PATVIRTINTA
Vilniaus lopšelio-darželio „Saulėtekis“
direktoriaus 2022 m. balandžio 20 d.
įsakymu Nr. V-26 (1.8.)

VILNIAUS LOPŠELIO-DARŽELIO „SAULĖTEKIS“ INFORMACINIŲ IR KOMUNIKACINIŲ TECHNOLOGIJŲ NAUDOJIMO BEI DARBUOTOJŲ STEBĖSENOS IR KONTROLĖS DARBO VIETOJE TVARKA,

priimta pagal 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo duomenų judėjimo nuostatas

1. Tvarkos tikslas – užtikrinti Vilniaus lopšelio-darželio „Saulėtekis“, įstaigos kodas 190014157, buveinės adresas Genių g. 12, LT-11219 Vilnius (toliau – „Įstaiga“), darbuotojo privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis (toliau – „Tvarka“).

2. Įstaiga, atsižvelgiant į darbuotojo einamas pareigas, savo nuožiūra darbuotojams suteikia darbo priemones. Įstaigai priklausančios Informacinės ir komunikacinės technologijos, t. y. kompiuteriai, mobilieji telefonai, prieiga prie interneto, elektroninis paštas, spausdintuvai, duomenų laikmenos ir kiti prietaisai, – yra skirtos išimtinai darbuotojų darbo funkcijoms vykdyti, jeigu Įstaiga su darbuotoju nesusitaria kitaip.

3. Visuose kompiuteriuose, kurie jungiami į kompiuterinį tinklą, turi nuolat veikti antivirusinė programa su naujausia virusų aprašymų duomenų baze.

4. Darbuotojas, palikdamas savo darbo vietą ilgesniam nei 30 minučių laikui, privalo išjungti visas programas, duomenų bazes. Galima palikti tik operacinės sistemos darbalaukį.

5. Bendros apsaugos nuo virusų taisyklės:

5.1. Prieš naudojant nežinomas išorines duomenų laikmenas arba kurios buvo naudojamos kitame kompiuteryje, būtina atlikti jų antivirusinę profilaktiką;

5.2. Kilus įtarimui patikrinti kompiuterį nuo virusų;

5.3. Siekiant išvengti kompiuterinių virusų, nepaleisti nežinomų programų. Gavus nežinomų siuntėjų atsiųstų elektroninių laiškų priedus, kuriuose gali būti kompiuterinių virusų, darbuotojas privalo neatidaryti gautų elektroninių laiškų priedų ir informuoti tiesioginį arba Įstaigos vadovą;

5.4. Darbuotojas, pastebėjęs virusų atakos požymius, privalo išjungti kompiuterį ir kreiptis į tiesioginį arba Įstaigos vadovą.

6. Darbuotojas neturi teisės savavališkai keisti jam priskirtos kompiuterinės įrangos (monitoriai, skeneriai, spausdintuvai bei kopijavimo aparatų spausdinimo valdikliai, klaviatūros, pelės, kolonėlės, ausinės, vaizdo kameros bei fotokameros, multimedijos projektoriai ir pan.) ir įdiegtos programinės įrangos.

7. Darbuotojams, naudojantiems elektroninį paštą, interneto prieigą ir kitą informacinių technologijų ir telekomunikacijų įrangą, draudžiama;

7.1. Siųsti elektroninio pašto žinutes, naudojantis kito asmens arba neegzistuojančiu elektroninio pašto adresu;

7.2. Siųsti elektroninio pašto žinutes, nuslepiant savo tapatybę;

7.3. Negavus Įstaigos vadovo sutikimo, siųsti elektroninius laiškus, kuriuose yra informacija pripažįstama konfidencialia informacija ar Įstaigos komercine paslaptimi, išskyrus, jei informacija siunčiama asmeniui, kuris turi teisę gauti šią informaciją;

7.4. Negavus Įstaigos vadovo sutikimo perduoti, platinti, atskleisti tretiesiems asmenims darbui su technine ir programine įranga jiems suteiktus prieigos vardus, slaptažodžius ar kitus duomenis;

7.5. Kurti ar platinti laiškus, skatinančius gavėją siųsti laiškus kitiems. Laiškai su perspėjimais dėl kompiuterinių virusų, telefonų pasiklausymų ar kitų tariamų reiškinių, kuriuose prašoma nusiųsti gautą laišką visiems savo kolegoms, draugams ar pažįstamiems, turi būti nedelsiant ištrinami. Jei pranešimas sukelia įtarimų, prieš jį pašalinant, pranešti tiesioginiam arba Įstaigos vadovui;

7.6. Naudoti interneto prieigą ir elektroninį paštą asmeniniams tikslams, Lietuvos Respublikos įstatymais draudžiamai veiklai, šmeižiančio, įžeidžiančio, grasinančiojo pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujančiai informacijai, kompiuterių virusams, masinei nepageidaujamai informacijai „spam“ siųsti ar kitiems tikslams, galintiems pažeisti Įstaigos ar kitų asmenų teisėtus interesus;

7.7. Atlikti veiksmus, pažeidžiančius fizinio ar juridinio asmens teises, kurias saugo autorių, gretutinių ir intelektinės nuosavybės teisių apsaugos įstatymai. Tarp tokių veiksmų yra programinės įrangos diegimas, naudojimas, saugojimas arba platinimas neturint licencijos, neleistinas autorių teisėmis apsaugotų kūrinių kopijavimas;

7.8. Parsisiųsti arba platinti tiesiogiai su darbu nesusijusią grafinę, garso ir vaizdo medžiagą, žaidimus ir programinę įrangą, siųsti duomenis, kurie užkrėsti virusais, turi įvairius kitus programinius kodus, bylas, galinčias sutrikdyti kompiuterinių ar telekomunikacinių įrenginių bei programinės įrangos funkcionavimą ir saugumą;

7.9. Atskleisti prisijungimo prie Įstaigos sistemų informaciją (prisijungimo vardą, slaptažodį) arba leisti naudotis savo prisijungimo vardu kitiems asmenims; Dirbant su slaptažodžiais reikia laikytis taisyklių:

7.9.1 Saugoti slaptažodį. Neužrašinėti jo ant popieriaus skiaučių, kalendorių ir pan. Nepalikti lapelio su slaptažodžiu priklijuoto prie vaizduoklio arba prie apatinės darbo stalo pusės;

7.9.2 Nenaudoti trumpų ir elementarių slaptažodžių sudarytų iš reikšminių žodžių.

7.9.3 Pažeisti bet kurio kompiuterio, tinklo ar paskyros autentifikacijos arba saugumo sistemas;

7.9.4 Ardyti ar išmontuoti ar kitaip keisti kompiuterinę įrangą;

7.9.5 Perkopijuoti programinę įrangą;

7.9.6 Savarankiškai šalinti kompiuterinės įrangos gedimus;

7.9.7 Parsisiųsti ar žaisti internetinius ar kitus kompiuterinius žaidimus;

7.9.8 Savavališkai blokuoti antivirusines programas ar kitas programas;

7.9.9 Sutrikdyti kompiuterinės sistemos darbą arba panaikinti galimybę naudotis teikiama paslauga ar informacija;

7.9.10 Dalyvauti interneto lažybose ir azartiniuose lošimuose;

7.9.11 Naudoti Įstaigos išteklius komercinei veiklai vystyti ar naudai gauti;

7.9.12 Savavališkai keisti kompiuterių ar kitų prietaisų tinklo parametrus (IP adresą ir pan.), savarankiškai keisti, taisyti informacinių technologijų ir telekomunikacijų techninę ir programinę įrangą;

7.9.13 Pažeisti kitų tinklų, kurių paslaugomis naudojamasi, naudojimo arba ekvivalentiškas taisykles;

7.9.14 Savavališkai keisti interneto naršyklės ir elektroninio pašto programinės įrangos parametrus, susijusius su apsauga arba prisijungimo būdu, nepaisyti bet kurio iš įdiegtų saugumo mechanizmų;

7.9.15 Atlikti bet kokius kitus su darbo funkcijų vykdymu nesusijusius ir teisės aktams prieštaraujančius veiksmus;

7.9.16 Neįgaliotiems asmenimis Įstaigoje ar už Įstaigos naudoti ir perduoti slaptažodžius ir kitus duomenis, kuriais pasinaudojus programinėmis ir techninėmis priemonėmis galima sužinoti Įstaigos duomenis ar kitaip sudaryti sąlygas susipažinti su Įstaigos duomenimis.

8. Keitimosi informacija politika.

8.1. Perduodant informaciją elektroniniu paštu, būtina:

8.1.1 Atidžiai užrašyti adresato elektroninio pašto adresą, kad informacija nebūtų perduota kitam asmeniui;

8.1.2 Už organizacijos ribų siunčiamiems laiškams naudoti el. pašto programoje numatytą el. laiško parašą (signature) ir jo nekeisti;

8.1.3 Priimant sprendimus pagal elektroniniu paštu gautą informaciją, būtina įsitikinti šios informacijos tikrumu (kitas asmuo gali apsimesti tikruoju siuntėju). Kilus įtarimui bei svarbiais atvejais rekomenduojama susisiekti su siuntėju ir įsitikinti ar gautas laiškas buvo jo išsiųstas.

8.2. Neatverti pridėtų (angl. „attached") failų, kurie yra gauti iš nepažįstamų asmenų, arba nėra galimybės įsitikinti šių failų turiniu.

8.3. Už pašalinių asmenų naudojimąsi internetu kompiuteryje ir informacijos perdavimą elektroniniu paštu yra atsakingas kompiuterio naudotojas.

8.4. Darbuotojai, naudojantys Įstaigos kompiuterinę techninę ir programinę įrangą privalo:

8.4.1 Kompiuterinę techninę ir programinę įrangą, elektroninio pašto ir interneto paslaugas naudoti tik darbo funkcijoms atlikti;

8.4.2 Kompiuterines programas naudoti vadovaujantis konkrečių kompiuterinių programų licencijų reikalavimais bei šia tvarka.

9. Nuotolinio darbo politika.

9.1. Nuotoliniam Įstaigos darbuotojų prisijungimui prie Įstaigos kompiuterių tinklo yra taikomi tokie pat saugumo standartai kaip ir lokaliam prisijungimui.

9.2. Asmenys, atliekantys nuotolinį prisijungimą turi užtikrinti, kad jų šeimos nariai ar pašaliniai asmenys neprieitų prie organizacijos duomenų ir kompiuterinės įrangos, nepažeistų organizacijos informacijos saugumo valdymo sistemos nuostatų.

9.3. Nuotoliniu būdu dirbantis darbuotojas turi laikytis šių reikalavimų:

9.3.1 Niekam neatskleisti prisijungimo ir kitų slaptažodžių;

9.3.2 Užtikrinti, kad kompiuterinė įranga nuotolinio prisijungimo prie organizacijos Tinklo metu nėra prisijungusi prie kitų išorinių tinklų;

9.3.3 Nenaudoti organizacijos informacinių resursų su darbu nesusijusiai veiklai;

9.3.4 Nekeisti nuotolinio prisijungimo įrangos parametrų;

9.3.5 Užtikrinti, kad nuotoliniu būdu prijungtame kompiuteryje naudojama operacinė sistema ir antivirusinė programinė įranga būtų reguliariai atnaujinama.

10. Nešiojamųjų kompiuterių naudojimo tvarka.

10.1. Nešiojamojo kompiuterio negalima palikti be priežiūros viešose vietose ir transporto priemonėse;

10.2. Keliaujant draudžiama nešiojamąjį kompiuterį atiduoti į lėktuvo, autobuso, traukinio ar kitos transporto priemonės bagažo skyrių, nebent vežėjo taisyklės reikalauja kitaip;

10.3. Dirbant viešose vietose, nešiojamasis kompiuteris turi būti tokioje padėtyje, kad pašaliniai asmenys negalėtų matyti ekrane rodomos informacijos;

10.4. Nesinaudojant nešiojamuoju kompiuteriu jį būtina išjungti, išregistruoti iš naudotojo paskyros arba užrakinti operacinę sistemą taip, kad jungiantis iš naujo reikėtų įvesti naudotojo vardą ir slaptažodį;

10.5. Draudžiama leisti naudotis nešiojamaisiais kompiuteriais pašaliniams asmenims. Draudžiama perduoti tretiems asmenims nešiojamame kompiuteryje esančios informacijos kopijas. Draudžiama naudoti nešiojamąjį kompiuterį neteisėtai veiklai vykdyti;

10.6. Draudžiama keisti nešiojamojo kompiuterio, jame esančios programinės įrangos techninius parametrus;

10.7. Nešiojamame kompiuteryje draudžiama diegti su darbu nesusijusią programinę įrangą;

10.8. Praradus nešiojamąjį kompiuterį, apie tai reikia nedelsiant pranešti tiesioginiam vadovui;

10.9. Visi aukščiau išvardinti reikalavimai yra taikomi (kiek tai techniškai yra įmanoma) ir kitiems organizacijoje naudojamiems nešiojamiems prietaisams, galintiems talpinti ir apdoroti informaciją (pvz. delniniai kompiuteriai, mobilūs telefonai ir pan.).

11. Įstaigos vadovas neužtikrina, kad bus išsaugotas privatumas to, ką Įstaigos darbuotojai sukuria, siunčia ar gauna Įstaigos informacinėje sistemoje.

12. Organizuojant stebėseną laikomasi proporcingumo, tikslingumo, skaidrumo, saugumo, tikslumo ir duomenų išsaugojimo bei būtinumo principų, ir stebėsenos priemonės taikomos tik tais atvejais, kai iškeltų tikslų kitomis, mažiau darbuotojų privatumą ribojančiomis priemonėmis, pasiekti neįmanoma arba, Įstaigos vertinimu, yra nepraktiška.

13. Stebėsenos ir kontrolės darbo vietoje tikslai:

13.1. Apsaugoti konfidencialius Įstaigos duomenis nuo atskleidimo tretiesiems asmenims;

13.2. Apsaugoti Įstaigos klientų ir darbuotojų asmens duomenis nuo neteisėto perdavimo tretiesiems asmenims;

13.3. Apsaugoti Įstaigos informacines sistemas nuo įsilaužimų ir duomenų vagysčių, virusų, pavojingų interneto puslapių, kenkėjiškų programų;

13.4. Apsaugoti Įstaigos turtą ir užtikrinti asmenų saugumą Įstaigos patalpose ar teritorijoje;

13.5. Apsaugoti Įstaigos turtinius interesus ir užtikrinti darbo pareigų laikymąsi.

14. Įstaiga pasilieka teisę be atskiro darbuotojo įspėjimo riboti prieigą prie atskirų interneto svetainių ar programinės įrangos. Nepakankant minėtų priemonių, Įstaiga gali tikrinti, kaip darbuotojas laikosi elektroninio pašto ir interneto resursų naudojimo reikalavimų nurodytais tikslais, tiriant incidentus, atiduoti darbuotojų naudojamą įrangą tirti tretiesiems asmenims, kurie teisės aktų nustatyta tvarka turi teisę tokius duomenis gauti.
