

## PALANGOS MIESTO SOCIALINIŲ PASLAUGŲ CENTRO INFORMACINIŲ TECHNOLOGIJŲ SAUGUMO TVARKOS APRAŠAS

### I BENDROSIOS NUOSTATOS

1. **Informacinių technologijų saugumo tvarkos aprašo (toliau – Aprašas) tikslas**-teisiniam ir finansiniam saugumui užtikrinti Palangos miesto socialinių paslaugų centre (toliau- Centras).
2. Politika parengta vadovaujantis Valstybinės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtinu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716:  
„Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio aprašo ir Valstybinės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, 2019 m. gruodžio 18 d. Valstybinės duomenų apsaugos inspekcijos gairėmis „Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams“.
3. Informacijos saugumo valdymas Centre yra svarstomas ir tikslinamas pagal organizacinę struktūrą, funkcijas ir atsakomybę, veiklos strategiją ir tikslus, pajėgumus ir išteklius, informacijos sistemas ir procesus.
4. Aprašo tikslas: apibrėžti bendruosius informacijos saugos reikalavimus, kurie atitiktų Centro veiklos strategiją, poreikius, galiojančius teisės aktus, bei užtikrintų Centro informacinių vertybių apsaugą nuo vidinių ar išorinių tyčinių ar atsitiktinių grėsmių.
5. Aprašas yra privalomas visiems Centro darbuotojams.

### II SAŲVOKOS

6. **Atsakingas asmuo** – už Centro IT sistemų priežiūrą atsakingas: IT priežiūros paslaugas teikiantis išorinis paslaugos teikėjas.
7. **Informacijos apdorojimo priemonės** – priemonės skirtos duomenims apdoroti (struktūruoti, analizuoti, atlikti skaičiavimus ir pan.).

8. **Informacinė sistema** – duomenų surinkimo, apdorojimo, perdavimo ir naudojimo sistema.
9. **Kompiuterinė įranga** – kompiuterių technikos fizinių priemonių visuma, t. y. mechaniniai, magnetiniai, elektriniai, elektroniniai įrenginiai ir įtaisai. Kompiuterinei įrangai priskiriama ne tik kompiuteris, bet ir visi išoriniai įrenginiai bei ryšio priemonės: monitorius, klaviatūra, pelė, spausdintuvas, garsiakalbiai, maitinimo įtaisas, kabeliai, jungtys ir pan.
10. **Konfidencialumas** – užtikrinimas, kad informacija būtų prieinama tik įgaliotiems asmenims, turintiems prieigos prie informacinių sistemų teises.
11. **Vientisumas** – informacijos ir apdorojimo metodų tikslumo ir užbaigtumo užtikrinimas.
12. **Prieinamumas** – užtikrinimas, kad įgaliotieji vartotojai, kai būtina, turėtų prieigą prie informacinių ir bendrų išteklių.
13. **Vartotojas** – kompiuterizuotos darbo vietos priemonės naudojantis darbuotojas ar įgaliotas trečiasis asmuo, nevykdantis jokių specialių informacijos apdorojimo sistemų priežiūros darbų.

### III KOMPIUTERINĖS ĮRANGOS APSAUGA

#### 14. Kompiuterinės įrangos įsigijimas ir instaliavimas

- 14.1. Pagrindiniai kompiuterinės įrangos įsigijimai turi būti vykdomi pagal patvirtintas įsigijimo procedūras.
- 14.2. Kompiuterinės įrangos instaliavimas gali būti vykdomas tik įgaliotų asmenų ir atitikti informacijos apsaugos politikas, tvarkas bei procedūras.

#### 15. Reikalavimai nepertraukiamam elektros maitinimui, spausdintuvams

- 15.1. Centro sistemos ar jų komponentai turi būti aprūpinti nepertraukiamo maitinimo šaltiniais.
- 15.2. Spausdinant slaptą informaciją į tinklo spausdintuvą, būtina užtikrinti informacijos saugumą spausdinimo metu ir po jo. Atspausdinti dokumentai su slapta informacija negali būti palikti spausdintuve, spausdinęs darbuotojas turi juos iš karto paimti.

#### 16. Reikalavimai eksploatacinėms medžiagoms

- 16.1. Naudotis išimamais įrašomais informacijos nešėjais (magnetiniais diskeliais, kompaktiniais diskais, atminties kortelėmis ir t.t.) gali tik darbuotojai, kuriems pagal jų pareigybės aprašymus suteikiama prieiga prie Centro tvarkomų asmens duomenų.
- 16.2. Visos nešiojamos kompiuterinės laikmenos (nešiojamieji kompiuteriai, nešiojami kietieji diskai, CD, DVD, USB atmintinės ir pan.) turi būti saugomos, naudojamos, perduodamos ir naikinamos atsižvelgiant į jose laikomos informacijos pobūdį.
- 16.3. Naikinant nešiojamas kompiuterines laikmenas, kuriose naudojami asmens duomenys, ir jų kategorijos turi būti sunaikinti taip, kad šių dokumentų nebūtų galima atkurti ar atpažinti jų turinio.

#### 17. Kompiuterinės įrangos dokumentacija

- 17.1. Kompiuterinės įrangos dokumentacija turi būti savalaikiai atnaujinama, lengvai suprantama ir prieinama darbuotojams, atsakingiems už jos aptarnavimą ir priežiūrą.
- 17.2. Visa Centro kompiuterinė įranga turi būti inventorizuojama kartą per metus įgalioto darbuotojo.

#### 18. Kiti kompiuterinės įrangos apsaugos klausimai

- 18.1. Nenaudojamos, nereikalingos kompiuterių įrangos šalinimas turi būti vykdomas įgaliotų darbuotojų, kurie turi užtikrinti informacijos apsaugos reikalavimų įvykdymą.
- 18.2. Sugeodus kompiuterinei įrangai, būtina nedelsiant informuoti atsakingus Centro darbuotojus.
- 18.1. Informacija nešiojamuose kompiuteriuose, išmaniuosiuose telefonuose, planšetėse turi būti šifruojama, apsaugota nuo vagysčių, pametimo ar sugadinimo. Kelionės metu įranga turi būti transportuojama kaip rankinis bagažas.
- 18.2. Paliekant darbo vietą, Centro darbuotojas privalo išsiregistruoti iš visų taikomųjų programų.
- 18.3. Siekiant apsaugoti kompiuterį nuo jo neteisėto naudojimo ar informacijos nuskaitymo, visuose Centro naudojamuose kompiuteriuose turi būti naudojamos automatinės ekrano užsklandos vartotojams kurį laiką (pvz., 15 minučių) nedirbant su kompiuteriu.
- 18.4. Įrangą išnešti ar leisti ją išnešti iš Centro patalpų gali tik Centro vadovo įsakymu įgalioti Centro darbuotojai. Šie darbuotojai visiškai atsako už išnešamą įrangos ir joje esančios informacijos apsaugą.

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

##### **19. Programinės įrangos įsigijimas ir instaliavimas**

- 19.1. Centre gali būti naudojama tik licencijuota programinė įranga.
- 19.2. Programinės įrangos diegimą ir atnaujinimą vykdo tik įgalioti ir kvalifikuoti specialistai.
- 19.3. Diegiant informacines sistemas, būtina pakeisti gamintojo ir/ar tiekėjo nustatytus slaptažodžius.

##### **20. Programinės įrangos priežiūra ir atnaujinimas**

- 20.1. Programinės įrangos klaidos turi būti registruojamos. Apie pastebėtas klaidas turi būti informuojami organizacijos ar asmenys, atsakingi už programinės įrangos priežiūrą ir aptarnavimą.
- 20.2. Programų taisymas ir diegimas avariniais atvejais galimas tik informuojant Centro direktorių. Diegimas vykdomas pagal iš anksto paruoštas ir patikrintas pakeitimų procedūras.
- 20.3. Realių duomenų naudojimas testavimui galimas tik tada, jei yra užtikrinamas reikalingas duomenų konfidencialumas ir integralumas.
- 20.4. Vartotojai turi būti reikiamai apmokyti darbui su nauja sistema.
- 20.5. Visos Centro sistemos/programos turi būti išsamiai ir suprantamai dokumentuotos. Sistemos/programos negali būti diegiamos be reikiamos dokumentacijos.

#### **V INFORMACINIŲ SISTEMŲ APSAUGA**

##### **21. Elektroninis paštas ir internetas**

- 21.1. Failų siuntimas iš interneto turi būti ypatingai kontroliuojamas, kad būtų išvengta piktavališkų programų ar netinkamos informacijos gavimo.

- 21.2. Slaptos ar konfidencialios informacijos siuntimas, jei įmanoma, turi būti vykdomas, siunčiant šifruotus elektroninius laiškus.
- 21.3. Gaunami el. laišakai, laiškų turinys turi būti vartotojų peržiūrėti su ypatingu atsargumu. Draudžiama atidarinti laiškuose esančius failus, jei jie nėra patikrinti dėl virusų ir piktavališkų programų arba gauti nuo nežinomų asmenų.
- 21.4. Centro darbuotojai, administruojantys interneto prieigą, turi užtikrinti, kad Centro kompiuterinis tinklas būtų apsaugotas nuo piktavališkų įsiveržimų įdiegiant ugniasienę.
- 21.5. Elektroninio pašto sistemai apsaugoti turėtų būti įdiegta nepageidautinų elektroninių laiškų (angl. *spam*) gavimą ir siuntimą kontroliuojanti sistema.
- 21.6. Susirašinėjant darbo reikalais turi būti naudojamos tik oficialios Centro elektroninio pašto dėžutės.
- 21.7. Centre turi būti naudojamos priemonės, leidžiančios uždrausti ar apriboti darbuotojams naudoti tam tikras interneto sritis. Turėtų būti blokuojami nepageidaujamo turinio internetiniai puslapiai.
- 21.8. Bevielio interneto tinklo prieigai (Wi-Fi) Centro patalpose yra sukonfigūruotos stotelės, skirtos Centro darbuotojams. Bevielis interneto tinklas apsaugotas slaptažodžiu, kurį suteikia ir keičia atsakingas darbuotojas.

## **22. Mobilus ryšio įrenginių naudojimas**

- 22.1. Mobilus ryšio įrenginys Centro darbuotojams suteikiamas tik darbo funkcijoms vykdyti.
- 22.2. Jei mobilus ryšio įrenginyje naudojamas elektroninis paštas, privaloma apriboti priėjimą prie mobilus įrenginio naudojant ekrano užraktą.
- 22.3. Slapta ar konfidenciali informacija negali būti perduodama mobiliaisiais įrenginiais, visiškai neįsitikinus dėl informacijos gavėjo autentiškumo ir jo teisės gauti informaciją.
- 22.4. Slapta ar konfidenciali informacija negali būti įrašinėjama į auto-atsakiklius / balso pašto sistemas.

## **23. Duomenų valdymas ir kontrolė**

- 23.1. Duomenų apdorojimas ar keitimas nestandartinėmis priemonėmis gali būti naudojamas tik išskirtiniais (avariniais) atvejais ir pagal šiems atvejams numatytas procedūras.
- 23.2. Informaciją iš magnetinių diskelių, kompaktinių diskų ar kitų nešiojamų informacijos laikmenų nuskaityti gali tik atitinkamas teisės turintys darbuotojai.
- 23.3. Duomenų archyvavimas ar saugojimas turi būti vykdomas atsižvelgiant į teisinius, techninius reikalavimus bei Centro vidinius veiklos dokumentus.
- 23.4. Personaliniuose ir nešiojamuose kompiuteriuose esantys laikini failai turi būti periodiškai šalinami.

## **24. Rezervinis kopijavimas, atstatymas, archyvavimas**

- 24.1. Atsakingas darbuotojas turi užtikrinti, kad informacinių sistemų rezervinio kopijavimo ir atstatymo procedūros yra paruoštos, vykdomos ir veikia korektiškai.
- 24.2. Svarbūs duomenys, esantys nešiojamuose kompiuteriuose, turi būti periodiškai kopijuojami. Kompiuterio vartotojas atsakingas už vykdomo rezervinio kopijavimo reguliarumą.
- 24.3. Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis.
- 24.4. Pilnos atsarginės duomenų kopijos daromos kas savaitę, pridedamosios atsarginės duomenų kopijos daromos kasdien.

## **25. Popierinių dokumentų valdymas**

25.1. Dokumentų su svarbia informacija savininkai turi užtikrinti reikiamą informacijos apsaugą dokumentų transportavimo metu.

25.2. Nereikalingos konfidencialių ar slaptų dokumentų kopijos turi būti sunaikintos dokumentų naikinimui pritaikytais smulkintuvais.

## **26. Apsauga nuo kenkėjiškų programų**

26.1. Visuose Centro kompiuteriuose turi veikti reguliariai atnaujinama antivirusinė programinė įranga.

26.2. Kompiuterinio viruso, kirmino ar kitos piktavališkos programos patekimas į Centro tinklą yra traktuojamas kaip labai pavojingas informacijos saugumo incidentas. Kiekvienu tokio incidento atveju turi būti nustatyti ir užkirsti piktavališkų programų patekimo į Centro tinklą keliai, turi būti ištirtas visas toks incidentas.

## **27. Informacijos apsaugos incidentai**

27.1. Išsami duomenų apsaugos pažeidimų valdymo tvarka pateikiama Centro Asmens duomenų saugumo priežiūros valdymo tvarkos apraše.

27.2. Įstatymuose numatytais atvejais apie informacijos saugumo incidentus turi būti informuojamos išorinės organizacijos. Tai gali atlikti tik Centro direktoriaus įgalioti atstovai.

27.3. Visi informacijos apsaugos incidentai turi būti registruojami.

27.4. Informacija apie incidentus ir jų tyrimus yra konfidenciali.

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

28. Prieiga prie visų Centro naudojamų informacinių sistemų, tinklų, duomenų bazių ar saugyklų internete yra draudžiama, išskyrus kai Centro informacinių sistemų naudotojui yra aiškiai suteiktos prieigos teisės.

29. Prieiga darbuotojui prie konkrečios informacinės sistemos suteikiama remiantis „būtinumo žinoti“ principu. Prieiga prie Centro informacinių sistemų nesuteikia darbuotojui teisių peržiūrėti ir naudoti visą informacinėse sistemose esančią informaciją.

30. Prieigos teisės suteikiamos ir darbuotojo paskyra informacinėse sistemose sukuriama naudojant šiuos asmens duomenis: vardą, pavardę, duomenis, jungiantis el. parašu arba el. bankininkyste. Naudojamų asmens duomenų apimtis atskirose Centro naudojamose informacinėse sistemose gali skirtis.

31. Sprendimą dėl prieigos teisių suteikimo konkrečiam Centro darbuotojui priima Centro vadovas.

32. Prieigos prie Centro sistemų slaptažodžiai, keičiami ir saugomi užtikrinant jų konfidencialumą, yra unikalūs iš ne mažiau kaip 7 simbolių (slaptažodyje turi būti didžioji raidė), nenaudojant asmeninio pobūdžio informacijos, keičiami susidarius tam tikroms aplinkybėms (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims ir pan.) ir naudotojo pirmojo prisijungimo metu. Centro darbuotojas prieigos prie asmens duomenų slaptažodžiais turi naudotis asmeniškai ir neatskleisti jų tretiesiems asmenims.

33. Darbuotojas turi teisę susipažinti su Centro konfidencialia informacija tik tais atvejais, jeigu darbuotojui tokie įgaliojimai suteikti pagal darbo sutartį, pareigines instrukcijas ar tokius įgaliojimus konkrečiam darbuotojui suteikė Centras.
34. Centro darbuotojai ar išoriniai paslaugų teikėjai, kuriems Centras suteikė prieigą prie Centro naudojamų informacinių sistemų, privalo laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino vykdydami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas.
35. Atsakingas darbuotojas reguliariai, bet ne rečiau kaip kartą per 6 mėnesius, peržiūri suteiktas prieigos prie Centro informacinių sistemų teises, ir, jei reikia, panaikina ar pakeičia suteiktas teises.
36. Prieigos teisės trečiosioms šalims (duomenų tvarkytojams) suteikiamos tik pasirašius sutartį, kurioje turi būti nustatytos duomenų tvarkymo sąlygos, nurodomos duomenų tvarkytojo taikomos techninės ir organizacinės duomenų saugumo priemonės, aptariami duomenų tvarkytojo atsakomybės ir kiti klausimai.
37. Pasibaigus darbo santykiams, darbuotojo prieigos teisės prie Centro naudojamų informacinių sistemų nedelsiant panaikinamos. Darbuotojo tiesioginis vadovas privalo pranešti atsakingam darbuotojui apie prieigos teisių panaikinimą ne vėliau kaip paskutinę darbuotojo darbo dieną.
38. Prieigos teisės trečiosioms šalims panaikinamos nutraukus paslaugų sutartį ne vėliau kaip paskutinę paslaugų teikimo dieną.
- 39.** Kiekvienas Centro darbuotojas, užregistruotas Centro naudojamose informacinėse sistemoje, yra priskiriamas darbuotojų grupei, pagal kurią nustatomos, kokios prieigos teisės suteikiamos konkrečiam darbuotojui.

## VII FIZINĖ APSAUGA

### **40. Patalpų apsauga**

- 40.1. Patalpos, kuriose yra kompiuteriai ir saugomi duomenys, turi būti apsaugotos nuo fizinio įsilaužimo, vagysčių, gaisro, potvynio ir kitų rizikų.
- 40.2. Patalpos, kuriose yra kompiuteriai ir saugomi duomenys, turi atitikti keliamus aplinkos reikalavimus.
- 40.3. Visos kompiuterių patalpos turi būti apsaugotos nuo neautorizuoto fizinio įėjimo. Priklausomai nuo patalpų svarbos turi būti naudojamos įvairaus sudėtingumo fizinės apsaugos technologijos.

### **41. Švaraus stalo politika**

- 41.1. Dokumentai ir išorinės duomenų laikmenos turi būti saugomi rakinamose spintose tuo metu, kai nėra naudojami, ypatingai nedarbo valandomis.
- 41.2. Slapta ar konfidenciali verslo informacija turi būti laikoma saugiai (pvz., seifuose arba rakinamose spintose), nepaliekama spausdintuvuose .

## VII BAIGIAMOSIOS NUOSTATOS

42. Šis Aprašas įsigalioja nuo jos patvirtinimo datos.
  43. Už Aprašo laikymosi priežiūrą ir kontrolę, periodinį, ne rečiau kaip kartą per 2 metus, atnaujinimą atsakingas Centro direktoriaus įgaliotas darbuotojas.
  44. Centro darbuotojai pažeidę šiame Apraše numatytų reikalavimų nuostatas - laikomas darbo pareigų pažeidimu.
-