sistema	1 val.
Didelė reputacinės žalos rizika	1 val.
Kita reikšminga situacija, galinti turėti didelį poveikį Centrui	1 darbo diena

92. Šioje lentelėje nurodytas laikas skaičiuojamas nuo momento, kai apie incidentą sužino IT administratorius arba informacijos saugos koordinatorius. Ne darbo valandomis, savaitgaliais ar švenčių dienomis pirminį reagavimą užtikrina IT administratorių pavaduojantis asmuo arba, jei tai numatyta sutartyje, budintis išorės IT paslaugų teikėjo atstovas. Šiame punkte nurodyti terminai suderinami su Centro IT paslaugas teikiančiu tiekėju sutartyje ir, esant poreikiui, koreguojami atsižvelgiant į realias Centro bei tiekėjo galimybes.

15.4. Reagavimo grupė ir atsakomybės

Funkcija	Atsakingas asmuo
Bendras incidento valdymas, galutiniai sprendimai	Direktorius
Incidento koordinavimas, vertinimas, komunikacija	Informacijos saugos koordinatorius (direktoriaus pavaduotojas ūkio reikalams)
Techninis incidento sprendimas (izoliavimas, atkūrimas)	IT administratorius
Asmens duomenų apsaugos aspektų vertinimas	Duomenų apsaugos pareigūnas kartu su informacijos saugos koordinatoriumi
Komunikacija su tėvais (globėjais), žiniasklaida, steigėju	Direktorius arba jo paskirtas asmuo

15.5. Sustabdymas, likvidavimas ir atkūrimas

93. Pirmiausia imamasi veiksmų incidento plitimui sustabdyti (pvz., paveikto įrenginio atjungimas nuo tinklo). Jei įtariama nusikalstama veika arba gali prireikti įrodymų, susijusi informacija (žurnalai, ekrano nuotraukos, įrenginiai) išsaugoma nepakeista ir, jei reikia, konsultuojamasi su teisėsaugos institucijomis ar atitinkamą patirtį turinčiais specialistais.

94. Vėliau šalinama incidento priežastis (pvz., kenkėjiška programa) vadovaujantis VI skyriuje nustatyta pakeitimų valdymo tvarka, o sistemos atkuriamos į įprastą veikimo būklę, pašalinant panaudotus pažeidžiamumus.

15.6. Pranešimas kitoms institucijoms

95. Kai incidentas susijęs su asmens duomenų saugumo pažeidimu, informacijos saugos koordinatorius kartu su duomenų apsaugos pareigūnu įvertina pažeidimo keliamą riziką ir taiko šiuos, BDAR nustatytus, atskirus terminus bei kriterijus:

- Valstybinei duomenų apsaugos inspekcijai (VDAI) pranešama nepagrįstai nedelsiant ir, jei įmanoma, ne vėliau kaip per 72 valandas nuo sužinojimo apie pažeidimą, jei pažeidimas gali kelti riziką fizinių asmenų teisėms ir laisvėms (BDAR 33 str.); pranešti nelaukiama 72 valandų termino pabaigos, o jei per šį terminą pranešti visgi neįmanoma, kartu su pranešimu nurodomos vėlavimo priežastys;
- duomenų subjektams (pvz., mokiniams, jų tėvams (globėjams), darbuotojams) pranešama be nepagrįsto delsimo tik tuo atveju, jei pažeidimas gali kelti DIDELĘ riziką jų teisėms ir laisvėms – šis pranešimo slenkstis yra aukštesnis nei pranešimui

VDAI, todėl ne kiekvienas VDAI praneštas pažeidimas reiškia, kad būtina informuoti ir duomenų subjektus (BDAR 34 str.).

96. Visi asmens duomenų saugumo pažeidimai registruojami ir dokumentuojami, įskaitant jų aplinkybes, poveikį, priimtus veiksmus bei atvejus, kai nuspręsta VDAI ar duomenų subjektų apie pažeidimą neinformuoti, ir tokio sprendimo motyvus (BDAR 33 str. 5 d.).

97. Prireikus (pvz., didelio masto incidento, galinčio turėti reikšmingą poveikį Centro veiklai, atveju) informuojamas Centro savininko teises ir pareigas įgyvendinančios institucijos atstovas.

15.7. Veiksmai po incidento

98. Išsprendus incidentą, informacijos saugos koordinatorius parengia trumpą incidento aprašymą (kas įvyko, kokių veiksmų imtasi, kokie padariniai, kokios prevencinės priemonės numatomos ateičiai) ir pateikia jį direktoriui. Reikšmingi incidentai ir jų priežastys aptariami artimiausios metinės Tvarkos peržiūros metu.

15.8. Kontaktai

99. Aktualūs vidiniai ir išoriniai kontaktai, naudojami incidento atveju, kaupiami A priede ir peržiūrimi ne rečiau kaip kartą per metus.

XVI. VEIKLOS TĘSTINUMO IR IT SISTEMŲ ATSTATYMO PLANAS

16.1. Tikslas

100. Šis planas skirtas užtikrinti Centro veiklos tęstinumą įvykus didelio masto sutrikimui, dėl kurio pagrindinės IT sistemos taptų nepasiekiamos (pvz., dėl įrangos gedimo, gaisro, elektros energijos dingimo, kibernetinės atakos ar kitos priežasties).

101. Plano tikslai: kuo greičiau atkurti kritinių IT sistemų veikimą arba laikiną jų pakaitalą; užtikrinti dalinį Centro veiklos (ugdymo proceso, administravimo) tęstinumą, kol sistemos visiškai atkuriamos; apsaugoti informaciją viso incidento metu; aiškiai paskirstyti atsakomybes ir komunikacijos tvarką.

16.2. Aktyvavimas

102. Planą aktyvuoja direktorius arba informacijos saugos koordinatorius, kai incidentas turi (ar gali turėti) didelį poveikį Centro veiklai ir jo neišsprendžia įprasta incidentų valdymo tvarka (žr. XV skyrių).

16.3. Kritinės sistemos ir prioritetai

103. Toliau pateiktoje lentelėje nurodomos Centro veiklai kritinės IT sistemos, orientacinis jų atkūrimo prioritetas, kiekvienai sistemai nustatomas tikslinis atkūrimo laikas (per kiek laiko sistema turi būti vėl pasiekiama) bei leistinas duomenų praradimo laikas (kiek

naujausių duomenų pokyčių, atsižvelgiant į atsarginio kopijavimo dažnumą, galima negrįžtamai prarasti). Lentelė turi būti užpildyta ir reguliariai atnaujinama Centro IT administratoriaus.

Sistema / paslauga	Prioritetas	Tikslinis atkūrimo laikas (RTO)	Leistinas duomenų praradimo laikas (RPO)	Pastabos (tiekėjas, atsakingas asmuo)
Elektroninis dienynas				
Buhalterinės apskaitos sistema				
Centro interneto svetainė				
Vidinis kompiuterių tinklas / interneto ryšys				
Elektroninis paštas				
Failų / dokumentų saugykla				
Vaizdo stebėjimo sistema (jei naudojama)				
Kita				

104. Šio punkto lentelė bei A ir C prieduose pateiktos formos užpildomos ne vėliau kaip per 30 dienų nuo šios Tvarkos patvirtinimo ir atnaujinamos ne rečiau kaip kartą per metus arba pasikeitus jose nurodytai informacijai.

16.4. Atkūrimo komanda

105. Atkūrimo komandą sudaro:

Vaidmuo	Atsakingas asmuo	Kontaktai
Plano savininkas	Direktorius	
Koordinatorius	Informacijos saugos koordinatorius	
Techninė dalis (IT atkūrimas)	IT administratorius / paslaugų teikėjas	

Vaidmuo	Atsakingas asmuo	Kontaktai
Administracinė dalis (dokumentai, ugdymo proceso organizavimas)	Pavaduotojas ugdymui / sekretorius	

106. Įvykus incidentui, plano savininkas suburia atkūrimo komandą, paaiškina situaciją, paskirsto užduotis ir nustato bendravimo su komandos nariais dažnumą, kol situacija išsprendžiama.

16.5. Ryšio palaikymas

107. Pagrindinė ryšio priemonė incidento metu – telefonas (fiksuotas ir (ar) mobilusis); elektroninis paštas naudojamas tik jei telefono ryšys nepasiekiamas. Visais atvejais vengiama atskleisti incidento detales pašaliniams asmenims, o svarbi informacija ir priimti sprendimai fiksuojami raštu.

108. Su žiniasklaida ir kitomis išorės šalimis bendrauja tik direktorius arba jo paskirtas asmuo.

16.6. Normalaus veikimo atstatymas

109. Sprendimą, kad situacija išspręsta ir galima grįžti prie įprasto sistemų veikimo pagrindinėje vietoje, priima direktorius, remdamasis atkūrimo komandos rekomendacija. Grįžimas prie įprasto veikimo, kai įmanoma, planuojamas mažiausio Centro veiklos intensyvumo metu (pvz., savaitgalį ar atostogų metu).

110. Reikšmingi ištekliai (išorinių tiekėjų priklausomybės), į kuriuos atsižvelgiama vykdant planą, nurodomi B priede.

XVII. DIRBTINIO INTELEKTO ĮRANKIŲ NAUDOJIMO TVARKA

17.1. Tikslas ir taikymo sritis

111. Šis skyrius nustato dirbtinio intelekto (DI) įrankių (pokalbių robotų, teksto, vaizdo, garso ar kito turinio generavimo priemonių, automatinio vertimo, duomenų analizės ir panašių sprendimų) naudojimo Centro veikloje taisykles, siekiant apsaugoti asmens ir kitus neskelbtinus duomenis, užtikrinti atitiktį galiojantiems teisės aktams bei skaidrų, atsakingą ir kontroliuojamą DI naudojimą ugdymo ir administraciniame procese.

112. Skyrius taikomas visiems Centro darbuotojams, naudojantiems DI įrankius su Centro veikla susijusiais tikslais (dokumentų rengimui, komunikacijai, ugdymo medžiagos kūrimui ir kt.), taip pat, kiek taikytina, DI naudojimui ugdymo procese su mokiniais.

17.2. Duomenų teikimo dirbtinio intelekto įrankiams apribojimai

113. 2 ar 3 klasifikavimo lygio informaciją (žr. III skyrių), įskaitant mokinių, jų tėvų (globėjų) ar darbuotojų asmens duomenis, į DI įrankius galima įvesti (įkelti, kopijuoti, diktuoti) tik tada, kai įrankis patvirtintas Centre (114 punktas) ir jo tiekėjas užtikrina, kad tokie

duomenys nebus naudojami DI modeliui mokyti ir bus tvarkomi laikantis BDAR reikalavimų. Draudžiama:

- asmens duomenų, mokinių pažymių, sveikatos ar kitos neskelbtinos informacijos įvedimas į DI įrankius, kurie nėra patvirtinti naudoti Centre;
- DI naudojimas galutiniams sprendimams dėl asmenų (pvz., mokinių pasiekimų vertinimo, personalo sprendimų) priimti be darbuotojo atsakingos peržiūros;
- prisijungimo duomenų, sutarčių ar kitos konfidencialios Centro informacijos įkėlimas į DI įrankius be išankstinio patvirtinimo.

114. DI įrankiai, kuriuos darbuotojai naudoja su darbu susijusiais tikslais, prieš pradedant juos naudoti įvertinami ir patvirtinami informacijos saugos koordinatoriaus kartu su IT administratoriumi (žr. VI skyrių), o jei tvarkomi asmens duomenys – prireikus pasitelkiant duomenų apsaugos pareigūną ir, kai taikytina, sudarant duomenų tvarkymo sutartį su DI įrankio tiekėju (žr. XIII skyrių). Patvirtintų DI įrankių sąrašą tvarko IT administratorius.

17.3. Turinio peržiūra ir darbuotojo atsakomybė

115. Naudojant DI įrankius sukurtas turinys (tekstai, atsakymai, dokumentų projektai, apibendrinimai ir pan.) prieš naudojant oficialiai ar viešai visada peržiūrimas ir, jei reikia, pataisomas jį naudojančio darbuotojo; darbuotojas išlieka atsakingas už galutinio turinio tikslumą, teisingumą ir tinkamumą taip pat, kaip ir už paties savarankiškai parengtą turinį.

116. DI įrankiai gali būti naudojami tik kaip pagalbinė priemonė – jais negali būti pakeičiamas darbuotojo profesinis sprendimas ar atsakomybė priimant sprendimus, turinčius teisinį ar reikšmingą poveikį asmenims (pvz., mokinio pasiekimų vertinimas, drausminės nuobaudos, personalo sprendimai).

17.4. Dirbtinio intelekto naudojimas ugdymo procese

117. Kai DI įrankiai naudojami ugdymo procese su mokiniais ar jų darbui, atsižvelgiama į mokinių amžių bei ugdymo tikslus, o tėvai (globėjai, rūpintojai), kiek tai susiję su jų vaiko asmens duomenimis ar mokymosi procesu, informuojami Centro nustatyta tvarka. Už metodinius DI naudojimo ugdyme aspektus atsako ugdymą organizuojantis darbuotojas (mokytojas), o už technologinę ir duomenų saugumo pusę – IT administratorius ir informacijos saugos koordinatorius.

17.5. Atsakomybė, mokymai ir stebėsena

118. Informacijos saugos koordinatorius, prireikus kartu su IT administratoriumi, ne rečiau kaip kartą per metus peržiūri Centre naudojamus DI įrankius bei jų atitiktį šiai Tvarkai ir galiojantiems teisės aktams, įskaitant Reglamentą (ES) 2024/1689 (Dirbtinio intelekto aktas) bei Lietuvos Respublikos 2026–2035 m. nacionalines dirbtinio intelekto strategines gaires.

119. Siekdamas užtikrinti pakankamą darbuotojų dirbtinio intelekto raštingumą (Reglamento (ES) 2024/1689 4 str. prasme), informacijos saugos koordinatorius organizuoja arba inicijuoja darbuotojų, naudojančių DI įrankius, supažindinimą su šia Tvarka ir, prireikus, papildomus mokymus.

120. Apie pastebėtą neleistiną DI įrankių naudojimą ar su tuo susijusį galimą duomenų saugumo incidentą pranešama ir veikiama vadovaujantis XV skyriuje nustatyta incidentų valdymo tvarka.

XVIII. BAIGIAMOSIOS NUOSTATOS

121. Ši Tvarka įsigalioja ją patvirtinus Centro direktoriui.

122. Su Tvarka visi Centro darbuotojai supažindinami pasirašytinai arba per Centre naudojamą elektroninę dokumentų valdymo/susipažinimo sistemą. Mokiniai ir jų tėvai (globėjai, rūpintojai), tiek, kiek jiems taikoma, su Tvarkos nuostatomis supažindinami Centro nustatyta tvarka (pvz., paskelbiant Centro internetiniame puslapyje ar elektroniniame dienyne).

123. Už šios Tvarkos pažeidimus darbuotojams gali būti taikoma drausminė atsakomybė, o kitiems asmenims – kitos teisės aktuose numatytos poveikio priemonės.

124. Tvarkos vykdymo priežiūrą atlieka informacijos saugos koordinatorius, kuris ne rečiau kaip kartą per metus teikia direktoriui informaciją apie Tvarkos įgyvendinimo būklę, per praėjusį laikotarpį įvykusius incidentus ir siūlymus dėl Tvarkos tobulinimo.

PRIEDAI

A priedas. Incidentų valdymo kontaktų sąrašas

Vardas, pavardė	Atsakomybė	Telefonas	El. paštas
Gaiva Petravičienė	Direktorius		
	Informacijos saugos koordinatorius		
	IT administratorius / paslaugų teikėjas		
	Duomenų apsaugos pareigūnas		

B priedas. Naudingi išoriniai kontaktai (tiekėjai, paslaugų teikėjai)

Organizacija	Paslauga / priklausomybė	Kontaktinis asmuo	Telefonas / el. paštas
	Interneto ryšio tiekėjas		
	Elektroninio dienyno tiekėjas		
	Buhalterinės sistemos tiekėjas		
	IT priežiūros paslaugų teikėjas		

C priedas. Atsarginių kopijų valdymo registro forma

Sistema / duomenys	Kopijavimo dažnumas	Saugojimo vieta	Saugojimo terminas	Paskutinio atstatymo testo data	Atsakingas asmuo

D priedas. Naudotojų prieigos teisių peržiūros forma

Sistema	Peržiūros data	Nustatyti neatitikimai	Atlikti veiksmai