PATVIRTINTA
Palangos miesto globos namų direktoriaus
2024 m. rugsėjo mėn. 20d. įsakymu
Nr.(1.5) ISV-51

INFORMACIJOS SAUGOS IR INFORMACINIŲ TECHNOLOGIJŲ NAUDOJIMO TAISYKLĖS

I BENDROSIOS NUOSTATOS

1. Palangos miesto globos namų Informacijos saugos ir informacinių technologijų naudojimo taisyklės (toliau – Taisyklės) nustato Palangos miesto globos namai (toliau – Įstaiga) informacijos saugos reikalavimus bei priemones, skirtas apsaugoti Įstaigos bei jos veikloje dalyvaujančių ugdytinių bei jų tėvų (globėjų), darbuotojų, taip pat kitų įstaigų ir institucijų informacinius išteklius, apibrėžia informacinių išteklių naudojimo reikalavimus bei taisykles, kurių privalo laikytis visi asmenys, kurie naudojasi Įstaigos informaciniais ištekliais, siekiant užtikrinti veiklos ir informacinių technologijų operacijų patikimą veikimą, saugumą bei veiklos tęstinumą.
2. Šių taisyklių pagrindiniai tikslai yra sudaryti sąlygas saugiai tvarkyti Įstaigos informaciją, numatyti informacinių išteklių naudojimo reikalavimus bei užtikrinti Įstaigos informacijos saugumą nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

3. Taisyklėse informacinės technologijos suprantamos kaip Informacijos sistemų ir paslaugų, duomenų, procesų, kompiuterinės įrangos visuma reikalinga Įstaigos veikloje.

4. Taisyklės ir jose nustatyti reikalavimai privalomi ir taikomi visiems naudotojams, kuriems nustatyta tvarka yra suteikta prieiga prie Įstaigos valdomų ar naudojamų informacinių sistemų ir informacijos: Įstaigos darbuotojams (įskaitant ir laikinus darbuotojus bei praktiką atliekančius asmenis), ugdytiniams ir jų tėvams ar globėjams, kitiems tretiesiems asmenims (rangovams, paslaugų teikėjams, kitų įstaigų darbuotojams), kuriems nustatyta tvarka suteiktos prieigos teisės.

5. Su Taisyklėmis ir (arba) jų pakeitimais turi būti supažindinami visi Įstaigos darbuotojai ir tretieji asmenys, kuriems yra suteikiama prieiga prie Įstaigos informacinių išteklių ir informacijos. Už supažindinimą atsakingas Įstaigos direktoriaus įgaliotas darbuotojas.

6. Prieiga prie informacinių išteklių ir informacijos Įstaigos darbuotojams ar kitiems asmenims gali būti suteikta tik pasirašytinai susipažinus su Taisyklėmis.

II. INFORMACIJOS SAUGOS VALDYMAS

7. Įstaiga savo veikloje jai priskirtų funkcijų vykdymui naudoja informacines sistemas, kurių sąrašas pateiktas Tvarkos 1 priede. Visos 1 priede ir Įstaigos Informacinių išteklių registre išvardintos informacinės sistemos (tiek valdomos Įstaigos, tiek kitų juridinių asmenų) kartu su įstaigos kompiuteriniu tinklu ir kitais techninės bei programinės įrangos komponentais sudaro Įstaigos informacinę infrastruktūrą, šioje taisyklėse nustatyta tvarka ir reikalavimai užtikrina Įstaigos informacinių išteklių valdymą ir jų bei informacijos saugumą. Informacinė infrastruktūra turi būti suvokiama ir naudojama kaip visuma, o ne atskiros sistemos, siekiant užtikrinti visos informacinės infrastruktūros ir informacijos saugą ir tinkamą naudojimą.

8. Šios Taisyklės yra taikomos Įstaigos valdomų ir naudojamų informacinių sistemų bei jose tvarkomos informacijos saugumui užtikrinti, tačiau informacinėms sistemoms, kurių valdytojai yra trečiosios šalys (kitos valstybės institucijos ar įstaigos ar privačios įmonės) ir kuriomis

naudojasi Įstaiga, gali būti nustatyti kiti ar papildomi saugumo reikalavimai konkrečių informacinių sistemų valdytojų patvirtintuose informacijos saugos dokumentuose.

9. Įstaiga yra atsakinga už informacijos saugos taisyklių ir reikalavimų Įstaigoje formavimą ir įgyvendinimą bei atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi.

III. ORGANIZACINIAI IR TECHNINAI INFORMACIJOS SAUGOS REIKALAVIMAI

10. Įrangos saugumas:

10.1. Įstaigoje leidžiama naudoti tik sankcionuotą techninę ir programinę įrangą (toliau – IT įranga).

10.2. Visa Įstaigos IT įranga (techninė ir programinė) turi būti inventorizuota ir suregistruota Įstaigos IT išteklių registre bei priskirti už konkrečią įrangą atsakingi asmenys. Darbuotojas privalo saugoti Įstaigos išduotą ir jam priskirtą IT įrangą.

10.3. Įstaigos IT įrangą darbuotojai gali naudoti darbo metu tik su Įstaiga susijusioms darbinėmis funkcijoms atlikti. Asmeninei komunikacijai Įstaigos įranga gali būti naudojama jei tai netrukdo darbinių funkcijų vykdymui bei nekelia saugumo grėsmių įstaigai ar jos įrangai.

10.4. Įstaigos valdomoje IT įrangoje (darbuotojų kompiuterinėse darbo vietose) turi būti naudojama tik legali, ir darbo funkcijoms vykdyti būtina programinė įranga.

10.5. Apsaugai nuo kenksmingos programinės įrangos (kompiuterinių virusų ir pan.) turi būti naudojama centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo priemonės (antivirusinė programinė įranga).

10.6. Programinę įrangą gali diegti tik Įstaigos IT specialistas ar trečiųjų šalių atstovai pagal sutartį teikiantys Įstaigos informacinių sistemų ir IT įrangos priežiūros ir administravimo paslaugas.

10.7. Programinė įranga turi būti nuolat reguliariai atnaujinama, laikantis gamintojo reikalavimų. Atnaujinimų diegimą bei įrangos priežiūrą atlieka Įstaigos IT specialistas ar trečiųjų šalių atstovai pagal sutartį teikiantys Įstaigos informacinių sistemų ir IT įrangos priežiūros ir administravimo paslaugas.

11. Prieigos teisių valdymas (prieigos suteikimas, keitimas ir panaikinimas):

11.1. Prieiga prie Įstaigos naudojamų informacinių sistemų leidžiama tik tiems naudotojams, kuriems buvo suteiktos prieigos teisės ir prisijungimo prie informacinės sistemos (arba kelių informacinių sistemų, jeigu nenaudojamas vieningas prisijungimas, angl. *Single Sign On, SSO*) naudotojo vardai bei slaptažodžiai .

11.2. Naudotojams prieigos teisės prie informacinių sistemų suteikiamos vadovaujantis principais „būtina darbui" ir „būtina žinoti", t. y. turi būti suteikiamos pagal jo užimamas pareigas minimalios ir tik jo tiesioginėms funkcijoms vykdyti reikalingos prieigos teisės.

11.3. Kiekvienas naudotojas informacinėse sistemose turi būti identifikuojamas unikaliai (asmens kodas negali būti naudojamas kaip naudotojo identifikatorius). Draudžiama naudoti bendras paskyras, nebent jei tai būtina Įstaigos veiklos procesas užtikrinti ir nėra kitų galimybių.

11.4. Prieiga prie informacinėse sistemose saugomos informacijos ir teisė ją keisti suteikiama tik naudotojui tinkamai patvirtinus savo tapatybę.

11.5. Naudotojai gali naudotis tik tomis informacinėmis sistemomis, jų dalimi ar jos komponentais ir juose tvarkoma informacija, prie kurių prieigą jiems buvo suteiktos prieigos teisės.

11.6. Pasikeitus darbuotojo pareigoms turi būti panaikinamos nereikalingos prieigos teisės ir suteikiamos naujos, atitinkančios darbuotojo naujas pareigas. Nutraukus darbo santykius arba pasibaigus sutartiniams santykiams (su trečiosiomis šalimis), visos prieigos teisės turi būti nedelsiant blokuojamos ir panaikinamos.

11.7. Naudotojams neturi būti suteikiamos administratoriaus teisės, suteikiančios privilegijuotus įgaliojimus.

12. Reikalavimai slaptažodžių saugumui:

12.1. Visi naudotojų slaptažodžiai, naudojami prisijungimui prie informacinių sistemų, turi atitikti šiuos minimalius reikalavimus:

Slaptažodžio ilgis	Ne trumpesnis kaip 8 simbolių
Slaptažodžio sudėtingumas	Turi būti naudojamos didžiosios raidės, mažosios raidės ir skaičiai. Draudžiama naudoti slaptažodžiams su asmeniu ar jo artimaisiais susijusią informaciją (vardai, pavardės, gimimo datos ir pan.) ar kitą su naudotoju aiškiai siejamą ir todėl lengvai nuspėjamą informaciją. Neturi būti iš eilės einančių skaitinių ar raidinių ženklų ir kompiuterių klaviatūros sekos, pvz., 12345678, qwerty, 456789, qazwsx ir pan.
Slaptažodžio galiojimas	Slaptažodis turi būti keičiamas ne rečiau kaip kas tris mėnesius arba vos tik kyla įtarimas, kad slaptažodį sužinojo pašaliniai asmenys.
Slaptažodžio pasikartojamumas	Keičiant slaptažodį negalima naudoti prieš tai naudotų 6 slaptažodžių. Nenaudoti to paties slaptažodžio prisijungimui prie skirtingų informacinių sistemų, ypač reikia vengti tų pačių slaptažodžių naudojimo darbinėse ir asmeninėse paskyrose.

12.2. Esant techninėms galimybėms turėtų būti naudojamos kelių faktorių autentifikavimo priemonės (pvz., slaptažodis ir patvirtinimo kodas SMS žinute).

12.3. Naudotojai privalo pasikeisti administratoriaus suteiktą pirminį ar laikiną slaptažodį pirmojo prisijungimo prie informacinės sistemos metu.

12.4. Draudžiama slaptažodžius atskleisti kitiems asmenims, įskaitant ir kitus Įstaigos darbuotojus.

12.5. Slaptažodžius būtina įsiminti, draudžiama saugoti slaptažodžius užrašytus popieriuje, skaitmeninėse laikmenose arba įrenginiuose (pvz. išmaniuosiuose telefonuose) .

13. Elektroninio pašto naudojimas.

13.1. Įstaigos suteiktas elektroninis paštas ir kitos bendradarbiavimo priemonės, įskaitant momentinių pranešimų sistemas, turi būti naudojami tinkamai. Naudotojai turi žinoti, kas yra priimtina ir nepriimtina naudojant savo elektroninį paštą ir kitas bendradarbiavimo sistemas.

13.2. Įstaigos elektroninio pašto ir bendradarbiavimo priemonių paskyros turi būti naudojamos tik Įstaigos numatytos veiklos tikslams pasiekti – darbinis elektroninis paštas turi būti naudojamas darbo reikmėms – visa darbinė informacija turi būti siunčiama tik naudojantis Įstaigos darbiniu elektroniniu paštu.

13.3. Elektroninio pašto informacijai saugoti darbuotojui skiriama nustatyto dydžio elektroninio pašto paskyra. Viršijus skirtą dydį, sistema apie tai informuoja naudotoją. Elektroninio pašto korespondencija yra Įstaigos veiklos įrašas – jis turi būti saugomas pagal bendrąją informacijos saugojimo tvarką. Darbuotojas savo naudojamoje įrangoje gali saugoti elektroninio pašto archyvus ne ilgiau kaip 1 metus, išskyrus atvejus, kai tiesioginis vadovas leidžia naudotis didesniais archyvais.

13.4. Elektroninio pašto naudotojai privalo laikytis saugaus elektroninio pašto naudojimosi reikalavimų bei užtikrinti siunčiamos informacijos konfidencialumą. Už elektroniniu paštu siunčiamos informacijos turinį ir saugumą atsako siuntėjas.

13.5. Naudotojams draudžiama naudoti darbiniams tikslams Įstaigos nepatvirtintas trečiųjų šalių viešąsias elektroninio pašto sistemas ir saugojimo serverius (pvz., asmeniškai naudojamas paskyras „Google Gmail", „Outlook.com", „Mail.ru", „Yahoo", „Hotmail" ir kt.) darbinei informacijai siųsti. Draudžiama peradresuoti Įstaigos darbinio elektroninio pašto korespondenciją į asmenines trečiųjų šalių viešąsias elektroninio pašto sistemas.

13.6. Elektroninį paštą mobiliuose įrenginiuose (išmaniuosiuose telefonuose, planšetėse) leidžiama naudoti tik naudojant įrenginio užrakinimą apsaugotą kodu, slaptažodžiu, biometrinės apsaugos priemonėmis (piršto antspaudas ir /ar veido atpažinimas).

13.7. Įstaigos konfidenciali informacija, įskaitant informaciją, kurioje yra asmens duomenys gali būti siunčiama elektroniniu paštu tik jei tokia informacija yra apsaugota naudojant šifravimą. Šifravimo raktai ar kodai informacijos gavėjui turi būti perduodami naudojant kitus perdavimo būdus ar kanalus – draudžiama šifravimo raktus ar kodus siųsti elektroniniu paštu.

13.8. Naudotojai, pastebėję elektroninio pašto sistemos sutrikimus privalo nedelsiant informuoti Įstaigos IT specialistą arba pranešti apie sutrikimą trečiųjų šalių atstovams pagal sutartį teikiantiems Įstaigos informacinių sistemų ir IT įrangos priežiūros ir administravimo paslaugas.

13.9. Elektroninio pašto naudotojai privalo laikytis saugaus elektroninio pašto naudojimosi reikalavimų:

13.9.1. Saugotis informacijos išviliojimo (angl. „phishing") ir socialinės inžinerijos bandymų: neatidaryti laiškų gautų iš nežinomų siuntėjų, įvertinti ar laiškas siųstas tikrai to siuntėjo (el. pašto adreso ir siuntėjo nesutapimai, keista, nelogiška pranešimo tema, neįprastas ar nežinomas siuntėjo elektroninio pašto adresas)

13.9.2. neatidaryti elektroninio pašto pranešimų, jei įtaria, kad gautas elektroninio pašto pranešimas yra užkrėstas kenkėjiška programinė įranga (pridėta neįprasta byla ar nuoroda į išorinės svetainės adresą) arba jei siuntėjas žinomas, bet abejojama dėl atsiųsto pranešimo turinio, naudojamos kalbos ar pridėtos bylos.

13.9.3. prieš siunčiant elektroninio pašto pranešimus, atidžiai patikrinti adresatų sąrašą ir įsitikinti, kad visi adresatai turi teisę susipažinti su siunčiama informacija;

13.9.4. užpildyti siunčiamo elektroninio pašto pranešimo rekvizitus (antraštę, laiško turinį, siuntėjo duomenis);

13.9.5. nuolat sekti aktualią elektroninio pašto informaciją, ištrinti pasenusius, neaktualius pranešimus;

13.9.6. nedelsiant informuoti atsakingus asmenis, jei kyla įtarimų dėl galimo neteisėto prisijungimo prie priskirto darbinio elektroninio pašto adreso, jo turinio valdymo ar kitus saugumo incidentus (pvz., praradus ar atskleidus prisijungimo duomenis).

13.10. Elektroninio pašto naudotojams draudžiama:

13.10.1. savavališkai keisti elektroninio pašto programinės įrangos parametrus, susijusius su sauga arba prisijungimo būdu, ir kitus įdiegtus saugumo mechanizmus;

13.10.2. naudojantis elektroninio paštu siųsti konfidencialią Įstaigos informaciją, įskaitant asmens duomenis, jei nenaudojamos papildomos informacijos saugos priemonės (pvz., siunčiamos informacijos šifravimas);

13.10.3. skelbti darbinio elektroninio pašto adresą viešojoje erdvėje, jeigu tai nėra susiję su darbo funkcijų vykdymu;

13.10.4. naudojantis elektroninio pašto paslauga siųsti pranešimus savo arba Įstaigos vardu, kurie gali pakenkti Įstaigos įvaizdžiui ir reputacijai sukelti materialinę žalą Įstaigai;

13.10.5. naudotis elektroniniu paštu sukčiavimo, reklamos ir asmeninės finansinės naudos tikslais;

13.10.6. kurti, saugoti ar platinti laiškus su smurtinio, diskriminacinio, rasistinio, seksualinio, pornografinio ar kitaip žmogaus garbę ir orumą žeminančio turinio informacija;

13.10.7. perduoti kitiems asmenims, įskaitant ir Įstaigos darbuotojus, savo ar kitų elektroninio pašto prisijungimo vardus ir slaptažodžius ir naudotis svetimais elektroninio pašto adresais ir slaptažodžiais.

13.11. Visos elektroninio pašto laiškams taikomos nuostatos vienodai galioja visoms bendradarbiavimo ir ryšių sistemoms, nepriklausomai nuo jų naudojimo būdo: kompiuteriams, išmaniesiems telefonams ar kitiems įrenginiams.

13.12. Asmeninis bendravimas darbuotojams darbo vietoje yra leidžiamas, tačiau jis turi būti vykdomas naudojant kitas priemones (elektroninio pašto paskyras, „Messenger", „Viber", „WhatsUp" ir kt. ar kitas paskyras), kurios neturi būti susijusios su darbiniu elektroninio pašto adresu.

13.13. Asmeninis bendravimas socialinių paslaugų gavėjams Įstaigoje leidžiamas tokias būdais, kaip numato Įstaigos vidaus taisyklės. Naudojant asmeninio bendravimo priemones negali būti pažeidžiamas Įstaigos informacinės infrastruktūros saugumas.

14. Nuotolinio mokymo sistemų naudojimas

14.1. Naudoti tik Įstaigos aprobuotas ir pripažintas tinkamomis nuotolinio mokymo platformas.

14.2. Siekti, jog šiose platformose prieinamas turinys (vaizdo ir garso įrašai, prezentacijos, tekstai ir kitas turinys) būtų prieinamas tik tiems mokiniams ar ugdytiniams, kuriems tai priklauso pagal numatytą tvarką.

14.3. Draudžiama naudoti nuotolinio mokymo platformų įrašus be jose dalyvaujančių asmenų sutikimo (tokio tipo turinys yra asmens duomenys).

14.4. Bet kokių video įrašų darymas, tiek įrašant lektorių veiksmus, tiek ir darbuotojų veiksmus yra laikomas asmens duomenų rinkimu ir tvarkomas kaip asmens duomenys. Šia informaciją draudžiama platinti be oje esančio asmens sutikimo.

15. Interneto naudojimo reikalavimai

15.1. Naudodami Įstaigos interneto resursus darbuotojai privalo laikytis etikos normų, autorių ir gretutinių teisių, šių ir kitų vidaus tvarką reglamentuojančių taisyklių.

15.2. Darbuotojai, registruodamiesi internetiniuose puslapiuose (pvz., socialiniuose tinkluose) atstovauja Įstaigai, todėl turi elgtis taip, kad nepakenktų Įstaigos reputacijai.

15.3. Įstaiga vertina su informacijos sauga susijusias interneto naudojimo rizikas ir, esant pagrįstumui, gali blokuoti rizikingo turinio kategorijas, tinklalapius arba su darbu nesusijusių programų komunikaciją internete.

15.4. Darbuotojui naudojantis Įstaigos interneto resursais draudžiama:

15.4.1. bet koks eksperimentavimas, susijęs su programinės įrangos atsparumu virusams ar patikrinimas dėl jos saugumo;

15.4.2. naudotis internetu reklamos ir asmeninės finansinės naudos tikslais;

15.4.3. siųstis iš interneto, taip pat platinti, su darbo funkcijomis nesusijusias grafines, garso bei vaizdo bylas;

15.4.4. talpinti interneto komentarus, pasiūlymus bei kitus duomenis, susijusius su diskriminuojančiu, nepadoriu, įžeidžiančiu, kurstančiu neapykantą ar kitu nepageidaujamu turiniu;

15.4.5. lankytis svetainėse, kuriose pateikiama pornografinė, smurtinė, terorizmą bei kitokią nusikalstamą veiklą skatinanti informacija ar kurios susijusios diskriminuojančiu, nepadoriu, įžeidžiančiu, skatinančiu neapykantą ar kitu nepageidaujamu turiniu, taip pat platinti tokią informaciją;

15.4.6. dalyvauti interneto lažybose ir azartiniuose lošimuose;

15.4.7. savavališkai keisti interneto naršyklės ir elektroninio pašto programinės įrangos parametrus, susijusius su apsauga arba prisijungimo būdu, apeiti bet kurį taikomą saugumo mechanizmą;

15.4.8. perduodant duomenis arba kitą informaciją internetu, draudžiama naudotis svetimais arba neegzistuojančiais elektroninio pašto adresais, t.y. mėginti apsimesti kitu vartotoju;

15.4.9. imtis veiksmų ar kitaip trikdyti interneto resursų greitaveiką Įstaigoje, bandyti išvengti Įstaigos teisėtai vykdomo stebėjimo ar kontrolės.

16. Nuotolinė prieiga prie Įstaigos informacinių sistemų:

16.1. Nuotolinė prieiga prie Įstaigos informacinių sistemų gali būti suteikiamas tik tais atvejais, jei tai būtina darbuotojo tiesioginių funkcijų atlikimui. Darbuotojas, jungdamasis prie Įstaigos informacinių sistemų, turi užtikrinti ir pasirūpinti prisijungimo vietos (pvz. namų interneto tinklo) saugumu, nesijungti iš nepatikimų vietų (pvz. nežinomo viešiosios interneto prieigos taško).

16.2. Virtualusis privatus tinklas (angl. *Virtual Private Network*, VPN) yra saugumą didinanti technologija, kuri gali būti taikoma kai dirbama ne Įstaigos vidiniame tinkle (t.y. ne įprastinėse darbo vietose). Nuotolinė prieiga galima tik naudojantis saugius šifruotus ryšio kanalus (SSL VPN tuneliu) arba naudojant sertifikatą.

16.3. Savavališka nuotolinė prieiga prie Įstaigos informacinių sistemų yra griežtai draudžiama.

16.4. VPN naudotojai atsako už tai, kad tretieji asmenys VPN naudojimo metu neprieitų prie Įstaigos vidinio tinklo, informacinių sistemų ir informacijos.

17. Nešiojamųjų įrenginių ir išorinių duomenų laikmenų saugumas:

17.1. Įstaigos nešiojamuose įrenginiuose (nešiojamuosiuose kompiuteriuose, planšetėse, išmaniuosiuose telefonuose ir pan.), jeigu jie naudojami ne Įstaigos vidiniame kompiuterių tinkle, įrenginiuose esanti Įstaigai svarbi informacija (pvz., konfidenciali informacija, asmens duomenys) ir prisijungimo prie Įstaigos informacinėse sistemose tvarkomos informacijos ir duomenų turi būti šifruojama, privaloma naudoti papildomas saugos priemones, kuriomis patvirtinama naudotojo tapatybė (slaptažodis, PIN kodas ir pan.).

17.2. Visuose Įstaigos nešiojamuosiuose kompiuteriuose turi būti įjungta „Bitlocker" ar panaši standžiojo ar atminties disko šifravimo technologija, kad užtikrinanti informacijos, saugomos įrenginyje apsaugą Įstaigos informacija būtų apsaugota kompiuterinės įrangos vagystės ar praradimo atveju.

17.3. Apie bet kokio įrenginio praradimą (pavogtas ar kitaip pamestas) darbuotojas privalo informuoti Įstaigos vadovą, o vagystės atveju – ir Policiją.

17.4. Asmeninius nešiojamus įrenginius prijungti prie Įstaigos tinklo (pvz., prie Įstaigos bevielio tinklo) galima tik jei įrenginys atitinka nustatytus saugumo reikalavimus (įdiegti visi rekomenduojami programinės įrangos atnaujinimai, naudojama kenksmingos programinės įrangos kontrolės priemonės, informacijos šifravimas ir kt.).

17.5. Draudžiama asmeniniuose (tai netaikoma Įstaigos kompiuterinei įrangai) nešiojamuose įrenginiuose saugoti Įstaigos informaciją. Ši nuostata netaikoma asmeniniams išmaniesiems telefonams, jei yra užtikrintas tinkamas jų saugumas ir užrakinimas.

17.6. Jei darbuotojui suteikta teisė išnešti nešiojamąjį įrenginį iš Įstaigos teritorijos, jis atsakingas už išnešamo įrenginio ir jame esančios informacijos saugumą.

17.7. Įstaigoje leidžiama naudoti tik Įstaigos išduotas išorines duomenų laikmenas (USB raktus, išorinius kietuosius diskus). Išorinėse duomenų laikmenose įstaigos informacija privalo būti saugoma šifruota.

18. Informacijos saugos incidentai:

18.1. Naudotojai, pastebėję Įstaigos informacinių sistemų sutrikimus, esamus arba įtariamus kibernetinius incidentus, nustatytų informacijos saugos reikalavimų pažeidimus, neveikiančias arba netinkamai veikiančias saugos priemones, kitų naudotojų ar asmenų neteisėtus veiksmus

ar nusikalstamos veikos požymius turinčius atvejus ar kitus įtartinus atvejus privalo nedelsiant pranešti Įstaigos IT specialistui ar kitam atsakingam asmeniui..

18.2. Informacijos saugos incidentai turi būti registruojami ir valdomi bei šalinami Įstaigos turimomis techninėmis ir programinėmis priemonėmis.

18.3. Naudotojai privalo vykdyti įstaigos IT specialisto ar kito atsakingo asmens nurodymus, susijusius su incidento valdymu ir likvidavimu (pateikti visą žinomą informaciją, pateikti su incidentu susijusią IT įrangą ir pan.).

18.4. Pašalinus incidentą turi būti atliekama analizė ir vertinimas siekiant nustatyti incidento priežastis bei imtis reikiamų priemonių panašių incidentų ateityje.

19. IT įrangos ir informacijos naikinimas:

19.1. Perduodant techninę įrangą išoriniams rangovams remontuoti ar nurašant netinkamą naudoti įrangą turi būti užtikrinama, kad perduodamoje ar nurašomoje įrangoje nėra Įstaigos konfidencialios informacijos. Informacija turi būti ištrinama naudojant specializuotą programinę įrangą, kad nebūtų galimybės atkurti informacijos, išimami vidiniai diskai arba jie fiziškai sunaikinami. Jei naudotojas pats negali užtikrinti šių reikalavimų vykdymo, privaloma kreiptis į įstaigos įgaliotą IT specialistą.

19.2. Nereikalingos ar nenaudojamos išorinės duomenų laikmenos, kuriose yra Įstaigos informacija, turi būti naikinamos ištrinant informaciją neatkuriamai naudojant specializuotą programinę įrangą (USB raktai, išoriniai kietieji diskai) arba fiziškai sunaikinant laikmenas jas sulaužant (CD / DVD diskai, USB raktai, išoriniai kietieji diskai) Popieriniai dokumentai, kuriuose yra Įstaigai svarbios informacijos, turi būti naikinami juos susmulkinant.

19.3. Įrangos ir laikmenų sunaikinimas turi būti registruojamas.

20. Naudotojų teisės ir pareigos:

20.1. Naudodamiesi Įstaigos informacinėmis sistemomis ar joje tvarkoma informacija naudotojai turi:

20.1.1. susipažinti su Įstaigos patvirtintais informacijos saugą reglamentuojančiais dokumentais ir laikytis juose nustatytų saugos reikalavimų;

20.1.2. naudoti Įstaigos IT įrangą darbo funkcijų vykdymui ir laikantis nustatytų saugos reikalavimų;

20.1.3. užtikrinti elektroninės informacijos konfidencialumą ir vientisumą;

20.1.4. laikytis „švaraus stalo ir švaraus ekrano" politikos – kiekvieną kartą nors ir trumpam palikdami savo darbo vietą, užtikrinti, kad pašaliniai asmenys negalėtų susipažinti su informacija – atsijungti nuo informacinės sistemos, įjungti slaptažodžiu apsaugotą ekrano užsklandą, o baigę darbą – atsijungti nuo informacinės sistemos ir išjungti Įrangą;

20.1.5. nedelsdami pranešti apie pastebėtus Įstaigos informacinių sistemų ar jų posistemių veikimo sutrikimus, esamus arba įtariamus kibernetinius incidentus, dokumentuose nustatytų reikalavimų pažeidimus, neveikiančias arba netinkamai veikiančias saugos priemones, kitų naudotojų ar asmenų neteisėtus veiksmus ar nusikalstamos veikos požymius turinčius atvejus ar kitus įtartinus atvejus Įstaigos IT specialistui ar kitam atsakingam asmeniui;

20.1.6. atliekant darbo funkcijas susipažinus su asmens duomenimis, neatkleisti (neviešinti) asmens duomenų, jei asmens duomenys neskirti skelbti viešai. Ši pareiga galioja ir pasibaigus darbo santykiams Įstaigoje;

20.1.7. vykdyti Įstaigos IT specialisto ir (arba) administratoriaus ar kito už saugą atsakingo asmens nurodymus dėl IT įrangos naudojimo ir nurodymus bei pavedimus, susijusius su saugos reikalavimų įgyvendinimu.

20.2. Naudotojams draudžiama:

20.2.1. savavališkai ar savarankiškai keisti jiems paskirtos Įrangos konfigūraciją, šalinti Įrangos gedimus;

20.2.2. savavališkai naudoti ir organizuoti nenustatytus kompiuterių ryšius iš darbo vietos su internetu ar kitais išorės tinklais;

20.2.3. naudoti kompiuterinę įrangą, informacines sistemas ir jos duomenų bazes, interneto ir elektroninio pašto teikiamas galimybes kitiems tikslams, nesusijusiems su darbinių funkcijų atlikimu;

20.2.4. priskirtoje Įrangoje naudoti ir platinti Įstaigos kompiuterių tinkluose ar kitais būdais nelicencijuotas kompiuterių programas;

20.2.5. platinti, atskleisti kitiems asmenims darbui su Įranga jiems suteiktus prieigos vardus, slaptažodžius, kodus, įrangos konfigūracijos ar kitus duomenis;

20.2.6. turėti ir naudoti programas, skaitančias, peržiūrinčias ir analizuojančias lokalius kompiuterių tinklus ir jais perduodamą informaciją;

20.2.7. keisti, atnaujinti, įdiegti ar šalinti programinę įrangą naudotojui priskirtoje IT įrangoje (ši nuostata netaikoma automatiniam programinės įrangos atnaujinimui);

20.2.8. leisti naudoti jam priskirtą Įrangą pašaliniams asmenims;

20.2.9. išnešti Įrangą iš Įstaigos teritorijos prieš tai nesuderinus su savo tiesioginiu vadovu ir atsakingu už Įrangą asmeniu. Šis draudimas netaikomas kompiuterinės įrangos remonto ir priežiūros funkcijas atliekantiems Įstaigos darbuotojams, bei šias funkcijas atliekančių paslaugų teikėjų įgaliotiems asmenims, su kuriais sudarytos kompiuterinės įrangos remonto ir priežiūros sutartys.

III. BAIGIAMOSIOS NUOSTATOS

21. Už šių Taisyklių įgyvendinimą ir vykdymo kontrolę Įstaigos direktoriaus įsakymu skiriamas direktoriaus pavaduotojas Algirdas Šiaulys, tel. +370 603 23643, el.p. administracija@palangosgnamai.lt

22. Šios Taisyklės turi būti peržiūrimos reguliariai ne rečiau kaip kartą per metus arba įvykus svarbiems esminiams organizaciniams, sisteminiams ar kitokiems pokyčiams Įstaigoje arba įvykus svarbiam informacijos saugos incidentui.

23. Naudotojai, pažeidę šių Taisyklių reikalavimus ar kitus informacijos saugos reikalavimus atsako teisės aktų nustatyta tvarka.

Pasirašau, patvirtindamas, kad esu susipažinęs su:

- Įstaigos Informacijos saugos ir informacinių technologijų naudojimo taisyklėmis,
- Taisyklių nesilaikymo pasekmėmis,
- kontaktais ir atsakingais asmenimis kilus klausimams ar problemoms.

Vardas ir pavardė	Parašas	Data, vieta

1 priedas

PALANGOS MIESTO GLOBOS NAMŲ VALDOMŲ IR (ARBA) NAUDOJAMŲ INFORMACINIŲ SISTEMŲ SĄRAŠAS

Informacijos sistemos pavadinimas, adresas internete	**Informacinės sistemos paskirtis ir techninė platforma**	**Sistemos valdytojas**	**Sistemos techninę priežiūrą užtikrina**
Elektroninis paštas	Darbuotojų el. pašto sistema Serveriai. lt platformoje	Įstaiga	Priežiūra vykdoma MB „Saugma.Lt" Tel: 8 649 0333
Įstaigos interneto svetainė www.palangosgnamai.lt	Įstaigos oficialus tinklapis laikomas Serveriai.lt platformoje	Įstaiga	MB „Saugma.Lt" Tel: 8 649 0333
Įstaigos socialinių tinklų paskyros	Facebook, Tik Tok, Instagram paskyros	Įstaiga	Socialinė darbuotoja Viktorija Rišytė
Lietuvos Respublikos sveikatos apsaugos ministerija (Elektroninė sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema (toliau – ESPBI IS)	Numatyta LR SAM norminiuose aktuose ir tvarkose	LR Sveikatos apsaugos ministerija	VĮ „Registrų Centras" ar kita LR SAM įgaliota įmonė
CVPIS https://pirkimai.eviesiejipirkimai.lt/	Numatyta Centrinės Viešųjų pirkimų valdymo agentūros, naudojama Įstaigos viešiesiems pirkimams	Centrinė Viešųjų pirkimų agentūra	CPVA
Viešųjų pirkimų sistema VIPIS	Numatyta savivaldybės naudojama įstaigos viešiesiems pirkimams	Savivaldybė	UAB ,,Nevda"
Dokumentų valdymo sistema (KONTORA)	Numatyta savivaldybės	Savivaldybė	Uab ,,Nevda"

	dokumentų valdymo sistema įstaigoje		
Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinė sistema (VSAKIS)	Numatyta LR finansų ministerijos	LR Finansų ministerija	LR Finansų ministerija
Biudžetinių įstaigų buhalterinė apskaita (FinNet)	Įstaigos finansinės apskaitos vykdymas	Savivaldybė	Palangos miesto savivaldybė
Įstaigos buhalterinė apskaita (FINAS)	Įstaigos finansinės apskaitos vykdymas	Įstaiga	UAB ,,Eksitonas"
Įstaigos buhalterinė apskaita (FINALGA)	Įstaigos darbo užmokesčio skaičiavimas	Įstaiga	UAB ,,Eksitonas"
Interneto prieiga (LITNET)	Įstaigos interneto prieigos teikimas (darbuotojų įranga) bei viešieji interneto priegos taškai (WiFi)	LITNET	LITNET