Asmens duomenų tvarkymo taisyklių
Priedas Nr. 19

(forma)

ŠIAULIŲ DAINŲ PROGIMNAZIJOS
RIZIKO VERTINIMO ATASKAITA

_____

1. BENDROS PASTABOS

1.1. Šioje Rizikos vertinimo ataskaitoje vartojamos sąvokos turi reikšmę, nurodytą Įstaigos Asmens duomenų tvarkymo taisyklėse, jie kontekstas nereikalauja kitaip.

1.2. Pagal Bendrojo duomenų apsaugos reglamento 24 ir 32 straipsnius organizacijos įpareigotos visais atvejais atlikti rizikos vertinimą. Kuriant (diegiant) ar vertinant turimas organizacines ir technines saugumo priemones, organizacijos turi visapusiškai atsižvelgti į „duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus ir riziką, susijusią su pavojais fizinių asmenų teisėms ir laisvėms“.

1.3. Valstybinė duomenų apsaugos inspekcija 2020-06-18 patvirtino (3 versija) Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gaires duomenų valdytojams ir duomenų tvarkytojams (toliau – „**Gairės**“).

1.4. Atsižvelgiant į tai ir vadovaujantis Gairėmis, Įstaiga atlieka šį rizikos vertinimą ir nustato Įstaigoje taikomas duomenų saugumo priemones, kurios privalomos ir Įstaigos pasitelktiems duomenų tvarkytojams. Nustatytos priemonės įtvirtinamos Įstaigos Duomenų saugumo politikoje.

2. RIZIKOS VERTINIMAS

2.1. Duomenų tvarkymo operacijos nustatymas ir jos kontekstas

2.1.1. Kokios yra Įstaigos Asmens duomenų tvarkymo operacijos? Kokių kategorijų Asmens duomenys yra tvarkomi? Koks tvarkymo tikslas? Kokios yra Duomenų subjektų kategorijos? Kas yra duomenų gavėjai?

Šiame punkte nurodyta informacija apie duomenų tvarkymą yra pateikta Įstaigos duomenų tvarkymo veiklos įrašų šio rizikos vertinimo dienos aktualioje redakcijoje.

2.1.2. Kokios priemonės naudojamos tvarkyti Asmens duomenis? Kur vykdomas Asmens duomenų tvarkymas?

Duomenys surenkami tiesiogiai iš Duomenų subjektų ar jų naudojamos techninės įrangos, jų atstovų, sutarčių kontrahentų, vaizdo kamerų, valstybės institucijų. Duomenys perduodami elektroniniu paštu, saugomi serveriuose, spausdinami ir laikomi bylose, perduodami pagal teisės aktų reikalavimus.

2.2. Poveikio supratimas ir vertinimas

Žemas: fizinis asmuo gali susidurti su tam tikrais nepatogumais (pvz., sugaištas laikas iš naujo suvedant informaciją, susierzinimas, nepasitenkinimas ir pan.);

Vidutinis: fizinis asmuo gali patirti didelių nepatogumų, kuriuos jis galės įveikti nepaisant tam tikrų sunkumų (pvz., papildomos išlaidos, prieigos prie reikalingų išteklių praradimas, stresas, nedideli fiziniai negalavimai ir kt.);

Aukštas: fizinis asmuo gali patirti reikšmingas pasekmes ir norint jas ištaisyti, pašalinti reikės susidurti su rimtais sunkumais (pvz., lėšų praradimas, asmens įtraukimas į finansinių institucijų juodąjį sąrašą, turto nuostoliai (žala), darbo vietos praradimas, teisminiai procesai, sveikatos būklės pablogėjimas ir pan.) arba dideles ar negrįžtamas pasekmes, kurių negalės ištaisyti, pašalinti (pvz., negalėjimas dirbti, ilgalaikiai psichiniai ar fiziniai negalavimai, mirtis ir pan.).

Jeigu Įstaigoje Specialių kategorijų ar pažeidžiamų asmenų Asmens duomenys tvarkomi dideliu mastu arba vykdomas sistemingas ir išsamus asmens savybių vertinimas, grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, tai poveikis dėl galimo Asmens duomenų saugumo pažeidimo turėtų būti vertinamas kaip „Aukštas“.

Aukščiausias nustatytas poveikis laikomas galutiniu poveikio, susijusio su bendru asmens duomenų tvarkymu, įvertinimo rezultatu.

Nr.	Klausimas	Poveikis
1.	Ar Įstaigoje tvarkomi specialių kategorijų asmens duomenys dideliu mastu?	Ne
2.	Kokį poveikį gali sukelti neleistinas tvarkomų Asmens duomenų atskleidimas, konfidencialumo praradimas Įstaigos veiklos kontekste ir kokį tai galėtų turėti poveikį fiziniam asmeniui.	Žemas
3.	Kokį poveikį gali sukelti neleistinas tvarkomų Asmens duomenų pakeitimas, vientisumo praradimas Įstaigos veiklos kontekste ir kokį tai galėtų turėti poveikį fiziniam asmeniui.	Žemas

4.	Kokį poveikį gali sukelti neleistinas tvarkomų Asmens duomenų sunaikinimas ar prieigos praradimas Įstaigos veiklos kontekste ir kokį tai galėtų turėti poveikį fiziniam asmeniui.	Žemas

Nustatytas poveikis – Žemas.

2.3. Galimų grėsmių nustatymas ir jų atsiradimo tikimybės vertinimas

2.3.1. Grėsmių ir jų atsiradimo tikimybės vertinimo klausimai

Tinklo ir techniniai ištekliai		
1.	Ar Įstaigoje yra sistemų ar įrenginių su asmens duomenimis, kurie prieinami internetu?	Ne
2.	Ar galima internetu prisijungti prie vidinių asmens duomenų tvarkymo sistemų (pvz., tam tikriems vartotojams arba vartotojų grupėms)	Ne
3.	Ar Įstaigos sistemos, kuriose tvarkomi asmens duomenys, yra tarpusavyje sujungtos, integruotos su kitomis išorinėmis ar vidinėmis informacinių technologijų (IT) sistemomis arba paslaugomis	Ne
4.	Ar neįgalioti asmenys gali lengvai prieiti prie duomenų tvarkymo aplinkos (pvz., neužtikrinamas tinkamas fizinės prieigos prie IT įrangos saugumas)?	Ne
5.	Ar Įstaigoje yra asmens duomenų tvarkymui naudojamų IT sistemų, kurios sukurtos ar įdiegtos nesilaikant gerosios praktikos (pvz., Agile, ISO 27000, ITIL ir kt.)?	Ne
Procesai ir procedūros, susiję su asmens duomenų tvarkymu		
6.	Ar Įstaigoje prieigos ir (ar) atsakomybės yra neaiškios arba neaiškiai apibrėžtos?	Ne
7.	Ar Įstaigoje yra / pasitaiko neaiškumų (dviprasmiškai suprantamų instrukcijų) dėl tinklo, sistemų ar fizinių išteklių naudojimo?	Ne
8.	Ar darbuotojams leidžiama naudoti asmeninius prietaisus, įrenginius ir jais prisijungti prie organizacijos asmens duomenų tvarkymo sistemų?	Ne
9.	Ar darbuotojams leidžiama perkelti, saugoti ar kitaip tvarkyti organizacijos asmens duomenis už organizacijos ribų (pvz., nešiojamuosiuose įrenginiuose, laikmenose)?	Ne
10.	Ar asmens duomenų tvarkymo veiksmai gali būti atliekami, nefiksuojant jų (be veiksmų atsekamumo) sistemų žurnalų įrašuose (angl. log files)?	Taip
Duomenų tvarkymo dalyviai		
11.	Ar asmens duomenis tvarko neapibrėžtas (nenustatytas konkrečiai) darbuotojų skaičius?	Ne
12.	Ar yra Įstaigos valdomų asmens duomenų, kuriuos tvarko duomenų tvarkytojai (pvz., rangovai, trečiosios šalys)?	Ne

13.	Ar Įstaigoje yra dviprasmiškai arba neaiškiai apibrėžtų asmens duomenų tvarkymo prievolių, susijusių su trečiosiomis šalimis / asmenimis?	Ne
14.	Ar Įstaigoje yra darbuotojų, dalyvaujančių asmens duomenų tvarkyme, bet kuriems trūksta kompetencijų konfidencialiai tvarkyti informaciją techniniu ar asmeninio sąžiningumo požiūriu?	Ne
15.	Ar Įstaigoje yra darbuotojų arba kitų duomenų tvarkytojų, dalyvaujančių asmens duomenų tvarkyme, kurie neturi galimybių tinkamai sunaikinti asmens duomenų laikmenas?	Ne
Veiklos sritys ir duomenų tvarkymo mastai		
16.	Ar Įstaiga, atsižvelgiant į jos veiklos sritį, potencialiai galėtų tapti dažnesniu kibernetinių atakų taikiniu?	Ne
17.	Ar per pastaruosius dvejus metus Įstaigoje buvo įvykęs asmens duomenų saugumo pažeidimas ar kitas saugumo incidentas?	Ne
18.	Ar per pastaruosius metus Įstaiga gavo kokius nors pranešimus ir (arba) skundus dėl IT sistemų, naudojamų asmens duomenų tvarkymui, saugumo?	Ne
19.	Ar Įstaiga tvarko asmens duomenis dideliu mastu? (Atsižvelgiama į šiuos veiksnius: susijusių duomenų subjektų skaičių - konkretų skaičių arba atitinkamo gyventojų skaičiaus procentinę dalį; duomenų vienetų kiekį ir (arba) intervalą; duomenų tvarkymo veiklos trukmę arba pastovumą; geografinę duomenų tvarkymo aprėptį (pvz., duomenys tvarkomi regioniniu, nacionaliniu ar tarpvalstybiniu lygmeniu).	Ne
20.	Ar yra veiklai (veiklos sričiai) būdingos gerosios saugumo praktikos ar standartų, kurių Jūsų organizacijoje nesilaikoma?	Ne

2.3.2. Grėsmės atsiradimo tikimybės įvertinimas kiekvienai sričiai

Kiekvienai vertinamai sričiai gali būti nustatytas grėsmės atsiradimo tikimybės lygis:

Žemas: mažai tikėtina, kad grėsmė pasitvirtins (jeigu iš penkių klausimų gautas ne daugiau kaip vienas atsakymai „Taip“);

Vidutinis: yra reali galimybė, kad grėsmė pasitvirtins (jeigu iš penkių klausimų gauti ne mažiau kaip du ir ne daugiau kaip trys atsakymai „Taip“);

Aukštas: tikėtina, kad grėsmė pasitvirtins (jeigu iš penkių klausimų gauti daugiau kaip trys atsakymai „Taip“).

Vertinimo sritis	**Tikimybė**	
	Lygis (žemas;vidutinis;aukštas)	**Balas (1;2;3)**

Tinklo ir techniniai ištekliai	Žemas	1
Procesai ir procedūros, susiję su asmens duomenų tvarkymu	Žemas	1
Duomenų tvarkymo dalyviai	Žemas	1
Veiklos sritys ir duomenų tvarkymo mastai	Žemas	1

2.3.3. Grėsmės atsiradimo įvertinimas pagal žemiau pateiktą lentelę – **žemas** (4 balai).

Bendra grėsmės atsiradimo balų suma	Grėsmės atsiradimo tikimybės lygis
4–5	Žemas
6–8	Vidutinis
9–12	Aukštas

2.3.4. Rizikos įvertinimas

		Poveikio lygis		
		Žemas	Vidutinis	Aukštas
Grėsmes atsiradimo tikimybės lygis	Žemas			
	Vidutinis			+
	Aukštas			

3. DUOMENŲ SAUGUMO PRIEMONIŲ VERTINIMAS (pagal Gaires)

Priemonės	Pastabos („Įgyvendinta“ arba „Įgyvendinti iki [___]“, arba „Nuspręsta neįgyvendinti“)

ORGANIZACINĖS DUOMENŲ SAUGUMO PRIEMONĖS	
Asmens duomenų saugumo politika ir procedūros	
Asmens duomenų ir jų tvarkymo saugumas organizacijoje turi būti dokumentuotas kaip informacijos saugumo politikos dalis.	Įgyvendinta
Organizacijos duomenų saugumo politika turi nustatyti bent: personalo pareigas (funkcijas) ir atsakomybes, pagrindines technines ir organizacines priemones, įdiegtas asmens duomenų saugumui užtikrinti, taip pat duomenų tvarkytojų ar trečiųjų šalių, susijusių su asmens duomenų tvarkymu, sąrašą.	Įgyvendinta
Atsižvelgiant į bendrą saugumo politiką, turi būti sukurtas ir prižiūrimas konkrečių su asmens duomenų saugumu susijusių politikos dokumentų, procedūrų, tvarkų aprašas.	Įgyvendinta
Saugumo politika turi būti peržiūrima ir, prireikus, tikslinama kas pusmetį.	Įgyvendinta
Vaidmenys ir atsakomybės	
Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal saugumo politiką.	Įgyvendinta
Turi būti aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras (vidaus organizacijos pertvarkymo ar darbuotojų atleidimo, funkcijų pasikeitimo metu).	Įgyvendinta
Reikėtų atlikti aiškų asmenų, atsakingų už konkrečias saugumo užduotis, paskyrimą, įskaitant saugos specialisto (saugos įgaliotinio) paskyrimą.	Įgyvendinta
Saugos specialistas turi būti oficialiai paskirtas (paskyrimą patvirtinant dokumentais). Saugos specialisto uždaviniai ir atsakomybės turi būti aiškiai nustatyti ir dokumentuoti.	Įgyvendinta
Nesuderinamos pareigybės (funkcijos) ir atsakomybių sritys, pavyzdžiui, saugos specialisto pareigybė ir duomenų apsaugos pareigūno pareigybė, turi būti atskirtos, siekiant sumažinti neleistino ar netyčinio asmens duomenų keitimo ar netinkamo naudojimo galimybes.	Įgyvendinta
Prieigos valdymo politika	

Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. need to know) principu.	Įgyvendinta
Prieigos kontrolės politika turi būti išsami ir dokumentuota. Organizacija šiame dokumente turi nustatyti atitinkamas prieigos kontrolės taisykles, prieigos teises ir apribojimus pagal konkrečias naudotojų pareigas, susijusias su asmens duomenų tvarkymo procesais ir procedūromis.	Įgyvendinta
Prieigos kontrolę užtikrinančių funkcijų atskyrimas (pvz., prieigos užklausų, prieigos leidimų, pačios prieigos administravimas) turi būti aiškiai apibrėžtas ir dokumentuotas	Įgyvendinta
Tam tikros pareigybės (funkcijos), turinčios dideles prieigos teises, turi būti aiškiai apibrėžtos ir priskirtos tik ribotam darbuotojų skaičiui.	Įgyvendinta
Išteklių ir turto valdymas	
Organizacija turi turėti IT išteklių (naudojamų asmens duomenims tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą). 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 turi būti priskirtas konkrečiam asmeniui, pvz., IT specialistui.	Įgyvendinta
IT išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas. Rekomenduojamas peržiūros dažnumas – kartą per 3 mėnesius.	Įgyvendinta
Visos pareigybės, turinčios prieigą prie IT išteklių, turi būti apibrėžtos ir patvirtintos dokumentais.	Įgyvendinta
Keitimų valdymas	
Organizacija turi užtikrinti, kad visi esminiai IT sistemų keitimai būtų stebimi ir registruojami konkretaus asmens (pvz., IT arba saugos specialisto).	Įgyvendinta
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	Įgyvendinta

Turi būti įdiegta išsami ir dokumentais pagrįsta IT keitimų valdymo politika. Keitimų valdymo politiką turi apibrėžti: pokyčių įvedimo ir įdiegimo procedūras, pareigybes ir vartotojus, kurių teisės buvo pakeistos, pokyčių įdiegimo laiko terminus. Pokyčių valdymo politika turi būti reguliariai atnaujinama.	Įgyvendinta
Duomenų tvarkytojai	
Prieš pradedant asmens duomenų tvarkymo veiklą, duomenų valdytojai turi apibrėžti, dokumentuoti ir suderinti formalias gaires ir procedūras, taikomas duomenų tvarkytojams (pvz., rangovams ar užsakomųjų paslaugų tiekėjams) dėl asmens duomenų tvarkymo. Šios gairės ir procedūros turi nustatyti tokį patį (ne žemesnį) asmens duomenų saugumo lygį, koks yra numatytas organizacijos saugumo politikoje.	Įgyvendinta
Duomenų tvarkytojas privalo nedelsdamas pranešti duomenų valdytojui apie nustatytus asmens duomenų saugumo pažeidimus.	Įgyvendinta
Duomenų tvarkytojas turi pateikti dokumentais pagrįstus įrodymus dėl atitikties jam keliamiems reikalavimams.	Įgyvendinta
Duomenų valdytojas turi reguliariai tikrinti duomenų tvarkytojo atitiktį nustatytų reikalavimų ir įsipareigojimų lygiui.	Įgyvendinta
Duomenų tvarkytojo darbuotojams, dirbantiems su asmens duomenimis, turi būti taikomi konkretūs dokumentais įtvirtinti informacijos konfidencialumo, neatskleidimo susitarimai.	Įgyvendinta
Asmens duomenų saugumo pažeidimai ir saugumo incidentai	
Turi būti nustatytas reagavimo į saugumo incidentus planas, užtikrinantis veiksmingą incidentų, susijusių su asmens duomenų saugumu, valdymą.	Įgyvendinta
Asmens duomenų saugumo pažeidimai turi būti fiksuojami (dokumentuojami). Apie juos turi būti nedelsiant pranešama vadovybei. Turi būti nustatyta pranešimo apie asmens duomenų saugumo pažeidimus kompetentingoms institucijoms ir duomenų subjektams tvarka.	Įgyvendinta
Saugumo incidentų likvidavimo planas turi būti patvirtintas dokumentais, tarp kurių būtų galimų saugumo incidento poveikio mažinimo priemonių sąrašas ir aiškus atskirų funkcijų paskirstymas.	Įgyvendinta

Visi saugumo incidentai, įskaitant ir asmens duomenų saugumo pažeidimus, turi būti fiksuojami kartu su visa susijusia informacija apie įvykį ir vėliau atliktus incidento poveikio mažinimo veiksmus.	Įgyvendinta
Veiklos tęstinumas	
Organizacija turi nustatyti pagrindines procedūras, kurių reikia laikytis saugumo incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas.	Įgyvendinta
Veiklos tęstinumo planas turi būti išsamiai apibūdintas ir patvirtintas dokumentais (laikantis bendros saugumo politikos). Jame turi būti pateiktas aiškus veiksmų planas ir funkcijų paskirstymas.	Įgyvendinta
Veiklos tęstinumo plane turi būti apibrėžtas garantuotos paslaugų kokybės lygis (angl. Service-level agreement (SLA), kuris nustatomas pagrindiniams veiklos procesams, kurie užtikrina asmens duomenų saugumą.	Įgyvendinta
Turi būti paskirti darbuotojai, turintys reikiamą atsakomybę, įgaliojimus ir kompetenciją valdyti veiklos tęstinumą saugumo incidento, asmens duomenų saugumo pažeidimo atveju.	Įgyvendinta
Turi būti numatyta alternatyvi infrastruktūros priemonė organizacijos darbui, atsižvelgiant į organizaciją ir jai priimtiną IT sistemų prastovą.	Įgyvendinta
Personalo konfidencialumas	
Organizacija turi užtikrinti, kad visi darbuotojai suprastų savo atsakomybes ir įsipareigojimus, susijusius su asmens duomenų tvarkymu. Vaidmenys ir atsakomybės turi būti aiškiai išdėstyti darbuotojui prieš pradedant vykdyti jam paskirtas funkcijas ir darbus.	Įgyvendinta
Darbuotojai, atsakingi už aukštos rizikos asmens duomenų tvarkymo operacijas, turi laikytis konkrečių jiems taikomų konfidencialumo sąlygų (pagal jų darbo sutartį ar kitą teisės aktą).	Įgyvendinta
Darbuotojai, prieš pradėdami eiti savo pareigas, turi būti pasirašytinai supažindinti su organizacijos saugumo politika, taip pat pasirašyti atitinkamus informacijos konfidencialumo ir neatskleidimo susitarimus.	Įgyvendinta
Mokymai	

Organizacija turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo reikalavimus, susijusius su jų kasdieniu darbu. Darbuotojai, susiję su asmens duomenų tvarkymu, turi būti mokomi apie atitinkamus duomenų saugumo reikalavimus ir atsakomybes, rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Siūlomas mokymų periodiškumas – kartą per metus.	Įgyvendinta
Organizacija turi rengti struktūrines nuolatines personalo mokymų programas, tarp kurių būtų ir speciali programa, skirta mokyti naujus darbuotojus (duomenų apsaugos tema).	Įgyvendinta
Kiekvienais metais turi būti parengtas ir įgyvendintas mokymų planas, kuriame būtų nustatyti siektini tikslai ir uždaviniai.	Įgyvendinta
TECHNINĖS DUOMENŲ SAUGUMO PRIEMONĖS	
Prieigų kontrolė ir autentifikavimas	
Turi būti įdiegta, įgyvendinta prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras.	Įgyvendinta
Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas.	Įgyvendinta
Turi būti 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.	Įgyvendinta
Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio.	Įgyvendinta
Vartotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. hash form).	Įgyvendinta
Turi būti nustatytos ir dokumentais patvirtintos slaptažodžių taisyklės. Taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius. naudojimo	Įgyvendinta

Privilegijuotiems vartotojams (pvz., sistemų administratoriams) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas dviejų veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamas dviejų veiksnių autentifikavimas. Autentifikavimo veiksniais gali būti slaptažodžiai, saugumo žetonai, USB raktai su slapta žyma, biometriniai duomenys ir kt.	Įgyvendinta
Turi būti naudojamas įrenginio autentifikavimas, garantuojantis, kad 21 asmens duomenys tvarkomi tik naudojant konkrečius tinklo įrenginius (pvz., 802.1X, RADIUS ir kt.).	Įgyvendinta
Techninių žurnalų įrašai ir stebėsena	
Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). Rekomenduojamas saugojimo terminas – ne trumpiau kaip 6 mėnesiai.	Įgyvendinta
Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį.	Įgyvendinta
Visi sistemų administratorių ir operatorių veiksmai (taip pat ir jų atliekamas vartotojo teisių papildymas, panaikinimas, keitimas) turi būti registruojami.	Įgyvendinta
Turi būti neįmanoma ištrinti ar pakeisti techninių įrašų turinio. Prieiga prie įrašų taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną.	Netaikoma
Stebėsenos sistema turi apdoroti techninius įrašus, ruošti sistemos būklės ataskaitas ir įspėti apie galimus pavojus	Įgyvendinta
Tarnybinių stočių, duomenų bazių apsauga	Netaikoma
Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos (OS) privilegijomis.	Netaikoma
Duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie asmens duomenys, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus.	Netaikoma

Konkrečioms saugomoms byloms ar įrašams apsaugoti turėtų būti naudojamas šifravimas, įdiegiant atitinkamą programinę ar techninę įrangą.	Netaikoma
Duomenų bazėse turi būti taikomi pseudonimizavimo metodai, atskiriant tiesioginius identifikatorius nuo esamų sąsajų su kitais duomenimis.	Netaikoma
Duomenų bazėje turi būti taikomi autorizuotų užklausų, šifruotos paieškos ir kiti privatumo užtikrinimo metodai.	Netaikoma
Darbo vietų apsauga	
Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų.	Įgyvendinta
Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti atnaujinamos ne rečiau kaip kas savaitę, rekomenduojama kartą per parą ar dažniau.	Įgyvendinta
Naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotos programinės įrangos.	Įgyvendinta
IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Rekomenduojamas neaktyvios sesijos laikas – ne ilgiau kaip 15 min.	Įgyvendinta
Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.	Įgyvendinta
Antivirusinės taikomosios programos ir jų informacijos apie virusus bei kenkimo programinę įrangą duomenų bazės turi būti atnaujinamos ne rečiau kaip kartą per parą.	Įgyvendinta
Turi būti uždrausta perduoti asmens duomenis iš kompiuterinių darbo vietų į išorinius saugojimo įrenginius (pvz., USB raktai, DVD, išorinius standžiuosius diskus ir kt.).	Netaikoma
Pageidautina, kad asmens duomenų tvarkymui naudojamos kompiuterinės darbo vietos nebūtų prijungtos prie interneto, nebent būtų imamasi saugumo priemonių, kad būtų išvengta neteisėto asmens duomenų tvarkymo, kopijavimo ir perdavimo.	Netaikoma
Kompiuterinėse darbo vietoje naudojamuose operacinės sistemos diskuose turi būti įgalintas pilnas standžiojo disko šifravimas (angl. fulldisk encryption).	Netaikoma

Tinklo ir komunikacijos sauga	
Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS/SSL).	Įgyvendinta
Belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidė prieiga turi būti apsaugota patikimais šifravimo mechanizmais.	Įgyvendinta
Reikėtų vengti nuotolinės prieigos prie IT sistemų. Tais atvejais, kai ši prieiga yra išties reikalinga, ji yra galima tik organizacijos paskirtam darbuotojui (pvz., sistemų administratoriui, saugumo specialistui) kontroliuojant ir stebint jos veikimą per iš anksto nustatytus įrenginius.	Netaikoma
Bet koks duomenų judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo ir prevencijos sistemas.	Įgyvendinta
Prisijungimas prie interneto neturi būti leidžiamas tarnybinėms stotims ir jose esančiai programinei įrangai, naudojamai asmens duomenims tvarkyti.	Įgyvendinta
Informacinės sistemos tinklas turi būti atskirtas nuo kitų duomenų valdytojo tinklų.	Įgyvendinta
Prieiga prie IT sistemos turi būti atliekama tik iš patvirtintų įrenginių ir terminalų, naudojant tam skirtas technologijas, pvz., MAC adresų filtravimą arba tinklo prieigos kontrolę.	Netaikoma
Atsarginės kopijos	
Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis.	Netaikoma
Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų.	Įgyvendinta
Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą.	Netaikoma
Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Rekomenduojamas atsarginių kopijų darymo dažnumas: - kasdien – pridedamoji kopija; - kas savaitę – pilna kopija.	Netaikoma

Atsarginės kopijos turi būti reguliariai testuojamos, siekiant užtikrinti, kad jos galėtų būti patikimai naudojamos ekstremalioje situacijoje.	Netaikoma
Reguliarus atsarginių kopijų kūrimas ar bent reguliarus papildantysis (angl. incremental) atsarginių kopijų kūrimas turi būti atliekamas bent kartą per parą.	Netaikoma
Atsarginės kopijos turi būti saugiai laikomos skirtingose vietose, kurios turi 26 būti geografiškai nutolusios viena nuo kitos.	Netaikoma
Atsarginės kopijos turi būti šifruojamos ir saugiai laikomos visiškai atjungus (angl. offline) nuo kompiuterinių tinklų.	Netaikoma
Mobilieji, nešiojamieji įrenginiai	Netaikoma
Mobiliųjų, nešiojamųjų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimą.	Netaikoma
Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti.	Netaikoma
Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti.	Netaikoma
Mobiliųjų, nešiojamųjų įrenginių valdymo funkcijos ir atsakomybės turi būti aiškiai apibrėžtos.	Netaikoma
Organizacija turi turėti galimybę nuotoliniu būdu ištrinti asmens duomenis mobiliajame, nešiojamame įrenginyje, kurio saugumas buvo sukompromituotas (pvz., pažeistos 27 saugumo nuostatos, prarastas patikimumas).	Netaikoma
Mobiliuosiuose, nešiojamuosiuose įrenginiuose turi būti atskirti privatūs ir organizacijos veiklos duomenys, naudojant saugias programinės įrangos talpyklas (konteinerius).	Netaikoma
Nenaudojami mobilieji, nešiojamieji įrenginiai turi būti fiziškai apsaugoti nuo vagystės.	Netaikoma
Prieigai prie mobiliųjų, nešiojamųjų įrenginių turėtų būti naudojamas dviejų veiksnių autentifikavimas.	Netaikoma

Asmens duomenys, saugomi mobiliajame įrenginyje (kaip organizacijos duomenų tvarkymo operacijos dalis), turi būti užšifruoti.	Netaikoma
Programinės įrangos sauga	Netaikoma
Informacinėse sistemose naudojama programinė įranga (asmens duomenims tvarkyti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras (angl. frameworks), standartus (pvz., Agile, OWASP ir kt.).	Netaikoma
Specifiniai saugos reikalavimai, susiję su organizacijos veiklos ypatumais, turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.	Netaikoma
Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.	Netaikoma
Po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją, jau turi būti laikomasi pagrindinių saugos reikalavimų.	Netaikoma
Prieš paleidžiant programinę įrangą, turi būti atliktas programinės įrangos ir infrastruktūros pažeidžiamumo ir atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti priimta naudoti, kol nėra pasiektas reikiamas saugumo lygis.	Netaikoma
Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai.	Netaikoma
Programinės įrangos atnaujinimai turi būti ištestuoti ir įvertinti prieš juos diegiant į darbo aplinką atitinkamomis veiklos sąlygomis.	Netaikoma
Duomenų naikinimas, šalinimas	
Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jei to padaryti neįmanoma (pvz., DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti.	Įgyvendinta
Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis	Įgyvendinta

Prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai (angl. *Multiple passes of software-based overwriting*).	Netaikoma
Jei saugiems duomenų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti sudaryta atitinkama paslaugų sutartis ir atliekamas sunaikintų įrašų protokolavimas	Netaikoma
Po duomenų ištrynimo reikėtų imtis papildomų priemonių, pvz., gali būti atliktas nepageidaujamos magnetinės informacijos pašalinimas (išmagnetinimas). Priklausomai nuo konkretaus atvejo, reikėtų įvertinti fizinio sunaikinimo galimybes.	Netaikoma
Jei saugiems įrašų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti užtikrinta, kad šis procesas vyktų duomenų valdytojo ir (ar) tvarkytojo patalpose, siekiant išvengti duomenų perdavimo trečiosioms šalims. Atskirais atvejais, kai to neįmanoma atlikti duomenų valdytojo ir (ar) tvarkytojo patalpose, sunaikinimas gali būti atliekamas kitoje fizinėje vietoje, tačiau tik stebint įgaliotam duomenų valdytojo atstovui.	Netaikoma
Fizinė sauga	
Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.	Įgyvendinta
Būtina naudoti aiškią visų darbuotojų ir lankytojų identifikavimo sistemą, naudojant tinkamas priemones.	Netaikoma
Atitinkamos saugios zonos turėtų būti apibrėžtos ir apsaugotos tinkamomis patekimo kontrolės priemonėmis. Popierinis ar elektroninis registravimo rinkmenų žurnalas turi būti saugiai laikomas, prižiūrimas ir stebimas.	Netaikomas
Įsilaužimo (įsibrovimo) aptikimo sistemos turi būti įdiegtos visose saugumo zonose.	Įgyvendinta
Prireikus turi būti kuriamos fizinės kliūtys, kad būtų užkirstas kelias neteisėtam fiziniam prieinamumui.	Netaikoma
Laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos.	Įgyvendinta

Tarnybinių stočių patalpoje turėtų būti įdiegta automatinė gaisro gesinimo sistema, uždara valdoma oro kondicionavimo sistema ir nepertraukiamo maitinimo šaltinis.	Netaikoma
Išorės subjektų personalui, įgyvendinančiam teikiamas palaikymo paslaugas, turi būti suteikta ribota prieiga prie saugių zonų.	Netaikoma

4. DAP NUOMONĖ

[___]

PATVIRTINTA

_____
(pareigos, vardas, pavardė, parašas) A.V.