ŠIAULIŲ DAINŲ PROGIMNAZIJOS DUOMENŲ SAUGUMO POLITIKA

1. BENDROSIOS NUOSTATOS

1.1. Įstaigos 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 3 skyriuje nurodytų reikalavimų vykdymo kontrolę atsakingas Saugumo specialistas, jei 3 skyriaus atskiruose papunkčiuose nenurodyta kitaip.

1.7. Už Saugumo politikos 4 skyriuje nurodytų reikalavimų įgyvendinimą yra atsakingas IT specialistas arba paslaugų teikėjas, su kuriuo sudaryta duomenų tvarkymo sutartis, sutartyje numatyta apimtimi; už įgyvendinimo kontrolę ir priežiūrą – Saugumo specialistas, jei 4 skyriaus atskiruose papunkčiuose nenurodyta kitaip.

2. ORGANIZACINĖS DUOMENŲ SAUGUMO PRIEMONĖS

2.1. Asmens duomenų saugumo politika ir procedūros

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

(ii) Dokumentai peržiūrimi ir prireikus atnaujinami ne rečiau kaip kartą per pusmetį.

(iii) 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.

(iv) Dokumentų sąrašas yra įtvirtintas Taisyklėse ir yra prižiūrimas Saugumo specialisto.

2.2. Vaidmenys ir atsakomybės

(i) Su Asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės yra aiškiai apibrėžti ir paskirstyti Dokumentuose.

(ii) 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.

(iii) DAP, IT specialistas ir Saugumo specialistas yra paskiriami Įstaigos vadovo įsakymu.

(iv) DAP negali būti paskirtas Saugumo specialistas ar IT specialistas. tačiau Saugumo specialistas ir IT specialistas gali būti vienas asmuo.

2.3. **Prieigos valdymo politika**

(i) 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 IT specialistas. Prieigos teisės yra nustatomos, atsižvelgiant į kiekvieno Darbuotojo pareigas, vykdomas funkcijas. IT 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 IT specialistas, tiesioginio konkretaus Darbuotojo vadovo siūlymu, esant Saugumo specialisto pritarimui. IT specialistas veda tokių prieigos teisių sąrašą.

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

(iii) 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.

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

(v) Jeigu Darbuotojas atleidžiamas iš darbo, pasikeičia jo funkcijos ir dėl to reikia keisti/naikinti prieigos teises, jo tiesioginis vadovas nedelsiant apie tai informuoja 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.

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

- fizinio priėjimo panaikinimą (pvz. raktų paėmimas);
- Įstaigos kompiuterinės ir programinės įrangos perėmimą, jei ji buvo suteikta Darbuotojui;
- bet kokių bendrų slaptažodžių ir PIN, kuriuos žinojo Darbuotojas, pakeitimą.

2.4. **Išteklių ir turto valdymas**

(i) IT specialistas veda IT išteklių (naudojamų asmens duomenims tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą) (forma Priedas Nr. 10 prie Taisyklių). IT išteklių registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę). IT išteklių registro tvarkymas priskiriamas IT specialistui.

(ii) IT išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas pagal poreikį, tačiau ne rečiau, kaip kartą per 3 mėnesius.

(iii) Asmenys, turintys prieigą prie IT išteklių, turi būti apibrėžti IT išteklių registre.

2.5. **Keitimų valdymas**

(i) Visi esminiai IT sistemų keitimai turi būti stebimi ir registruojami IT specialisto.

(ii) 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.

(iii) Visais atvejais esminiai IT sistemų keitimai privalo būti derinami su DAP, Saugumo specialistu bei IT specialistu, o realių duomenų naudojimui testavimo tikslais privalo būti gautas jų patvirtinimas. Įdiegiant pakeitimus taip pat privalo dalyvauti šie asmenys. IT specialistas ir Saugumo specialistas pasirūpina kad tiek dokumentiškai, tiek techniškai būtų įgyvendinti pareigybių ir vartotojų teisių pakeitimai arba paveda tai padaryti kitiems asmenims. IT specialistas ir Saugumo specialistas atsakingi už IT sistemų keitimo procedūros dokumentavimą.

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

(i) 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.

(ii) Darbuotojai, prieš pradėdami eiti savo pareigas, turi pasirašyti konfidencialumo įsipareigojimą (forma Priedas Nr. 20).

(iii) Už Konfidencialumo susitarimų su Darbuotojais sudarymą ir įsegimą į Darbuotojo bylą yra atsakingas Saugumo specialistas.

2.10. Mokymai

(i) Darbuotojų mokymai apie duomenų apsaugą Įstaigoje yra vykdomi Taisyklėse nustatyta tvarka.

(ii) 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.

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

(iv) Mokymus veda DAP arba išorinis paslaugų teikėjas.

3. TECHNINĖS DUOMENŲ SAUGUMO PRIEMONĖS

3.1. Prieigų kontrolė ir autentifikavimas

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

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

(iii) 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.

(iv) Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio.

(v) Vartotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. *hash form*).

(vi) Įstaigoje nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Tokiose taisyklėse apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius. Taisyklės įtvirtintos Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos apraše (Priedas Nr. 5 prie Taisyklių).

3.2. **Darbo vietų apsauga**

(i) Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų.

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

(iii) Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.

3.3. **Tinklo ir komunikacijos sauga**

(i) Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS/SSL).

(ii) Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidė prieiga turi būti apsaugota patikimais šifravimo mechanizmais.

(iii) Bet koks duomenų judėjimas iš, į IT sistemą stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo ir prevencijos sistemas.

3.4. **Fizinė sauga**

(i) Įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.

(ii) Patalpose įrengta signalizacija ir vaizdo kameros.

(iii) Laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos.

Priedas Nr. 1 prie

ASMENS DUOMENŲ SAUGUMO POLITIKOS

Organizacinė Įstaigos struktūra (pagal pareigybes)