Asmens duomenų tvarkymo
Šiaulių miesto savivaldybės administracijoje taisyklių
1 priedas

ŠIAULIŲ MIESTO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACIJOS SAUGUMO POLITIKA

1. Šiaulių miesto savivaldybės administracijos (toliau – Administracija) informacijos saugumo politika reglamentuoja technines ir organizacines asmens duomenų saugumo priemones, kurios taikomos Administracijos tvarkomų asmens duomenų atžvilgiu.
2. Administracijos informacijos saugumo politika taikoma Administracijos darbuotojams, Administracijos pasitelktiems paslaugų teikėjams, teikiantiems su asmens duomenų tvarkymu ir (ar) duomenų saugumo užtikrinimu susijusias paslaugas.
3. Administracijos darbuotojai privalo laikytis Taisyklių nuostatų ir prisidėti įgyvendinant Administracijoje įdiegtas organizacines ir technines priemones, skirtas apsaugoti asmens duomenis nuo atsitiktinio ar neteisėto naikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo. Administracijos darbuotojai turi užkirsti kelią atsitiktiniam ar neteisėtam asmens duomenų sunaikinimui, pakeitimui, atskleidimui, taip pat bet kokiam kitam neteisėtam tvarkymui, saugodami dokumentus Administracijos teisės aktų nustatyta tvarka.
3. Administracijos informacijos saugumo politika peržiūrima ir prireikus atnaujinama ne rečiau kaip kartą per metus.
4. Administracija tvarkydama asmens duomenis taiko šias techninės ir organizacinės asmens duomenų saugumo priemones:

Nr.	Techninės ir organizacinės saugumo priemonės
1.	**Prieigų ir paskyrų valdymas**
1.1.	Administratoriaus funkcijos atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms naudotojo funkcijoms atlikti.
1.2.	Naudotojams nesuteikiamos administratoriaus teisės
1.3.	Naudotojas unikaliai atpažįstamas
1.4.	Naudotojui panaikinta prieiga prie informacinių išteklių nedelsiant, jei prieiga tampa neaktuali, nutraukiami darbo santykiai ar darbuotojas nušalinamas nuo pareigų.
1.5.	Baigus darbą ar naudotojui pasitraukiant iš darbo vietos, naudotojas imamasi priemonių, kad su informacija, kuri tvarkoma informaciniuose ištekliuose, negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinių išteklių, įjungiama ekrano užsklanda su slaptažodžiu.
1.6.	Reguliariai vykdoma prieigų kontrolė
1.7.	Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, yra priskiriamos konkrečios prieigos kontrolės teisės, vadovaujantis „*būtina žinoti*“ (*angl. need to know*) principu
1.8.	Naudotojų paskyros yra asmeninės. Naudotojų identifikatoriai (prisijungimo vardai) yra unikalūs ir asmeniniai. Bendrų paskyrų naudojimas yra draudžiamas, išskyrus

	informacinių sistemų integracijos be informacinių technologijų infrastuktūros priežiūros tikslais
1.9.	Administracijoje įgyvendinta prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema leidžia kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras
2.	**Slaptažodžių politika**
2.1.	Nustatomas leistinų nepavykusių prisijungimų prie programinės įrangos skaičius, kurį pasiekus naudotojo paskyra blokuojama bent 15 minučių.
2.2.	Kur techniškai įmanoma, slaptažodžiai sudaromi iš kompleksinių simbolių.
2.3.	Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, turėti galiojimo terminą ir privalo būti pakeistas pirmo prisijungimo metu. Slaptažodžiai negali būti saugomi viešai ir negali būti prieinami kaip visuma.
2.4.	Slaptažodžiai turi būti keičiami vadovaujantis naudojamos informacinės sistemos saugos nuostatais, taip pat susidarius tam tikroms aplinkybėms (pasikeitus darbuotojui, iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims ir pan.) – dažniau. Įpratai naudotojų slaptažodis keičiamas ne rečiau kaip kas 60 kalendorinių dienų.
2.5.	Naudotojo slaptažodį sudaro ne mažiau kaip 8 simboliai, iš kurių bent keli turi būti skaičius ir raidė. Slaptažodis negali sutapti su darbuotojų ar jų šeimos narių asmeniniais duomenimis.
2.6.	Administratoriaus slaptažodis keičiamas ne rečiau kaip kas 60 kalendorinių dienų
2.7.	Administratorių slaptažodį sudaro ne mažiau kaip 12 simbolių.
2.8.	Draudžiama informacinių išteklių techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie pakeičiami į atitinkančius reikalavimus.
2.9.	Slaptažodžiai duomenų bazėje saugomas užšifruotai
3.	**Informacinių išteklių infrastruktūra**
3.1.	Priemonės, naudojamos informacinių išteklių sąsajoje su viešųjų elektroninių ryšių tinklu, nustatytos taip, kad fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais
3.2.	Pagrindinėse tarnybinėse stotyse įjungtos saugasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su informacinių išteklių funkcionalumu ir administravimu susijusį, duomenų srautą.
3.3.	Tarnybinėse stotyse naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės
3.4.	Kenksmingosios programinės įrangos aptikimo priemonė automatiškai informuoja administratorių apie tai, kuriems informacinių išteklių posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas ar buvo aptiktas kenksmingas kodas

3.5.	Operatyviai ištestuojami ir įdiegiami informacinės sistemos tarnybinių stočių operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai
3.6.	Tarnybinėse stotyse naudojama tik legali programinė įranga;
3.7.	Techninė ir programinė įranga prižiūrima laikantis gamintojo rekomendacijų;
3.8.	Techninės ir programinės įrangos priežiūrą ir gedimų šalinimą atlieka paslaugų teikėjai ir Informacinių technologijų skyriaus atsakingi specialistai.
3.9.	Tarnybinėje stotyje naudojama tik informacinio ištekliaus veiklai reikalinga programinė įranga
3.10.	Šifruojamos tarnybinių stočių atminties laikmenos
3.11.	Nenaudojamos atminties laikmenos sunaikinamos ar pažeidžiamos taip, kad nebūtų galima atstatyti jose esančios informacijos
3.12.	Techninėje ir programinėje įrangoje nenaudojama (blokuota) gamintojo prieiga
3.13.	Reguliariai daromos atsarginės kopijos
3.14.	Uždrausta naršyti svetainės aplankuose (angl. Directory browsing)
3.15.	Informacinių sistemų portalai apsaugoti ne mažesniu kaip 128 bitų raktu.
3.16.	Informacinių sistemų portaluose naudojamas TLS (angl. Transport Layer Security) standartas
3.17.	Informacinės sistemos programiniame kode nėra saugomi prisijungimų duomenys
3.18.	Informacinės sistemos apsaugotos nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. SQL injection), įterptinių instrukcijų atakų (angl. Cross-site scripting), atkirtimo nuo paslaugos (angl. DOS), paskirstyto atsisakymo aptarnauti (angl. DDOS) ir kitų.
3.19.	Tarnybinė stotis, kurioje yra svetainė, nerodo svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį
4.	**Kompiuterinės darbo vietos**
4.1.	Kompiuteriuose naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės.
4.2.	Kenksmingosios programinės įrangos aptikimo priemonė automatiškai informuoja administratorių apie tai, kuriems informacinių išteklių posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas ar buvo aptiktas kenksmingas kodas.
4.3.	Operatyviai ištestuojami kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai.
4.4.	Kompiuteriuose aktyvuotos lokalios saugasienės ir sukonfigūruotos taip, kad blokuotų visą nereikalingą srautą

4.5.	Kompiuterinė įranga ir duomenų perdavimo tinklas prižiūrimi pagal gamintojo rekomendacijas
4.6.	Kompiuterinės įrangos priežiūrą ir gedimų šalinimą atlieka paslaugų teikėjai ir Administracijos bendrųjų reikalų skyriaus Informacinių technologijų poskyriaus atsakingi specialistai.
4.7.	Vartotojams negali deaktyvuoti ar apeiti saugumo nustatymų
4.8.	Kompiuterinėje įrangoje naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga.
4.9.	Panaikintos ar pervadintos standartinės gamintojo paskyros
4.10.	Nenaudojamos atminties laikmenos sunaikinamos ar pažeidžiamos taip, kad nebūtų galima atstatyti jose esančios informacijos
4.11.	Kompiuteriuose nustatyta, kad prisijungus prie vidinio tinklo išjungiama belaidė periferinė prieiga
4.12.	Kompiuterių naudotojai negali savavališkai diegtis programinės įrangos
5.	**Tinklas**
5.1.	Vidinis tinklas segmentuotas, atskirtos bevielio tinklo zona, kompiuterių zona, tarnybinių stočių zona.
5.2.	Reguliariai atnaujinama programinė aparatinė įranga
5.3.	Informacinių išteklių elektroninės informacijos perdavimo tinklas atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę; ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos.
5.4.	Tinklo perimetro apsaugai naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo.
5.5.	Belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, kontroliuojamoje zonoje
5.6.	Jei techniškai įmanoma, uždrausta belaidėje sąsajoje naudoti SNMP (angl. Simple Network Management Protocol) protokolą valdymui
5.7.	Jei techniškai įmanoma, uždrausta visi nebūtini valdymo protokolai
5.8.	Jei techniškai įmanoma, išjungti nenaudojami TCP (angl. Transmission Control Protocol) / UDP (angl. User Datagram Protocol) prievadai
5.9.	Jei techniškai įmanoma, uždraustas lygiarangis (angl. peer to peer) funkcionalumas, neleidžiantis belaidžiais įrenginiais tarpusavyje palaikyti ryšį
5.10.	Belaidis ryšys šifruojamas mažiausiai 128 bitų ilgio raktu.
5.11.	Prieš pradedant šifruoti belaidį ryšį, pakeisti belaidės prieigos stotelėje standartiniai gamintojo raktai.
6.	**Atsarginės kopijos**

6.1.	Atsarginės kopijos saugomos kitose patalpose nei yra pagrindinė įranga
6.2.	Reguliariai atliekami bandymai atstatyti duomenis iš atsarginių kopijų
6.3.	Užtikrinamas duomenų atkūrimas iš naujausių turimų atsarginių duomenų kopijų, praradus duomenis dėl aparatinės kompiuterių įrangos gedimo, programinės įrangos klaidos ar kitaip pažeidus duomenų vientisumą
6.4.	Atsarginės asmens duomenų kopijos daromos, saugomos kitoje patalpoje ar geografinėje vietoje negu aktyvi (veikianti) duomenų bazė
6.5.	Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą
6.6.	Atsarginių duomenų kopijų laikmenos, saugomos atsarginių kopijų saugykloje atskirai nuo pagrindinės buveinės
7.	**Duomenų perdavimas**
7.1.	Užtikrinamas saugių protokolų ir (arba) slaptažodžių naudojimas, kai asmens duomenys perduodami išoriniais duomenų perdavimo tinklais.
7.2.	El. paštu perduodami asmens duomenys šifruojami
7.3.	Duomenis perduodant išorine laikmena, užšifruojama laikmena arba perduodami duomenys
7.4.	Asmens duomenys perduodant popierinėje formoje, užtikrinama, jog ji yra perduodama tiesiogiai klientui, naudojantis patvirtintomis informacijos perdavimo paslaugomis: asmeniškai; registruotu laišku; per kurjerius
8.	**Duomenų tvarkymas**
8.1.	Realizuotas asmens duomenų ištrynimas, perkėlimas kai asmens duomenys tvarkomi duomenų subjekto sutikimu.
8.2.	Perdavus duomenis išorine laikmena, jie yra ištrinami, taip kad nepavyktų atkurti.
9.	**Organizaciniai reikalavimai**
9.1.	Registruojami visi incidentai, susiję su asmens duomenų pažeidimais, kibernetiniai incidentai
9.2.	Esant poreikiui vykdomi darbuotojų mokymai asmens duomenų tvarkymo, informacijos saugumo temomis
9.3.	Atliekamas rizikos vertinimas
9.4.	Atliekamas infrastruktūros ir informacinių sistemų pažeidžiamumų vertinimas internetu pasiekiamos informacinėms sistemoms
9.5.	Vykdomas informacinių sistemų, infrastruktūros pokyčių valdymas, vertinant ar pokytis neturėjo įtakos asmens duomenų tvarkymui ar duomenų saugumui
9.6.	Vykdomas įsilaužimų testavimas internetu pasiekiamos informacinėms sistemoms

9.7.	Informacinių sistemų testavimas neatliekamas su realiais asmens duomenimis
9.8.	Pildomas IT išteklių, naudojamų asmens duomenims tvarkyti registras (techninės, programinės ir tinklo įrangos). Registras apima šią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinė darbo vietą), vietą (fizinę ar elektroninę). IT ištekliai reguliariai peržiūrimi ir atnaujinami. Peržiūros dažnumas: kartą per metus.
9.9.	Administracija užtikrina, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo kontrolę, susijusią su jų kasdieniu darbu. Administracijos darbuotojai, susiję su asmens duomenų tvarkymu, apmokomi dėl atitinkamų duomenų apsaugos reikalavimų ir teisinių įsipareigojimų rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Mokymų dažnumas: kartą per metus
10.	**Fizinis saugumas**
10.1.	Į tarnybinių stočių patalpas, gali patekti tik tokią teisę turintys asmenys
10.2.	Patalpose įrengti priešgaisriniai ir signalizacijos davikliai.
10.3.	Rakinamos patalpos.
10.4.	Pagrindinė techninė įranga turi turėti rezervinį maitinimą
10.5.	Tarnybinių stočių patalpos turi turėti kondicionavimo įrangą
10.6.	Prireikus turi būti kuriamos fizinės kliūtys, kad būtų užkirstas kelias neteisėtam fiziniam prieinamumui
10.7.	Administracijos darbuotojai privalo laikytis Švaraus stalo ir Švaraus ekrano politikos
10.8.	Išorės subjektų personalui, įgyvendinančiam teikiamas palaikymo paslaugas, turi būti suteikta ribota prieiga prie saugių zonų
11.	**Mobiliųjų įrenginių ir nuotolinio darbo valdymas**
11.1.	Mobiliųjų ir nešiojamų įrenginių (nešiojamuosiuose kompiuteriuose, planšetėse, išmaniuosiuose telefonuose ir pan.) administravimo procedūros nustatytos ir dokumentuotos, aiškiai aprašytas tinkamas tokių įrenginių naudojimas
11.2.	Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti
11.3.	Mobiliuosiuose įrenginiuose, jeigu jie naudojami ne Administracijos vidiniame kompiuterių tinkle, esantys asmens duomenys ir prisijungimo prie Administracijos tvarkomų asmens duomenų informacija šifruojami ar apsaugomi tokiomis priemonėmis, kurios atitiktų asmens duomenų atskleidimo keliamą riziką
11.4.	Administracija turi turėti galimybę nuotoliniu būdu ištrinti asmens duomenis mobiliajame, nešiojamame įrenginyje, kurio saugumas buvo sukompromituotas (pvz., pažeistos saugumo nuostatos, prarastas patikimumas)
11.5.	Nenaudojami mobilieji, nešiojamieji įrenginiai turi būti fiziškai apsaugoti nuo vagystės

11.6.	Darbo tikslais naudojamuose mobiliuosiuose įrenginiuose turi būti naudojamos ne mažesnio saugumo lygio priemonės, nei SIM kortelė su PIN kodu arba ekrano užsklanda su slaptažodžiu. SIM kortelės ir ekrano užsklandos kodai turi būti skirtingi
11.7.	Administracijos darbuotojams draudžiama leisti naudotis turimomis elektroninėmis darbo priemonėms tretiesiems asmenims (šeimos nariams ir kt.)
11.8.	Jei Administracijos darbuotojas Administracijos sutikimu naudoja darbui nuosavas elektronines darbo priemones, būtina užtikrinti, kad nuosavuose įrenginiuose bus įdiegtos tokios pačios apsaugos priemonės, kokios yra įdiegiamos Administracijos įrenginiuose. Neužtikrinus tinkamos apsaugos, nuosavus įrenginius naudoti darbui draudžiama
11.9.	Naudojant darbui nuosavus įrenginius, darbuotojas privalo darbo tikslais sukurti ir šios Saugumo politikos reikalavimus atitinkančiu slaptažodžiu apsaugoti atskirą paskyrą ir / arba naudoti kitas priemones, kurios padėtų atskirti duomenis, tvarkomus vykdant darbo funkcijas, nuo duomenų, tvarkomų asmeniniais tikslais
11.10.	Kai Administracijos darbuotojas baigia tarnybą Administracijoje arba nutraukia sutartį su Administracija, jis privalo Administracijos atstovo akivaizdoje ištrinti visus su darbu Administracijoje susijusius asmens duomenis iš nuosavų įrenginių ir išorinių laikmenų. Administracijos darbuotojas taip pat turi sudaryti galimybę Administracijos atstovui peržiūrėti darbo tikslams naudotus įrenginius ir įsitikinti, jog su darbu Administracijoje susiję asmens duomenys yra tinkamai ištrinti