PATVIRTINTA
Kelmės „Kūlverstuko“ lopšelio-darželio direktoriaus 2026 m. vasario 17 d.
įsakymu Nr. V-118

KELMĖS „KŪLVERSTUKO“ LOPŠELIO-DARŽELIO DUOMENŲ SAUGUMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1.1. Kelmės „Kūlverstuko“ lopšelio-darželio (toliau-Įstaiga) Duomenų saugumo politikoje (toliau - Saugumo politika) vartojamos sąvokos turi reikšmę, nurodytą Įstaigos Asmens duomenų tvarkymo taisyklėse.

1.2. Saugumo politika reglamentuoja technines ir organizacines Asmens duomenų saugumo priemones, kurios taikomos Įstaigos tvarkomų Asmens duomenų atžvilgiu.

1.3. Saugumo politika taikoma Įstaigos Darbuotojams, Įstaigos paskirtiems Duomenų tvarkytojams ir jų darbuotojams, tvarkantiems asmens duomenis, nepriklausomai nuo jų priėmimo į darbą sąlygų.

1.4. Įstaigos Darbuotojai, įgalioti tvarkyti Asmens duomenis bei Duomenų tvarkytojų darbuotojai, turi būti supažindinti su Saugumo politika ir privalo jos laikytis.

1.5. DAP pavedama stebėti kaip laikomasi Saugumo politikos.

1.6. Už Saugumo politikos II ir III skyriuose nurodytų reikalavimų vykdymo kontrolę atsakingas Saugumo specialistas, IT specialistas, jei II ir III skyrių atskiruose papunkčiuose nenurodyta kitaip.

II SKYRIUS
ORGANIZACINĖS DUOMENŲ SAUGUMO PRIEMONĖS

2.1. Asmens duomenų saugumo politika ir procedūros

2.1.1. Asmens duomenų ir jų tvarkymo saugumas Įstaigoje yra dokumentuotas kaip informacijos saugumo politikos dalis Saugumo politikoje ir kituose Dokumentuose.

2.1.2. Dokumentai peržiūrimi ir prireikus atnaujinami ne rečiau kaip kartą per pusmetį.

2.1.3. Dokumentai nustato: personalo pareigas (funkcijas) ir atsakomybes, pagrindines technines ir organizacines priemones, įdiegtas Asmens duomenų saugumui užtikrinti, taip pat Duomenų tvarkytojų ar Trečiųjų asmenų, susijusių su Asmens duomenų tvarkymu, sąrašą. Pastarųjų asmenų sąrašas pateikiamas Įstaigos duomenų tvarkymo veiklos įrašuose.

2.1.4. Dokumentų sąrašas yra įtvirtintas Taisyklėse ir yra prižiūrimas Saugumo specialisto.

2.2. **Vaidmenys ir atsakomybės**

2.2.1**.** Su Asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės yra aiškiai apibrėžti ir paskirstyti Dokumentuose.

2.2.2. Jei DAP, Saugumo specialistas, IT specialistas ar kitas asmuo, paskirtas atsakingu už Dokumentų ar juose nurodytų pareigų įgyvendinimą negali vykdyti jam priskirtų pareigų dėl bet kokios laikinos ar nuolatinės priežasties (liga, atostogos, Darbuotojų atleidimas), jas vykdo

tiesioginio tokio asmens vadovo paskirtas asmuo, o jei tiesioginis vadovas tokio asmens nepaskiria, tiesioginis vadovas. DAP funkcijų Įstaigos vadovas negali vykdyti, jis nedelsiant paskiria kitą asmenį laikinai ar nuolatos eiti DAP pareigas. Tuo atveju, jei naikinama pareigybė ar keičiama Įstaigos organizacinė struktūra, Įstaigos vadovas privalo apie tai pranešti Saugumo specialistui ir Saugumo specialistas privalo pasiūlyti atitinkamus Dokumentų pasikeitimus, kurie būtų patvirtinti ir įsigalioti iki pakeitimų įgyvendinimo ir, kurie atspindėtų įvykusius pasikeitimus, tokiu būdu, kad būtų užtikrintas atsakingų Darbuotojų funkcijų ir pareigų nepertraukiamas perimamumas. Įstaigos organizacinė struktūra pagal pareigybes pridedama prie Saugumo politikos kaip Priedas Nr. 1. Dokumentuose gali būti įtvirtintos šiame punkte nurodytos taisyklės išimtys.

2.2.3. DAP, IT specialistas ir Saugumo specialistas yra paskiriami Įstaigos vadovo įsakymu.

2.2.4. DAP negali būti paskirtas Saugumo specialistas ar IT specialistas, tačiau Saugumo specialistas ir IT specialistas gali būti vienas asmuo.

2.3. Prieigos valdymo politika

2.3.1. Prieigos teisės prie Įstaigos informacinių sistemų, kuriose tvarkomi Asmens duomenys, pagal konkrečias pareigybes tvirtinamos Įstaigos vadovo įsakymu, Saugumo specialisto siūlymu. Prieigos teises konkretiems Darbuotojams suteikia ir registruoja Saugumo specialistas. Prieigos teisės yra nustatomos, atsižvelgiant į kiekvieno Darbuotojo pareigas, vykdomas funkcijas. Saugumo specialistas turi užtikrinti, kad tik Darbuotojai, kuriems suteiktas leidimas naudotis Įstaigos informacinėmis sistemomis, kuriose tvarkomi Asmens duomenys, turėtų prieigą tik prie tų Asmens duomenų, kuriems taikomas jų prieigos leidimas (prieigos duomenų kontrolė). Tais atvejais, kai būtina nukrypti nuo Prieigos teisių suteikimo taisyklių (Priedas Nr. 9 prie Taisyklių), arba reikia pavaduoti konkretų Darbuotoją, prieigos teises suteikia Saugumo specialistas, tiesioginio konkretaus Darbuotojo vadovo siūlymu, veda tokių prieigos teisių sąrašą.

2.3.2. Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, yra priskiriamos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. *need to know*) principu.

2.3.3. Įstaiga, suteikdama prieigą prie informacijos, taip pat vadovaujasi šiais principais: mažiausių privilegijų principas – naudotojams suteikti leidimai turi atitikti paskirtį, kuriai informacija bus naudojama; ir pareigų atskyrimo principas – sprendimai dėl prieigos teisių turi būti priimami atsižvelgiant į galimus interesų konfliktus. Didelės prieigos teisės, gali būti priskirtos tik ribotam Darbuotojų skaičiui.

2.3.4. Prieigos kontrolės politika yra įtvirtinta Saugumo politikoje bei įgyvendinta Prieigos teisių suteikimo taisyklėse (Priedas Nr. 9 prie Taisyklių).

2.3.5. Jeigu Darbuotojas atleidžiamas iš darbo, pasikeičia jo funkcijos ir dėl to reikia keisti/naikinti prieigos teises, jo tiesioginis vadovas nedelsiant apie tai informuoja Saugumo arba IT specialistą, kuris atitinkamai imasi tokių veiksmų - nedelsdamas išbraukia jį iš vartotojų sąrašo, panaikindamas suteiktą adresą elektroninio pašto serveryje ir kitus prisijungimus ar prieigas prie visų informacinių sistemų, arba nustato vartotojo prieigos panaikinimo terminą, paskutinę jo darbo dieną, ar pakeičia prieigos teises.

2.3.6. Be 3.3 (v) punkte nurodytų prieigų teisių panaikinimo, Darbuotojo darbo santykių su Įstaiga nutraukimo procedūras sudaro (įgyvendinimą užtikrina darbuotojo tiesioginis vadovas):

a) fizinio priėjimo panaikinimą (pvz. raktų paėmimas);

b) Įstaigos kompiuterinės ir programinės įrangos perėmimą, jei ji buvo suteikta Darbuotojui;

c) bet kokių bendrų slaptažodžių ir PIN, kuriuos žinojo Darbuotojas, pakeitimą.

2.4. Išteklių ir turto valdymas

2.4.1. 2.4.1. Saugumo specialistas ir/ar IT specialistas veda IT išteklių (naudojamų asmens duomenims tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą) (forma Priedas Nr. 10 prie Taisyklių).

2.4.2. IT išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas pagal poreikį, tačiau ne rečiau, kaip kartą per pusmetį.

2.5. **Keitimų valdymas**

2.5.1. Visi esminiai IT sistemų keitimai turi būti stebimi ir registruojami Saugumo ir/ar IT specialisto.

2.5.2. Programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant asmens duomenis. Testuojant sistemas, reikia naudoti testinius duomenis. Tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros.

2.5.3. Visais atvejais esminiai IT sistemų keitimai privalo būti derinami su DAP, Saugumo specialistu ir/ar IT specialistu. Saugumo specialistas ir/ar IT specialistas pasirūpina kad tiek dokumentiškai, tiek techniškai būtų įgyvendinti pareigybių ir vartotojų teisių pakeitimai arba paveda tai padaryti kitiems asmenims.

2.6. **Duomenų tvarkytojai**

Duomenų tvarkytojų atrinkimo, Asmens duomenų tvarkymo sutarties sudarymo ir Duomenų tvarkytojų kontrolės procedūros yra įtvirtintos Taisyklėse.

2.7. **Asmens duomenų saugumo pažeidimai ir saugumo incidentai**

Reagavimo į saugumo incidentus planas, užtikrinantis veiksmingą incidentų, susijusių su Asmens duomenų saugumu, valdymą, saugumo incidentų fiksavimo, pranešimo, likvidavimo reikalavimai, atsakingų asmenų pareigos, nustatyti Asmens duomenų saugumo pažeidimų reagavimo tvarkos apraše (Priedas Nr. 6 prie Taisyklių).

2.8. **Veiklos tęstinumas**

Pagrindinės procedūros, kurių reikia laikytis saugumo incidento ar Asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas, garantuotos paslaugų kokybės lygis yra įtvirtinti Asmens duomenų saugumo pažeidimų reagavimo tvarkos apraše (Priedas Nr. 6 prie Taisyklių) ir Duomenų tvarkymo informacinės sistemos veiklos tęstinumo valdymo plane (Priedas Nr. 8 prie Taisyklių).

2.9. **Personalo konfidencialumas**

2.9.1. Įstaiga užtikrina, kad visi Darbuotojai suprastų savo atsakomybes ir įsipareigojimus, susijusius su asmens duomenų tvarkymu, supažindinant Darbuotojus su Dokumentais bei vykdant mokymus. Vaidmenys ir atsakomybės yra aiškiai išdėstyti Darbuotojams Dokumentuose, darbo sutartyse, pareiginiuose nuostatuose, su kuriais Darbuotojai supažindinami prieš pradedant vykdyti jiems paskirtas funkcijas ir darbus.

2.9.2. Darbuotojai, prieš pradėdami eiti savo pareigas, turi pasirašyti konfidencialumo pasižadėjimą.

2.9.3. Už Konfidencialumo susitarimų su Darbuotojais sudarymą ir įsegimą į Darbuotojo bylą yra atsakingas DAP.

2.10. **Mokymai**

2.10.1. Darbuotojų mokymai apie duomenų apsaugą Įstaigoje yra vykdomi Taisyklėse nustatyta tvarka.

2.10.2. Mokymų metu Darbuotojai informuojami apie IT sistemų saugumo reikalavimus, susijusius su jų kasdieniu darbu. Darbuotojai, susiję su Asmens duomenų tvarkymu, mokomi apie atitinkamus duomenų saugumo reikalavimus ir atsakomybes, rengiant reguliarius mokymus, informavimo renginius ar instruktažus.

2.10.3. Saugumo specialistas turi rengti personalo mokymų programas, tarp kurių būtų ir speciali programa, skirta mokyti naujus Darbuotojus (duomenų apsaugos tema).

2.10.4. Mokymus veda DAP arba išorinis paslaugų teikėjas.

III SKYRIUS
TECHNINĖS DUOMENŲ SAUGUMO PRIEMONĖS

3.1. **Prieigų kontrolė ir autentifikavimas**

3.1.1. Įstaigoje įgyvendinta prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema leidžia kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras.

3.1.2. Bendrų naudotojų paskyrų naudojimas leidžiamas tik išimtiniais atvejais, iš anksto patvirtinus Saugumo ir/ar IT specialistui. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas.

3.1.3. Įstaigoje yra veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį.

3.1.4. Įstaigoje nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Taisyklės įtvirtintos Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos apraše (Priedas Nr. 5 prie Taisyklių).

3.1.5 Privilegijuotiems vartotojams (pvz., sistemų administratoriams) prisijungimui prie Asmens duomenų tvarkymo sistemų, kuriose dideliu mastu tvarkomi Specialių kategorijų ar pažeidžiamų asmenų (pvz. vaikai) asmens duomenys (toliau – **Ypatingos sistemos**), turi būti taikomas dviejų veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamas dviejų veiksnių autentifikavimas. Autentifikavimo veiksniais gali būti slaptažodžiai, USB raktai ir kt.

3.2. **Darbo vietų apsauga**

3.2.1. Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų.

3.2.2. Naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotos programinės įrangos.

3.2.3. Ekrano užsklandą galima pašalinti tik įvedus slaptažodį arba PIN kodą. Penkis kartus įvedus neteisingą slaptažodį arba PIN kodą, prietaisas turi užsiblokuoti, taip, kad jį atblokuoti galėtų tik IT specialistas.

3.2.4. Mobiliuose įrenginiuose turi būti nustatyta, kad nedirbant su jais ne ilgiau kaip 2 minutes, įsijungtų ekrano užsklanda, kurią būtų galima pašalinti tik įvedus, slaptažodį,. Už šių reikalavimų vykdymą atsakingas Darbuotojas, naudojantis įrenginį.

3.2.5. Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.

3.2.6. Antivirusinės taikomosios programos ir jų informacijos apie virusus bei kenkimo programinę įrangą duomenų bazės turi būti reguliariai atnaujinamos.

3.2.7. Draudžiama perduoti asmens duomenis iš kompiuterinių darbo vietų, kuriose dideliu mastu tvarkomi pažeidžiamų asmenų ar Specialių kategorijų asmens duomenys, į išorinius saugojimo įrenginius (pvz., USB raktai, išorinius standžiuosius diskus ir kt.). Už šio draudimo laikymąsi atsako kiekvienas naudotojas.

3.3. **Tinklo ir komunikacijos sauga**

3.3.1. Belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių.

3.3.2. Nuotolinė prieiga Darbuotojams suteikiama Darbuotojo prašymu patvirtinus jo tiesioginiam vadovui. Darbui per nuotolį ir techninei įrangai taikomi tokie patys reikalavimai, kaip ir fiziškai dirbant Įstaigoje. Kilus įtarimų, kad dėl nuotolinio darbo gali būti pažeistas Asmens duomenų konfidencialumas, prieiga panaikinama.

3.4. **Mobilieji, nešiojamieji įrenginiai**

3.4.1. Mobiliųjų, nešiojamųjų įrenginių administravimo procedūros nustatytos ir dokumentuotos Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos apraše (Priedas Nr. 5 prie Taisyklių).

3.4.2. Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti.

3.4.3. Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga Asmens duomenims tvarkyti.

3.4.4. Mobiliųjų, nešiojamųjų įrenginių valdymo funkcijos ir atsakomybės apibrėžtos Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos apraše (Priedas Nr. 5 prie Taisyklių).

3.5. **Duomenų naikinimas, šalinimas**

3.5.1. Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys. Jei to padaryti neįmanoma (pvz., DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti.

3.5.2. Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis

3.5.3. Jei būtina, prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai (angl. *Multiple passes of software-based overwriting*).

3.5.4. Jei saugiems duomenų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti sudaryta atitinkama paslaugų sutartis ir atliekamas sunaikintų įrašų protokolavimas.

3.5.5. Po dideliu mastu tvarkomų pažeidžiamų asmenų ir Specialių kategorijų asmens duomenų ištrynimo, reikėtų imtis papildomų priemonių., Priklausomai nuo konkretaus atvejo, reikėtų įvertinti fizinio sunaikinimo galimybes.

3.5.6. Kiek tai liečia pažeidžiamų asmenų ar Specialių kategorijų asmens duomenų tvarkymą dideliu mastu, jei saugiems įrašų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos Trečiojo asmens paslaugos, turi būti užtikrinta, kad šis procesas vyktų Įstaigos patalpose, siekiant išvengti Asmens duomenų perdavimo Tretiesiems asmenims. Atskirais atvejais, kai to neįmanoma atlikti Įstaigos patalpose, sunaikinimas gali būti atliekamas kitoje fizinėje vietoje, tačiau tik stebint įgaliotam Įstaigos atstovui.

3.6. **Fizinė sauga**

3.6.1. Įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.

3.6.2. Būtina naudoti aiškią visų Darbuotojų ir lankytojų identifikavimo sistemą, naudojant tinkamas priemones.

3.6.3. Patalpose įrengta signalizacija ir vaizdo kameros.

3.6.4. Prireikus turi būti kuriamos fizinės kliūtys, kad būtų užkirstas kelias neteisėtam fiziniam prieinamumui.

3.6.5. Laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos.

3.6.6. Išorės subjektų personalui, įgyvendinančiam teikiamas palaikymo paslaugas, turi būti suteikta ribota prieiga prie saugių zonų.

3.6.7. Darbuotojai privalo laikytis švaraus stalo principo.

3.6.8. Atspausdinti dokumentai nedelsiant, ne vėliau kaip per 3 min. turi būti paimti nuo spausdintuvo.

PRITARTA
Kelmės „Kūlverstuko“ lopšelio-darželio
įstaigos tarybos 2026 m. vasario 4 d.
posėdžio protokoliniu nutarimu
(2026-02-04 posėdžio protokolas NR. ĮT-1)

SUDERINTA
Milda Alijošienė
Kelmės „Kūlverstuko“ lopšelio-darželio
profesinės sąjungos pirmininko pavaduotoja
2026-02-17

Priedas Nr. 1

PATVIRTINTA
Kelmės „Kūlverstuko“ lopšelio-darželio
direktoriaus 2024 m. rugsėjo 2 d.
įsakymu Nr. V-590

KELMĖS „KŪLVERSTUKO“ LOPŠELIO-DARŽELIO STRUKTŪRA

