PATVIRTINTA
Vilniaus r. Nemenčinės muzikos
mokyklos direktoriaus
2021 m. balandžio 22 d.
įsakymo Nr. V - 8

VILNIAUS R. NEMENČINĖS MUZIKOS MOKYKLOS

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 pakeitimus, 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 1 priedas. 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 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 (9 priedas 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 (9 priedas 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) (10 priedas 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 (6 priedas 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 (6 priedas prie Taisyklių) ir Duomenų tvarkymo informacinės sistemos veiklos tęstinumo valdymo plane (8 priedas 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 20 priedas).

(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) 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.

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

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

(v) 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 (5 priedas prie Taisyklių).

3.2. **Techninių žurnalų įrašai ir stebėsena**

(i) Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai tvarkyti Asmens duomenims. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie Asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). Saugojimo terminas – ne trumpiau kaip 6 mėnesiai.

(ii) 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.

(iii) Visi sistemų administratorių ir operatorių veiksmai (taip pat ir jų atliekamas vartotojo teisių papildymas, panaikinimas, keitimas) turi būti registruojami.

(iv) Turi būti neįmanoma ištrinti ar pakeisti techninių įrašų turinio. Prieiga prie įrašų taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną.

(v) Stebėsenos sistema turi apdoroti techninius įrašus, ruošti sistemos būklės ataskaitas ir įspėti apie galimus pavojus.

3.3. **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) IT sistemos turi nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija yra nutraukiama. Neaktyvios sesijos laikas – ne ilgiau kaip 15 min. Ekrano užsklandą galima pašalinti tik įvedus slaptažodį arba PIN kodą. Penkis kartus įvedus neteisingą slaptažodį arba PIN kodą, prietaisas turi užsiblokuoti taip, kad jį atblokuoti galėtų tik IT specialistas.

(iv) Mobiliuose įrenginiuose turi būti nustatyta, kad nedirbant su jais ne ilgiau kaip 2 minutes, automatiškai įsijungtų ekrano užsklanda, kurią būtų galima pašalinti tik įvedus slaptažodį, PIN kodą. Penkis kartus įvedus neteisingą slaptažodį arba PIN kodą, prietaisas turi užsiblokuoti ne trumpiau kaip 5 minutėms. Už šių reikalavimų vykdymą atsakingas Darbuotojas, naudojantis įrenginį.

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

(vi) Antivirusinės taikomosios programos ir jų informacijos apie virusus bei kenkimo programinę įrangą duomenų bazės turi būti atnaujinamos ne rečiau kaip kartą per parą.

(vii) Draudžiama perduoti asmens duomenis iš kompiuterinių darbo vietų, kuriose dideliu mastu tvarkomi pažeidžiamų asmenų ar Specialių kategorijų asmens duomenys, į išorinius saugojimo įrenginius (pvz., USB raktai, DVD, išorinius standžiuosius diskus ir kt.). Už šio draudimo laikymąsi atsako kiekvienas naudotojas.

(viii) Pageidautina, kad dideliu mastu tvarkomų pažeidžiamų asmenų ar Specialių kategorijų 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.

(ix) Kompiuterinėse darbo vietose, naudojamose pažeidžiamų asmenų ar Specialių kategorijų asmens duomenų tvarkymui dideliu mastu, naudojamuose operacinės sistemos diskuose turi būti įgalintas pilnas standžiojo disko šifravimas (angl. *fulldisk encryption*).

3.4. **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) 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.

(iii) Nuotolinė prieiga Darbuotojams suteikiama Darbuotojo prašymu patvirtinus jo tiesioginiam vadovui. Darbui per nuotolį ir techninei įrangai taikomi tokie patys reikalavimai, kaip ir fiziškai dirbant Įstaigoje. IT specialistas kontroliuoja ir stebi nuotolinės prieigos veikimą per iš anksto nustatytus įrenginius. Kilus įtarimų, kad dėl nuotolinio darbo gali būti pažeistas Asmens duomenų konfidencialumas, prieiga panaikinama.

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

(v) Prisijungimas prie interneto neturi būti leidžiamas tarnybinėms stotims ir jose esančiai programinei įrangai, naudojamai pažeidžiamų asmenų ir Specialių kategorijų asmens duomenims tvarkymui dideliu mastu.

(vi) Informacinės sistemos tinklas, kuriame dideliu mastu tvarkomi pažeidžiamų asmenų ir Specialių kategorijų asmens duomenys, turi būti atskirtas nuo kitų Įstaigos tinklų.

(vii) Prieiga prie IT sistemos, kurioje dideliu mastu tvarkomi pažeidžiamų asmenų ir Specialių kategorijų asmens duomenys, turi būti atliekama tik iš patvirtintų įrenginių ir terminalų, naudojant tam skirtas technologijas, pvz., MAC adresų filtravimą arba tinklo prieigos kontrolę.

3.5. **Atsarginės kopijos**

(i) Atsarginės kopijos (angl. *backup*) daromos automatiškai, naudojant specializuotą programinę įrangą, į rezervinėje serverinėje esančią atsarginių kopijų informacinę

sistemą. Duomenys iš atsarginių kopijų atstatomi nedelsiant, bet ne vėliau kaip per 8 valandas darbo dieną.

(ii) Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų.

(iii) Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą.

(iv) Atsarginės kopijos turi būti testuojamos kas mėnesį, siekiant užtikrinti, kad jos galėtų būti patikimai naudojamos ekstremalioje situacijoje.

(v) Reguliarus atsarginių kopijų kūrimas ar bent reguliarus papildantysis (angl. *incremental*) atsarginių kopijų kūrimas turi būti atliekamas bent kartą per parą, pilna kopija ne rečiau nei kartą per savaitę.

(vi) Atsarginės kopijos turi būti saugiai laikomos skirtingose vietose, kurios turi būti geografiškai nutolusios viena nuo kitos.

(vii) Dideliu mastu tvarkomų pažeidžiamų asmenų ir Specialių kategorijų asmens duomenų atsarginės kopijos turi būti šifruojamos ir saugiai laikomos visiškai atjungus (angl. *offline*) nuo kompiuterinių tinklų.

3.6. **Mobilieji, nešiojamieji įrenginiai**

(i) Mobiliųjų, nešiojamųjų įrenginių administravimo procedūros nustatytos ir dokumentuotos Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos apraše (5 priedas prie Taisyklių).

(ii) Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti.

(iii) Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga Asmens duomenims tvarkyti.

(iv) Mobiliųjų, nešiojamųjų įrenginių valdymo funkcijos ir atsakomybės apibrėžtos Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos apraše (5 priedas prie Taisyklių).

(v) Įstaiga turi turėti galimybę nuotoliniu būdu ištrinti Asmens duomenis mobiliajame, nešiojamame įrenginyje, kurio saugumas buvo sukompromituotas (pvz., pažeistos saugumo nuostatos, prarastas patikimumas).

(vi) Mobiliuosiuose, nešiojamuosiuose įrenginiuose turi būti atskirti privatūs ir Įstaigos veiklos duomenys, naudojant saugias programinės įrangos talpyklas (konteinerius).

(vii) Nenaudojami mobilieji, nešiojamieji įrenginiai turi būti fiziškai apsaugoti nuo vagystės.

(viii) Prieigai prie mobiliųjų, nešiojamųjų įrenginių, kuriuose dideliu mastu tvarkomi pažeidžiamų asmenų ir Specialių kategorijų asmens duomenys, turėtų būti naudojamas dviejų veiksnių autentifikavimas.

(ix) Dideliu mastu tvarkomi pažeidžiamų asmenų ir Specialių kategorijų asmens duomenys, saugomi mobiliajame įrenginyje (kaip organizacijos duomenų tvarkymo operacijos dalis), turi būti užšifruoti.

3.7. **Programinės įrangos sauga**

(i) 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.).

(ii) Specifiniai saugos reikalavimai, susiję su Įstaigos veiklos ypatumais, turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.

(iii) Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.

(iv) Po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją, jau turi būti laikomasi pagrindinių saugos reikalavimų.

(v) 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.

(vi) Turi būti atliekami periodiški, ne rečiau kaip kartą per dvejus metus, infrastruktūros atsparumo skverbimuisi testavimai.

(vii) Specialiai Įstaigai sukurti programinės įrangos atnaujinimai turi būti ištestuoti ir įvertinti prieš juos diegiant į darbo aplinką atitinkamomis veiklos sąlygomis.

3.8. **Duomenų naikinimas, šalinimas**

(i) Prieš pašalinant bet kokią duomenų laikmeną turi būti sunaikinti visi joje esantys duomenys. Jei to padaryti neįmanoma (pvz., DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti.

(ii) Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis.

(iii) Jei būtina, prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai (angl. *Multiple passes of software-based overwriting*).

(iv) 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.

(v) Po dideliu mastu tvarkomų pažeidžiamų asmenų ir Specialių kategorijų asmens duomenų ištrynimo, reikėtų imtis papildomų priemonių, pvz., gali būti atliktas nepageidaujamos magnetinės informacijos pašalinimas (išmagnetinimas). Priklausomai nuo konkretaus atvejo reikėtų įvertinti fizinio sunaikinimo galimybes.

(vi) Kiek tai liečia pažeidžiamų asmenų ar Specialių kategorijų asmens duomenų tvarkymą dideliu mastu, jei saugiems įrašų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos Trečiojo asmens paslaugos, turi būti užtikrinta, kad šis procesas vyktų Įstaigos patalpose, siekiant išvengti Asmens duomenų perdavimo Tretiesiems asmenims. Atskirais atvejais, kai to neįmanoma atlikti Įstaigos patalpose, sunaikinimas gali būti atliekamas kitoje fizinėje vietoje, tačiau tik stebint įgaliotam Įstaigos atstovui.

3.9. **Fizinė sauga**

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

(ii) Būtina naudoti aiškią visų Darbuotojų ir lankytojų identifikavimo sistemą, naudojant tinkamas priemones.

(iii) Patalpose įrengta signalizacija ir vaizdo kameros.

(iv) Prireikus turi būti kuriamos fizinės kliūtys, kad būtų užkirstas kelias neteisėtam fiziniam prieinamumui.

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

(vi) Išorės subjektų personalui, įgyvendinančiam teikiamas palaikymo paslaugas, turi būti suteikta ribota prieiga prie saugių zonų.

(vii) Darbuotojai privalo laikytis švaraus stalo principo.

(viii) Atspausdinti dokumentai nedelsiant, ne vėliau kaip per 3 min., turi būti paimti nuo spausdintuvo.
