

PATVIRTINTA
Vilniaus dailės akademijos
rektorius 2026 m. balandžio 24 d.
įsakymu Nr. VĮU-58-(2.2 E)
(Aktuali redakcija
Vilniaus dailės akademijos
Rektoriaus 2026 m. rugsėjo 21 d.
įsakymas Nr. VĮU-122-(2.2 E))

VILNIAUS DAILĖS AKADEMIJOS INFORMACIJOS SAUGOS POLITIKA

I SKYRIUS BENDROSIOS NUOSTATOS

1. Informacijos konfidencialumas, vientisumas ir prieinamumas yra esminės prielaidos ilgalaikiam Vilniaus dailės akademijos veiklos palaikymui bei teisiniam ir finansiniam organizacijos saugumui. Vilniaus dailės akademijos informacijos saugos politika (toliau – **Politika**) nustato pagrindinius Vilniaus dailės akademijos (toliau – **VDA, Akademija**) taikomus informacijos apsaugos principus ir jų įgyvendinimo tvarką Akademijos veikloje.
2. Informacijos saugumo valdymas VDA yra svarstomas ir tikslinamas pagal organizacinę struktūrą, funkcijas ir atsakomybę, veiklos strategiją ir tikslus, pajėgumus ir išteklius, informacijos sistemas ir procesus, bei sutartinius santykius.
3. Politikos tikslas – apibrėžti bendruosius informacijos saugos reikalavimus, kurie atitiktų VDA veiklos strategiją, poreikius, galiojančius teisės aktus, bei užtikrintų Akademijos informacinių išteklių apsaugą nuo vidinių ar išorinių tyčinių ar atsitiktinių grėsmių.
4. Politika privaloma visiems Akademijos darbuotojams ir informacinių technologijų paslaugų teikėjams.

II SKYRIUS SĄVOKOS

5. Atsakingas (-i) darbuotojas (-ai) – už VDA IT sistemų priežiūrą atsakingas (-i) darbuotojas (-ai) ir (ar) IT priežiūros paslaugas teikiantis išorinis paslaugos teikėjas.
6. Informacijos apdorojimo priemonės – priemonės skirtos duomenims apdoroti (rūšiuoti, sisteminti, analizuoti, atlikti skaičiavimus ir pan.).
7. Informaciniai ištekliai - duomenys, informacinės sistemos, informacinių technologijų platformos ir informacinių technologijų priemonės.
8. Informacijos saugos incidentas – pavienis įvykis arba tarpusavyje susiję įvykiai, kurių Akademija neplanavo ir neinicijavo, ir kurie turi arba, tikėtina, turės neigiamą poveikį informacinių išteklių vientisumui, prieinamumui, konfidencialumui ir (arba) autentiškumui.
9. Informacinė sistema – duomenų surinkimo, apdorojimo, perdavimo ir naudojimo sistema.

10. Informacinės sistemos savininkas – Akademijos darbuotojas, rektoriaus įsakymu paskirtas atsakingu už informacinės sistemos veiklos tikslus ir procesus bei tinkamo sistemos veikimo kontrolę.

11. Kompiuterinė įranga – kompiuterių technikos fizinių priemonių visuma, t. y. mechaniniai, magnetiniai, elektriniai, elektroniniai įrenginiai ir įtaisai. Kompiuterinei įrangai priskiriama ne tik kompiuteris, bet ir visi išoriniai įrenginiai bei ryšio priemonės: monitorius, klaviatūra, pelė, spausdintuvas, garsiakalbiai, maitinimo įtaisas, kabeliai, jungtys ir pan.

12. Konfidencialumas – užtikrinimas, kad informacija būtų prieinama tik įgaliotiems asmenims, turintiems prieigos prie informacinių sistemų teises.

13. Vientisumas – informacijos ir apdorojimo metodų tikslumo ir užbaigtumo užtikrinimas.

14. Prieinamumas – užtikrinimas, kad įgaliotieji vartotojai, kai būtina, turėtų prieigą prie informacinių ir bendrų išteklių.

15. Vartotojas (-ai) – kompiuterizuotos darbo vietos priemonės naudojantis (-ys) darbuotojas (-ai) ir / ar darbuotojas (-ai), kurie jungiasi prie IT sistemų vykdydami darbo funkcijas.

III SKYRIUS

INFORMACIJOS SAUGOS ORGANIZAVIMAS

16. Akademijos Rektorius ar jo įgaliotas asmuo formuoja Akademijos informacijos saugos politiką, organizuoja Akademijos informacijos saugą reglamentuojančių vidinių teisės aktų rengimą, užtikrina Akademijos informacijos saugumui gyvendinti reikalingų lėšų ir kitų priemonių suteikimą bei palaiko informacijos saugos kultūros diegimą Akademijoje.

17. Akademijos Informacijos saugos vadovo funkcijas atliekantis darbuotojas ar trečiosios šalies paslaugos teikėjas užtikrina Politikos nuostatų įgyvendinimo kontrolę, atlieka Politikos ir kitų informacijos saugą reglamentuojančių dokumentų (politikos, nuostatų, procedūrų ir kt.) savalaikį atnaujinimą ir pateikimą tvirtinti Akademijos rektoriui, koordinuoja saugumo incidentų valdymą bei analizę, teikia ataskaitas apie informacijos saugumo būklę Akademijoje, organizuoja Darbuotojų mokymus informacijos saugumo temomis, atlieka kitas su informacijos saugumu susijusias funkcijas.

18. Akademijos IT padalinio vadovas arba jo paskirtas IT specialistas užtikrina techninių informacijos saugumo kontrolės priemonių įgyvendinimą, valdymą ir priežiūrą (antivirusinę programinę įrangos priežiūrą, operacinės sistemos atnaujinimas, informacijos šifravimas, atsarginis kopijavimas ir informacinės sistemos atkūrimas incidento atveju ir kt.), užtikrina tinkamą ir savalaikę techninės ir programinės įrangos priežiūrą, naujinimą, atlieka kitas IT padalinio vadovui deleguotas funkcijas užtikrinant IT saugos priemonių funkcionavimą.

IV SKYRIUS

INFORMACIJOS KLASIFIKAVIMAS

19. Akademijoje informacijos klasifikavimui naudojamos šios kategorijos:

19.1. konfidenciali informacija – tai tokia Akademijos informacija, kuri turi vertę dėl to, kad jos nežino kiti asmenys, ir kurios atskleidimas ar pakeitimas padarytų didelę žalą Akademijai. Konfidencialia laikoma informacija apie Akademijos materialų ir nematerialų turtą, komercinė informacija apie Akademijos veikloje naudojamus išteklius, finansines operacijas, prisijungimo prie informacinių išteklių ir jų konfigūracijos duomenys, informacija apie Akademijos paslaugų gavėjus ir bendruomenės narius, kuri nėra viešai

prieinama. Taip pat konfidencialia informacija laikomi asmens duomenys, jei konkrečiu jų naudojimo atveju nėra nustatyta kitaip;

- 19.2. vidinio naudojimo informacija – tai tokia Akademijos informacija, kuri nėra priskirta viešai ar konfidencialiai informacijai, naudojama Akademijos veikloje ir darbuotojų darbo funkcijoms vykdyti ir kurios atskleidimas neturėtų neigiamo poveikio Akademijos veiklai, tačiau dėl savo pobūdžio ji nėra skirta platinti viešai;
- 19.3. vieša informacija – tai Akademijos informacija, kurios atskleidimas tretiesiems asmenims nedaro jokio neigiamo poveikio Akademijai, todėl ji gali būti laisvai platinama;
- 19.4. asmens duomenys – tai bet kokia informacija apie fizinį asmenį (duomenų subjektą), kurią žinant ar naudojant yra ar gali būti nustatyta jo tapatybė ir kurią tvarko Akademia ar Akademijos įgaliosios trečiosios šalys (duomenų tvarkytojai).

V SKYRIUS

BENDRI INFORMACIJOS SAUGOS REIKALAVIMAI

20. Žmogiškieji ištekliai:

- 20.1. Prieš įdarbinant Akademijoje yra vertinama kandidatuojančio asmens darbo istorija ir atitiktis keliams profesiniams reikalavimams, taip gali būti tikrinama jo reputacija, ir tai atliekama laikantis galiojančių įstatymų bei kitų teisės aktų, norminių aktų ir etikos reikalavimų.
- 20.2. Prieš suteikiant prieigą prie Akademijos informacinių išteklių, kiekvienas darbuotojas ir trečiasis asmuo turi būti supažindinamas su Politika ir kitais galiojančiais Akademijos teisės aktais, reglamentuojančiais informacijos saugumą. Darbuotojų supažindinimą su informacijos sauga reglamentuojančiais teisės aktais vykdo personalo administravimo funkciją atliekantis Akademijos darbuotojas arba kitas Rektoriaus įgalios asmuo.
- 20.3. Visi darbuotojai turi pasirašyti konfidencialumo sutartis arba konfidencialumo pasižadėjimus. Konfidencialumo sutartyse ar pasižadėjimuose turi būti nustatyta Darbuotojų atsakomybė už Akademijos konfidencialios ar neviešos informacijos atskleidimą.
- 20.4. Kiekvienas darbuotojas visus gautus slaptažodžius, kodus ir kitas identifikavimo priemones privalo saugoti paslapyje. Tais atvejais kai naudojama kelių faktorių autentifikacija, darbuotojas ar trečiasis asmuo privalo užtikrinti, kad šiam autentifikavimui naudojamos priemonės (pvz. telefonas ar el. paštas) netaptų prieinamos kitiems asmenims nesankcionuotai.
- 20.5. Sutartyse su paslaugų teikėjais turi būti numatytos konfidencialumo nuostatos, užtikrinančios trečiojo asmens atsakomybę už Akademijos konfidencialios ar neviešos informacijos atskleidimą.

21. Darbo procedūros ir darbuotojų pareigos:

- 21.1. Informacinės sistemos ir (ar) įrangos diegimo, konfigūravimo, administravimo dokumentacija turi būti saugoma centralizuotai, Akademijos naudojamoje dokumentų valdymo informacinėje sistemoje, ir prieinama tik informacinės sistemos ir (ar) įrangos administratoriams, priežiūros specialistams ir informacinės sistemos savininkui. Sistemos atkūrimo procedūra taip pat turi būti saugoma popieriniame formate, saugioje vietoje, prieinamoje tik tam teise turintiems asmenims (seife, trečiosios šalies saugyklose ir pan.).
- 21.2. Sudarytas ir nuolat atnaujinamas Akademijos informacijos apdorojimui ir kaupimui naudojamos programinės ir techninės įrangos sąrašas (informacinių išteklių registras, kurio forma tvirtinama kaip šios Politikos Priedas Nr. 2.)

- 21.3. Akademijos informacinių išteklių registras turi būti peržiūrimas ne rečiau kaip vieną kartą per pusmetį.
- 21.4. Darbuotojams suteikta darbui skirta Akademijos kompiuterinė įranga gali būti naudojama asmeniniams tikslams kiek tai neprieštarauja šios Politikos ir kitų teisės aktų nuostatoms, reglamentuojančioms informacijos saugumą.
- 21.5. Jeigu yra pagrįstų įtarimų, kad Darbuotojo veikloje buvo neteisėtos veiklos požymių, siekiant išsiaiškinti Akademijos konfidencialios, vidinio naudojimo informacijos ar asmens duomenų atskleidimo ir kitus atvejus, kai Akademijos informacijos saugumui, reputacijai ar teisėms kyla pavojus, IT padalinio vadovas ar įgaliotas asmuo gali atlikti darbuotojo atliekamų veiksmų, kompiuterinėje darbo vietoje bei Akademijos informacinėse sistemose saugomos informacijos patikrinimą, kuris atliekamas tik Akademijos rektoriaus įsakymu.
- 21.6. Akademijos darbuotojai privalo laikytis „švaraus stalo“ ir „švaraus ekrano“ taisyklių, t. y. pašalinams asmenims Akademijos informacija negali būti matoma darbuotojo kompiuterių monitoriuose, palikta spausdintuvuose, kopijavimo aparatuose ar daugiafunkciniuose įrenginiuose, bei ant darbo stalo be priežiūros. Atsitraukdamas nuo kompiuterinės darbo vietos darbuotojas turi aktyvuoti slaptažodžiu apsaugotą ekrano užsklandą, o baigus darbą nutraukti visas aktyvias Akademijos informacinių sistemų sesijas.
- 21.7. Darbuotojui neatliekant jokių veiksmų kompiuterinėje darbo vietoje ilgiau nei 5 minutes, kompiuterinės darbo vietos turi būti automatiškai užrakinamos (paleidžiama slaptažodžiu apsaugota ekrano užsklanda).
- 21.8. Visuose Akademijos informacijos kaupimui ir (ar) apdorojimui naudojamuose įrenginiuose (kompiuteriai, tarnybinės stotys, duomenų saugyklos, planšetės, išmanieji telefonai ir pan.) turi būti įdiegtos ir įjungtos standžiųjų diskų, atminčių, duomenų šifravimo (pvz., „Bitlocker“, „FileVault“) technologijos ir nuotolinio įrangos valdymo technologijos, užtikrinančios Akademijos informacijos apsaugą įrangos vagystės ar praradimo atveju.
- 21.9. Darbuotojams draudžiama naudoti asmeninius įrenginius Akademijos konfidencialios, vidinio naudojimo informacijos bei asmens duomenų apdorojimui ar saugojimui išskyrus numatytus atvejus, tokius kaip darbinio el. pašto paskyros peržiūrėjimas asmeniniame išmaniajame telefone.
- 21.10. Darbuotojai, paliekantys jiems Akademijos suteiktą įrangą be priežiūros turi užtikrinti jos fizinę apsaugą (pvz., naudoti specialias įrangos prirakinimui skirtas priemones, seifus, numatyti saugią vietą namuose ir kt.).
- 21.11. Įrangą išnešti iš Akademijos patalpų darbuotojams galima tik gavus Akademijos rektoriaus įsakymu įgalioto VDA darbuotojo leidimą. Leidimą gavęs darbuotojas visiškai atsako už išnešamos įrangos ir joje esančios informacijos saugumą.
- 21.12. Darbuotojas praradęs įrangą, nedelsiant, bet ne vėliau kaip per 24 valandas nuo įvykio, turi pranešti apie tai atsakingam už IT padalinio specialistui, o esant įtarimui dėl vagystės taip pat turi pranešti teisėsaugos institucijai apie galimai įvykdytą Akademijos įrangos vagystę.

VI SKYRIUS

KOMPIUTERINĖS ĮRANGOS APSAUGA

22. Kompiuterinės įrangos įsigijimas, instaliavimas ir naudojimas

- 22.1. Pagrindiniai kompiuterinės įrangos įsigijimai turi būti vykdomi pagal patvirtintas įsigijimo procedūras.

- 22.2. Darbuotojai, įgalioti priimti sprendimus dėl kompiuterinės įrangos nuomos ar pirkimo, turi užtikrinti, kad paslaugos ir (ar) techninė bei programinė įranga būtų perkama iš gerą reputaciją turinčių, patikimų įmonių ir atitiktų gerai žinomų standartų reikalavimus, taikomus perkamoms paslaugoms, techninei ir (ar) programinei įrangai. Esant poreikiui, turi būti sudaroma Akademijos poreikius ir reikalavimus atitinkanti paslaugų lygio sutartis (SLA).
- 22.3. Kompiuterinės įrangos instaliavimas gali būti vykdomas tik įgaliotų darbuotojų ar trečių šalių ir atitikti informacijos apsaugos politikas, tvarkas bei procedūras.
- 22.4. Įrangos priežiūros, perdavimo tarp Darbuotojų ir (ar) naikinimo veiksmai turi būti atliekami įgaliotų darbuotojų ar trečiųjų asmenų, turinčių reikiamą kvalifikaciją įrangos priežiūrai atlikti.
- 22.5. Tais atvejais, kai kompiuterinė įranga numatoma panaudoti kitiems tikslams nei buvo naudojama iki šiol, turi būti užtikrinamas jos elementų, kuriuose yra arba gali būti saugoma Akademijos konfidenciali, vidinio naudojimo informacija ar asmens duomenys, sunaikinimas arba saugus perrašymas pašalinant visą buvusią įrenginyje informaciją be galimybės ją atstatyti.
- 22.6. Nebereikalinga Akademijos įranga, kuri yra nurašoma, ar jos elementai, kuriuose yra arba gali būti saugoma Akademijos konfidenciali, vidinio naudojimo informacija ar asmens duomenys, turi būti saugiai sunaikinami arba saugiai perrašomi pašalinant visą buvusią įrenginyje informaciją be galimybės ją atstatyti.
- 22.7. Akademijai priklausančios įrangos remontas turi būti atliekamas tik kvalifikuotų specialistų, o įsigyjant remonto paslaugą iš trečiųjų asmenų, būtina užtikrinti Akademijos informacijos pašalinimą iš remontuotinos įrangos, iki jos perdavimo remonto paslaugos teikėjui. Už Akademijos informacijos pašalinimą atsako įgaliotas ir reikiamą kvalifikaciją turintis IT padalinio darbuotojas ar trečiosios šalies paslaugų teikėjai.
- 22.8. Sugedus kompiuterinei įrangai, būtina nedelsiant informuoti atsakingus VDA darbuotojus.
- 22.9. Informacija nešiojamuose kompiuteriuose, išmaniuosiuose telefonuose, planšetėse turi būti apsaugota slaptažodžiu, apsaugota nuo vagysčių, pametimo ar sugadinimo. Kelionės metu įranga turi būti transportuojama kaip rankinis bagažas.
- 23. Reikalavimai nepertraukiamam elektros maitinimui, spausdintuvams**
- 23.1. VDA sistemos ar jų komponentai turi būti aprūpinti nepertraukiamo energijos maitinimo šaltiniais.
- 23.2. Spausdinant konfidencialią informaciją į tinklo spausdintuvą, būtina užtikrinti informacijos saugumą spausdinimo metu ir po jo. Atspausdinti dokumentai su konfidencialia informacija negali būti palikti spausdintuve, spausdinęs darbuotojas turi juos iš karto paimti.
- 24. Reikalavimai mobiliajai įrangai**
- 24.1. Vartotojams draudžiama į išimamus įrašomus informacijos nešėjus (magnetiniai diskai, kompaktiniai diskai, atminties kortelės ir t.t.) įsirašyti Akademijos informaciją, kurioje yra asmens duomenų.
- 24.2. Visos nešiojamos kompiuterinės laikmenos (nešiojamieji kompiuteriai, nešiojami kietieji diskai, CD, DVD, USB atmintinės ir pan.) turi būti saugomos, naudojamos, perduodamos ir naikinamos atsižvelgiant į jose laikomos informacijos pobūdį.
- 24.3. Naikinant nešiojamas kompiuterines laikmenas, kuriose naudojami asmens duomenys, ir jų kategorijos turi būti sunaikinti taip, kad šių dokumentų nebūtų galima atkurti ar atpažinti jų turinio.

- 25. Kompiuterinės įrangos dokumentacija
- 25.1. Kompiuterinės įrangos dokumentacija turi būti savalaikiai atnaujinama, lengvai suprantama ir prieinama darbuotojams, atsakingiems už jos aptarnavimą ir priežiūrą.
- 25.2. Visa VDA kompiuterinė įranga turi būti inventorizuojama kartą per metus įgalioto darbuotojo (-ų).

VII SKYRIUS

PROGRAMINĖS ĮRANGOS APSAUGA

- 26. **Programinės įrangos įsigijimas ir instaliavimas**
- 26.1. VDA gali būti naudojama tik licencijuota programinė įranga.
- 26.2. Nelegalios ir neautorizuotos programinės įrangos naudojimas kontroliuojamas. Nustatyta nelegali programinė įranga yra šalinama.
- 26.3. Programinės įrangos diegimą ir atnaujinimą vykdo tik įgalioti ir kvalifikuoti specialistai.
- 26.4. Diegiant programinę įrangą, būtina pakeisti gamintojo ir/ar tiekėjo nustatytus slaptažodžius.
- 27. **Programinės įrangos bei informacinių sistemų priežiūra ir atnaujinimas**
- 27.1. Apie pastebėtas informacinių sistemų klaidas turi būti informuojami organizacijos ar asmenys, atsakingi už informacinės sistemos priežiūrą ir aptarnavimą.
- 27.2. Informacinių sistemų taisymas ir diegimas avariniais atvejais galimas tik informavus Rektorių ir IT padalinio vadovą. Diegimas vykdomas pagal iš anksto paruoštas ir patikrintas pakeitimų procedūras.
- 27.3. Realų duomenų naudojimas testavimui galimas tik tada, jei yra užtikrinamas reikalingas duomenų konfidencialumas ir integralumas.
- 27.4. Vartotojai turi būti reikiamai apmokyti dirbti su nauja informacine sistema.
- 27.5. Visos VDA sistemos/programos turi būti išsamiai ir suprantamai dokumentuotos. Sistemos/programos negali būti diegiamos be reikiamos dokumentacijos.

VIII SKYRIUS

INFORMACINIŲ SISTEMŲ APSAUGA

- 28. **Elektroninis paštas ir internetas**
- 28.1. Failų siuntimas iš interneto turi būti ypatingai kontroliuojamas, kad būtų išvengta piktavališkų programų ar netinkamos informacijos gavimo. Akademijoje nenaudojami nesaugiais laikomi duomenų perdavimo protokolai (pvz. telnet, POP3, FTP, SMBv1, TLS1.0, TLS1.1 ir t.t.).
- 28.2. Gaunami el. laiškai, laiškų turinys turi būti Vartotojų peržiūrėti su ypatingu atsargumu. Draudžiama atidarinėti laiškuose esančius failus, jei jie nėra patikrinti dėl virusų ir piktavališkų programų arba gauti nuo nežinomų asmenų.
- 28.3. VDA darbuotojai, administruojantys interneto prieigą, turi užtikrinti, kad VDA kompiuterinis tinklas būtų apsaugotas nuo piktavališkų įsiveržimų įdiegiant ugniasienę.
- 28.4. Elektroninio pašto sistemai apsaugoti turėtų būti įdiegta nepageidautinų elektroninių laiškų (angl. *spam*) gavimą ir siuntimą kontroliuojanti sistema.
- 28.5. Susirašinėjant darbo reikalais turi būti naudojamos tik oficialios VDA elektroninio pašto dėžutės.

28.6. VDA turi būti naudojamos priemonės, leidžiančios uždrausti ar apriboti darbuotojams naudoti tam tikras interneto sritis. Turėtų būti blokuojami nepageidaujamo turinio internetiniai puslapiai.

28.7. Bevielio interneto tinklo prieigai (Wi-Fi) VDA patalpose yra sukonfigūruotos stotelės, skirtos VDA darbuotojams. Bevielis interneto tinklas apsaugotas slaptažodžiu, kurį suteikia ir keičia Atsakingas (-i) darbuotojas (-ai).

29. Mobilaus ryšio įrenginių naudojimas

29.1. Mobilaus ryšio įrenginys VDA darbuotojams suteikiamas tik darbo funkcijoms vykdyti.

29.2. Jei mobilaus ryšio įrenginyje naudojamas elektroninis paštas, privaloma apriboti prieigą prie mobilaus įrenginio naudojant ekrano užraktą.

29.3. Konfidenciali informacija negali būti perduodama mobiliaisiais įrenginiais, visiškai neįsitikinus dėl informacijos gavėjo autentiškumo ir jo teisės gauti informaciją.

29.4. Konfidenciali informacija negali būti įrašinėjama į auto-atsakiklius / balso pašto sistemas.

30. Duomenų valdymas ir kontrolė

30.1. Duomenų apdorojimas ar keitimas nestandartinėmis priemonėmis gali būti naudojamas tik išskirtiniais (avariniais) atvejais ir pagal šiems atvejams numatytas procedūras.

30.2. Informaciją iš magnetinių diskų, kompaktinių diskų ar kitų nešiojamų informacijos laikmenų nuskaityti gali tik atitinkamas teises turintys darbuotojai.

30.3. Duomenų archyvavimas ar saugojimas turi būti vykdomas atsižvelgiant į teisinius, techninius reikalavimus bei VDA vidinius veiklos dokumentus.

30.4. Personaliniuose ir nešiojamuose kompiuteriuose esantys laikini failai turi būti periodiškai šalinami.

31. Rezervinis kopijavimas ir archyvavimas

31.1. Atsakingas (-i) darbuotojas (-ai) turi užtikrinti, kad informacinių sistemų rezervinio kopijavimo ir atstatymo procedūros yra paruoštos, vykdomos ir veikia korektiškai.

31.2. Svarbūs duomenys, esantys nešiojamuose kompiuteriuose, turi būti periodiškai kopijuojami. Vartotojas atsakingas už vykdomo rezervinio kopijavimo reguliarumą.

31.3. Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis.

31.4. Pilnos atsarginės duomenų kopijos daromos kas savaitę, pridedamosios atsarginės duomenų kopijos daromos kasdien.

31.5. Atsarginės kopijos turi būti saugomos ne trumpiau kaip 30 (trisdešimt) kalendorinių dienų, jeigu Lietuvos Respublikos teisės aktai ir (ar) VDA vidaus dokumentai nenustato ilgesnio saugojimo termino.

31.6. Atsarginės kopijos turi būti saugomos atskiroje laikmenoje ar saugykloje, fiziškai arba logiškai atskirtoje nuo pagrindinės informacinės sistemos infrastruktūros.

31.7. Jei naudojamos išorinės laikmenos, jos turi būti pažymėtos, registruojamos ir saugomos užrakintose patalpose arba seifuose, prie kurių prieiga suteikiama tik įgaliotiems darbuotojams.

31.8. Atsakingas (-i) darbuotojas (-ai) turi periodiškai tikrinti atsarginių kopijų tinkamumą atkūrimui, ne rečiau kaip kartą per metus atlikdamas bandomąjį duomenų atkūrimą.

31.9. Atsarginių kopijų kūrimo ir atkūrimo procesai turi būti dokumentuojami, fiksuojant kopijų sukūrimo datą, laikmeną, Atsakingą darbuotoją ir atliktus veiksmus. Duomenų

atkūrimo proceso registravimo forma patvirtinta šios Politikos Priede Nr. 1, o Atsarginių duomenų kopijų atkūrimo procedūra – Priede Nr. 3.

- 31.10. Atsarginės kopijos turi būti apsaugotos nuo neteisėto naudojimo, praradimo, sunaikinimo ar sugadinimo, naudojant technines ir organizacines saugos priemones.

32. Įvykių registravimas ir stebėseną

- 32.1. Akademijoje centralizuotai tvarkomi, saugomi ir peržiūrimi kritinių informacinių sistemų, kompiuterių, tarnybinių stočių, kompiuterių tinklo valdymo ir saugos sistemų vartotojų veiklos, trikčių ir informacijos saugumo įvykių žurnalai. Už stebėsenos priemonių administravimą, stebėsenos rezultatų vertinimą, periodinių ataskaitų peržiūrą ir reagavimo priemonių inicijavimą atsakingas Akademijos IT padalinio vadovas arba jo įgaliotas IT specialistas.
- 32.2. Akademijoje naudojamos techninių ir saugumo įvykių stebėsenos priemonės turi užtikrinti automatizuotą žurnalinių įrašų analizę, informacinių sistemų ir tinklo infrastruktūros būklės stebėseną, periodinių ataskaitų apie sistemų veikimą, saugumo įvykius ir nustatytas tendencijas rengimą bei atsakingų darbuotojų perspėjimą apie galimus informacijos saugumo pavojus, incidentus, neįprastą veiklą, nesankcionuotus veiksmus, kritinius sutrikimus ar kitus nustatytus saugumo rizikos požymius.
- 32.3. Akademijoje vykdoma nuolatinė kritinių informacinių sistemų, tarnybinių stočių, tinklo įrangos, saugumo priemonių ir kitų informacinių technologijų išteklių stebėseną. Stebimi duomenų srautai, sistemų prieinamumas, veikimo našumas, resursų (procesoriaus, operatyviosios atminties, duomenų saugyklų, tinklo pralaidumo ir kitų svarbių išteklių) naudojimas bei jų pokyčiai. Žurnalinių įrašų valdymo procedūra patvirtinta šios Politikos Priede Nr. 4.
- 32.4. Tvarkomi ir kaupiami įvykiai susiję su vartotojo nesėkmingais bandymais prisijungti, pranešimai apie sistemos klaidas, sistemos administratoriaus veiksmai ir kitų administratoriaus teisių panaudojimas, bandymai pakeisti įvykių žurnalo įrašus.
- 32.5. Informacinių sistemų, kompiuterių, tarnybinių stočių, kompiuterių tinklo valdymo ir apsaugos bei kitos įrangos prijungtos prie Akademijos vidinio kompiuterių tinklo, laikas sinchronizuojamas iš vieningų šaltinių. Darbuotojų kompiuteriuose ribojama galimybė keisti sistemos laiką.
- 32.6. Žurnaliniai įrašai kaupiami tam skirtoje tarnybinėje stotyje, kuri tinkamai apsaugota, nuo žurnalinių įrašų sunaikinimo, sugadinimo ar pakeitimo.
- 32.7. Stebėsenos rezultatų analizė atliekama reguliariai siekiant nustatyti pasikartojančius incidentus, pažeidžiamumus, nepakankamai veiksmingas saugumo priemones bei tobulinti Akademijos informacijos saugumo kontrolės priemones.
- 32.8. Žurnalinių įrašų duomenų analizė turi būti atliekama ne rečiau kaip kartą per mėnesį Akademijos IT padalinio vadovo arba jo įgalioto asmens. Analizės metu turi būti vertinami informacijos saugumo įvykiai, neįprasti naudotojų veiksmai, nesėkmingi prisijungimo bandymai, privilegijuotų paskyrų naudojimas, sistemų veikimo sutrikimai bei kiti galimi informacijos saugumo incidentų požymiai.
- 32.9. Nustačius reikšmingus nukrypimus nuo įprastų veikimo parametrų, neįprastą naudotojų elgesį, galimus kibernetinio saugumo incidentus ar kitus saugumo pažeidimų požymius, turi būti automatiškai arba nedelsiant informuojami Akademijos IT padalinio vadovas arba jo įgaliotas IT specialistas ir (arba) kiti Rektoriaus įsakymu už informacijos saugumą paskirti atsakingi asmenys ir, prireikus, inicijuojamas incidentų valdymo procesas.

32.10. Įvykių žurnaliniai įrašai saugomi netrumpiau kaip 3 mėnesius ir ne ilgiau kaip 12 mėnesių.

33. Incidentų valdymas

33.1. Esant informacinės sistemos sutrikimui, duomenų praradimui ar saugos incidentui, Atsakingas (-i) darbuotojas (-ai) turi nedelsdamas (-i) inicijuoti duomenų atkūrimo procedūrą:

33.1.1. nustačius informacinės sistemos sutrikimą, duomenų praradimą ar galimą saugos incidentą, darbuotojas nedelsdamas informuoja Atsakingą (-us) darbuotoją (-us);

33.1.2. Atsakingas (-i) darbuotojas (-ai) įvertina incidento pobūdį, nustato galimą duomenų praradimo mastą ir sprendžia dėl duomenų atkūrimo iš atsarginių kopijų poreikio;

33.1.3. prieš pradedant atkūrimo procesą nustatoma paskutinė tinkama atsarginė kopija, iš kurios gali būti atkuriami duomenys, ir įvertinama, ar kopija nėra pažeista ar užkrėsta kenkėjiška programine įranga;

33.1.4. jei būtina, informacinė sistema arba jos dalis laikinai sustabdoma, siekiant išvengti papildomo duomenų sugadinimo ar praradimo;

33.1.5. Atsakingas (-i) darbuotojas (-ai) atkuria duomenis iš pasirinktos atsarginės kopijos į testinę arba izoliuotą aplinką ir patikrina atkurtų duomenų vientisumą bei tinkamumą naudoti;

33.1.6. patvirtinus, kad atkurtų duomenų būklė yra tinkama, duomenys perkeliama į pagrindinę informacinės sistemos aplinką ir atkuriamas normalus sistemos veikimas;

33.1.7. po atkūrimo patikrinama, ar informacinė sistema veikia tinkamai, ar visi būtini duomenys yra prieinami Vartotojams ir ar nėra likusių veikimo sutrikimų;

33.1.8. duomenų atkūrimo procesas dokumentuojamas Duomenų atkūrimo proceso registravimo formoje (Priedas Nr. 1): užfiksuojama incidento data ir laikas, incidento aprašymas, atkurtos atsarginės kopijos data, atkūrimo pradžios data ir laikas, atkūrimo pabaigos data ir laikas, atlikti veiksmai, Atsakingas (-i) asmuo (-ys);

33.1.9. jei incidentas susijęs su informacijos saugos pažeidimu, apie jį informuojamas Rektorius ir (ar) kiti VDA atsakingi darbuotojai ir, jei taikoma, laikomasi VDA vidaus teisės aktuose ir (ar) dokumentuose nustatytos pranešimo kompetentingai (-oms) institucijai (-oms) (Valstybinė duomenų apsaugos inspekcija, Nacionalinis kibernetinio saugumo centras, policija, ir kt.) tvarkos.

34. Pakeitimų valdymas

34.1. Informacinių sistemų keitimas Akademijoje turi būti kontroliuojamas ir atliekamas vadovaujantis informacinių sistemų pokyčių valdymo procesu.

34.2. Informacinių sistemų keitimas Akademijoje turi būti kontroliuojamas ir atliekamas įgalioto ir reikiamą kvalifikaciją turinčio darbuotojo ar trečiosios šalies paslaugos teikėjo.

34.3. Jei Programinės įrangos, sistemos ar duomenų bazių kūrimą ar konfigūravimo darbus atlieka trečioji šalis, VDA atskiru susitarimu įpareigoja trečiąją šalį užtikrinti pakeitimų valdymo procesą tokiu būdu, jog kiekvienas pakeitimas būtų tinkamai inicijuojamas, priimtas, registruojamas, testuojamas ir įdiegiamas.

35. Popierinių dokumentų valdymas

35.1. Dokumentų su svarbia informacija savininkai turi užtikrinti reikiamą informacijos apsaugą dokumentų transportavimo metu.

- 35.2. Nereikalingos konfidencialių ar slaptų dokumentų kopijos turi būti sunaikintos dokumentų naikinimui pritaikytais smulkintuvais.
- 36. Apsauga nuo kenkėjiškų programų**
- 36.1. Visuose VDA kompiuteriuose (tame tarpe serveriuose ir nešiojamuose kompiuteriuose) turi veikti reguliariai atnaujinama antivirusinė programinė įranga.
- 36.2. Kompiuterinio viruso, kirmino ar kitos piktavališkos programos patekimas į VDA tinklą yra traktuojamas kaip labai pavojingas informacijos saugumo incidentas. Kiekvienu tokio incidento atveju turi būti siekiama nustatyti ir užkirsti piktavališkų programų patekimo į VDA tinklą keliai, turi būti ištirtas visas toks incidentas.
- 36.3. Antivirusinė programinė įranga turi veikti automatiškai, be vartotojo įsikišimo atsinaujinti kenkėjiškos programinės įrangos atpažinimo bibliotekas ir metodus.
- 36.4. Antivirusinė programinė įranga turi periodiškai, ne rečiau kaip vieną kartą per savaitę, nustatytu metu atlikti pilną kompiuterinės įrangos patikrą.
- 36.5. Antivirusinė programinė įranga taip pat turi atlikti pajungiamų išorinių duomenų laikmenų patikrą jų pajungimo metu.
- 37. Dirbtinio intelekto sistemų naudojimas**
- 37.1. Griežtai draudžiama naudoti bet kokią Akademijai nuosavybės teise priklausančią informaciją dirbtinio intelekto sprendimuose, neįvertinus rizikos ir negavus Rektorius pritarimo. VDA informacijos (pvz., konfidencialaus dokumento) pateikimas dirbtinio intelekto sprendimui, pavyzdžiui, "ChatGPT", „CoPilot“, „Gemini“ ir kt. gali lemti nepageidaujamą šios informacijos atskleidimą, tolesnį jos naudojimą kitose užklausoje ir analizėse, intelektinės nuosavybės ir praktinės patirties praradimą. Bet koks dirbtinio intelekto sistemų naudojimas turėtų būti atidžiai pasvertas rizikos požiūriu, užklausoje neturėtų būti Akademijos konfidencialių duomenų, asmens duomenų ir konkrečių faktinių aplinkybių.
- 37.2. Naudojant dirbtinio intelekto sistemas turėtų būti laikomasi galiojančių teisės aktų (pvz., ES dirbtinio intelekto akto) ir kitų taikytinų teisės aktų.
- 37.3. Leidimą dėl DI generuojamų rezultatų įtraukimo į Akademijos kuriamus sprendimus ar dokumentus turėtų suteikti Akademijos rektorius.

IX SKYRIUS

PRIEIGOS TEISIŲ SUTEIKIMO, PANAIKINIMO IR PAKEITIMO PROCEDŪRA

38. Prieiga prie visų VDA naudojamų informacinių sistemų, tinklų, duomenų bazių ar saugyklų internete yra draudžiama, išskyrus kai Vartotojams yra aiškiai suteiktos prieigos teisės.
39. Prieiga Vartotojui prie konkrečios informacinės sistemos suteikiama remiantis „būtinumo žinoti“ principu ir mažiausių privilegijų principu, t.y. suteikiamos tik minimalios prieigos teisės reikalingos vartotojo darbo funkcijoms atlikti.
40. Prieigos teisės suteikiamos ir Vartotojo paskyra informacinėse sistemose sukurama naudojant šiuos asmens duomenis: vardą, pavardę, el. pašto adresą, darbuotojo tabelio numerį, jungiantis el. parašu arba el. bankininkyste (jeigu taikoma). Naudojamų asmens duomenų apimtis atskirose naudojamose informacinėse sistemose gali skirtis.
41. Esant techninėms galimybėms Akademijos informacinių išteklių apsaugai turi būti naudojamos kelių faktorių autentifikavimo priemonės. Dviejų faktorių autentifikavimo sprendimas gali būti taikomas ir atskiroms sistemoms ar informaciniams ištekliams, jei jie turi tokias galimybes.

42. Vartotojams jungiantis pirmą kartą prie informacinės sistemos turi būti suteikiamas laikinas slaptažodis. Laikinam slaptažodžiui turi būti taikomas galiojimo laiko ribojimas.
43. Vartotojai privalo pasikeisti administratoriaus ar informacinės sistemos suteiktą pirminį ar laikiną slaptažodį pirmojo prisijungimo prie informacinės sistemos metu. Laikinam slaptažodžiui taikomi tokie patys minimalūs slaptažodžio sukūrimo reikalavimai.
44. Draudžiama naudoti gamyklinius programinės ar techninės įrangos slaptažodžius ir jie turi būti keičiami įrangos diegimo metu. Taip pat, esant galimybėms, turi būti keičiamas ir paskyros vardas.
45. Slaptažodžiai į internetu pasiekiamas sistemas vedami tik įsitikinus, kad naudojamas saugus perduodamų duomenų šifravimas (<https://>, ne žemesnės nei TLS1.2 versijos).
46. Paskyros prisijungimo duomenys yra konfidenciali informacija, kurie negali būti perduoti kitiems asmenims, tame tarpe ir kitiems Akademijos darbuotojams. Informacinės sistemos vartotojas negali naudoti kitiems asmenims suteiktų paskyrų prisijungimų ir slaptažodžių.
47. Kiekvienas vartotojas informacinėje sistemoje turi būti identifikuojamas unikalium prisijungimo vardu ar kodu. Asmens kodas negali būti naudojamas kaip vartotojo identifikatorius.
48. Kiekvienas vartotojas yra asmeniškai atsakingas už informacinėse sistemose atliktus veiksmus, naudojant jam suteiktus prisijungimo vardus ir slaptažodžius.
49. Sprendimas dėl prieigos teisių Akademijos informacinėse sistemose suteikimo darbuotojams, atsižvelgiant į jų darbines funkcijas, įforminamas Rektorius įsakymu. Prieigos teisių registrų funkciją atlieka informacinių sistemų vartotojų posistemės. Darbuotojams ir studentams suteiktos prieigos teisės gali būti registruojamos ir Akademijos žmogiškųjų išteklių valdymo informacinėje sistemoje (jei techniškai įmanoma).
50. Prieigos prie sistemų slaptažodžiai, keičiami ir saugomi užtikrinant jų konfidencialumą, turi būti unikalūs, nenaudojant asmeninio pobūdžio informacijos, keičiami susidarius tam tikroms aplinkybėms (pasikeitus Vartotojui (darbuotojui), iškilus įsilaužimo grėsmei, kilus įtarimui, kad slaptažodis tapo žinomas tretiesiems asmenims ir pan.) ir Vartotojo pirmojo prisijungimo metu. Vartotojas prieigos prie asmens duomenų slaptažodžiais turi naudotis asmeniškai ir neatskleisti jų tretiesiems asmenims.
51. 5 kartus iš eilės neteisingai suvedus paskyros prisijungimo duomenis (neteisingas prisijungimo vardas ir (ar) slaptažodis, kelių faktorių autentifikavimo sistemos klaida), informacinė sistema, esant techninėms galimybėms, turi automatiškai laikinai blokuoti vartotojo bandymus prisijungti ne trumpesniam nei 10 minučių laikotarpiui.
52. Vartotojas turi teisę susipažinti su VDA konfidencialia informacija tik tais atvejais, jeigu Vartotojui tokie įgaliojimai suteikti pagal darbo sutartį, pareigybės aprašymą ar tokius įgaliojimus konkrečiam darbuotojui suteikė Rektorius.
53. Vartotojai, kuriems VDA suteikė prieigą prie VDA naudojamų informacinių sistemų, privalo laikytis konfidencialumo principo ir laikyti paslapyje bet kokią su asmens duomenimis susijusią informaciją, su kuria jie susipažino vykdydami savo pareigas, nebent tokia informacija būtų vieša pagal galiojančių įstatymų ar kitų teisės aktų nuostatas.
54. Paskyros, kurios nenaudojamos ilgiau kaip 45 kalendorinės dienos, laikomos neaktyviomis ir jų naudojimas turi būti blokuojamas.
55. Paskyros, kurios buvo blokuotos ilgiau kaip 12 mėnesių laikomos nebenaudojamomis ir turi būti panaikintos.

56. Darbuotojams, studentams ir tretiesiems asmenims nėra suteikiamos informacinės sistemos, programinės ar techninės įrangos privilegijuoto vartotojo (administratoriaus) teisės. Privilegijuoto vartotojo teisės suteikiamos tik tiems darbuotojams, kurių funkcijoms atlikti jos yra būtinos.

57. Akademijos informacinių sistemų ar įrangos administravimo funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą turinčią reikiamas prieigos teises.

58. Privilegijuoto vartotojo paskyra negali būti naudojama kasdienėms darbuotojo funkcijoms atlikti (darbas su el. paštu, tekstinių redaktorių naudojimas, specializuotos programinės įrangos naudojimas ir pan.). Privilegijuoto vartotojo paskyra privalo būti apsaugota kelių faktorių autentifikavimo priemonėmis.

59. Pasikeitus privilegijuotas teises turinčios paskyros valdytojui, naujasis valdytojas turi nedelsiant pakeisti paskyros slaptažodį.

60. Akademijoje paskyrų valdymas yra centralizuotas.

61. Atsakingas (-i) darbuotojas (-ai) reguliariai, bet ne rečiau kaip kartą per 6 (šešis) mėnesius, peržiūri suteiktas prieigos prie VDA informacinių sistemų teises, ir, jei reikia, panaikina ar pakeičia suteiktas teises.

62. Pasibaigus darbo santykiams ar studijoms, Vartotojo prieigos teisės prie VDA naudojamų informacinių sistemų nedelsiant panaikinamos. Vartotojo tiesioginis vadovas privalo pranešti Atsakingam (-iems) darbuotojui (-ams) apie prieigos teisių panaikinimą ne vėliau kaip paskutinę Vartotojo darbo ar studijų dieną.

63. Kiekvienas Vartotojas, užregistruotas VDA naudojamoje informacinėje sistemoje, esant poreikiui gali būti priskiriamas Vartotojų grupei, pagal kurią nustatomos, kokios prieigos teisės suteikiamos konkrečiam Vartotojui. Grupės formuoja, prieigos teises suteikia arba panaikina Atsakingas (-i) darbuotojas (-ai).

X SKYRIUS

FIZINĖ APSAUGA

64. Patalpų apsauga

64.1. Tarnybinių stočių ir ryšio įrangos patalpos turi būti fiziškai atskirtos nuo kitos paskirties patalpų, apsaugotos nuo fizinių įsilaužimų, vagysčių, gaisro, potvynio, žaibo, komunalinių paslaugų (elektros tiekimo, vėdinimo ir kondicionavimo ir kt.) sutrikimų ir kitų rizikų bei turi atitikti įrangos veikimo aplinkos reikalavimus (pvz., oro temperatūros, drėgmės ir kt.).

64.2. Patekti į tarnybinių stočių ir (ar) ryšio įrangos patalpas gali tik tokia teisę turintys Darbuotojai ar įgalioti Tretieji asmenys ir tik savo darbo funkcijoms atlikti.

64.3. Visos tarnybinių stočių ir (ar) ryšio įrangos patalpos turi būti apsaugotos nuo neautorizuoto fizinio įėjimo. Priklausomai nuo patalpų svarbos turi būti naudojamos įvairaus sudėtingumo fizinės apsaugos technologijos.

64.4. Patalpos, svarbios informacijos saugos požiūriu, neturi būti žymimos, nurodant jų funkciją (pvz., tarnybinių stočių (serverių) patalpa, ryšių įrangos patalpa ir kt.).

64.5. Nesaugomose patalpose esantys nenaudojami kompiuterių tinklo kištukiniai lizdai turi būti atjungti nuo Akademijos kompiuterių tinklo ir jungiami tik tuo atveju, kai autorizuojama prieiga prie kompiuterių tinklo. Kompiuterių tinklo kabelius montuoti ir prižiūrėti gali tik kvalifikuoti ir įgalioti darbuotojai ar paslaugų teikėjai.

65. Švaraus stalo politika

65.1. Dokumentai ir išorinės duomenų laikmenos turi būti saugomi rakinamose spintose tuo metu, kai nėra naudojami, ypatingai nedarbo valandomis.

65.2. Konfidenciali informacija turi būti laikoma saugiai (pvz., rakinamose spintose ir pan.), nepaliekama spausdintuvuose po atspausdinimo.

XI SKYRIUS BAIGIAMOSIOS NUOSTATOS

66. Ši Politika įsigalioja nuo jos patvirtinimo datos.

67. Už Politikos laikymosi priežiūrą ir kontrolę, periodinį, ne rečiau kaip kartą per metus, arba dažniau pasikeitus aplinkybėms, atnaujinimą atsakingas Atsakingas (-i) asmuo (-ys).

68. Vartotojai pažeidę šioje Politikoje numatytus reikalavimus atsako Lietuvos Respublikos teisės aktuose nustatyta tvarka.

69. Su Politika visi Vartotojai (Akademijos darbuotojai) supažindinami darbinio el. pašto adresu arba per dokumentų valdymo sistemą. Aukščiau šiame Politikos punkte nurodytu būdu Politiką išsiuntus Vartotojui (darbuotojui) yra laikoma, kad su Politika Vartotojas (darbuotojas) yra supažindintas tinkamai.

70. Šios Politikos priedus sudaro „Duomenų atkūrimo proceso registravimo forma“ Priedas Nr. 1 „Informacinių išteklių registro forma“ Priedas Nr. 2, „Atsarginių duomenų kopijų atkūrimo procedūra“ Priedas Nr. 3 ir „Žurnalinių įrašų valdymo procedūra“ Priedas Nr. 4.

(Forma)

Duomenų atkūrimo proceso registravimas

Nr.	Incidento data ir laikas	Incidento aprašymas	Atkurtos atsarginės kopijos data	Atkūrimo pradžios data ir laikas	Atkūrimo pabaigos data ir laikas	Atlikti veiksmai	Atsakingas (-i) darbuotojas (-ai)

(Forma)

Informacinių išteklių registras

Sistemos ID	Sistemos pavadinimas	Vartotojų grupė	Prieigos tipas	Sistemos lokacija	IP arba URL adresas	Funkcija/Paskirtis/ Aprašymas	Tiekėjas (gamintojas)	IT palaikymo kontaktas	Pradžios data	Paskutinis atnaujinimas	Serverio lokacija	Asmens duomenys	Pastabos

ATSARGINIŲ DUOMENŲ KOPIJŲ ATKŪRIMO PROCEDŪRA

1. Tikslas

Vilniaus dailės akademijos Atsarginių duomenų kopijų atkūrimo procedūros (toliau – Procedūra) tikslas yra nustatyti atsarginių duomenų kopijų atkūrimo tvarką, užtikrinančią informacijos, informacinių sistemų ir paslaugų atkūrimą po techninių gedimų, kibernetinių incidentų, naudotojų klaidų, duomenų sugadinimo ar kitų incidentų.

2. Taikymo sritis

Procedūros taikymo objektai yra šie:

- 2.1. informacinės sistemos;
- 2.2. duomenų bazės;
- 2.3. tarnybinės stotys;
- 2.4. virtualios aplinkos;
- 2.5. debesijos paslaugos;
- 2.6. tarnybinėse stotyse saugomi duomenys;
- 2.7. kitos informacijos apdorojimo priemonės, kurioms kuriamos atsarginės kopijos.

3. Atsakomybės

- 3.1. IT padalinio vadovas tvirtina duomenų atkūrimo darbus, koordinuoja veiksmus didelės apimties sutrikimų atveju, priima sprendimus dėl prioritetų atkuriant sistemas.
- 3.2. IT administratorius arba kitas įgaliotas IT specialistas vykdo duomenų ir sistemų atkūrimo darbus, tikrina atkurtų duomenų vientisumą, dokumentuoja atkūrimo procesą, inicijuoja atsarginių kopijų testavimą.
- 3.3. Informacinių sistemų savininkai patvirtina atkurtų duomenų tinkamumą naudoti, įvertina atkūrimo rezultatų atitikimą veiklos poreikiams.

4. Atkūrimo inicijavimas

Atsarginių kopijų atkūrimas gali būti vykdomas šiais atvejais:

- 4.1. netyčia ištrynus duomenis;
- 4.2. sugadinus duomenis;
- 4.3. sutrikus informacinės sistemos veikimui;
- 4.4. įvykus techniniam gedimui;
- 4.5. įvykus kibernetiniam incidentui;
- 4.6. atkuriant veiklą po ekstremaliosios situacijos;
- 4.7. atliekant planinius atkūrimo bandymus.

5. Prašymo atlikti atkūrimą registravimas

- 5.1. Duomenų atkūrimo poreikis registruojamas pagal Akademijoje nustatytą informacijos saugos incidentų arba paslaugų užklausų valdymo tvarką.
- 5.2. Prašyme turi būti nurodyta atkurtinas objektas, duomenų vieta, pageidaujama atkūrimo data, incidento arba priežasties aprašymas, prašymo teikėjo duomenys (vardas, pavardė, pareigos, duomenys kontaktams).
- 5.3. Kritinių sistemų atkūrimo darbai gali būti inicijuojami nedelsiant, nelaukiant formalaus prašymo patvirtinimo.

6. Atkūrimo proceso vykdymas

- 6.1. **Pasirengimas atkūrimui.** Prieš atkuriant duomenis privaloma nustatyti įvykio, dėl kurio reikia atkurti duomenis, priežastį, įsitikinti, kad atkūrimas neperrašys svarbių aktualių duomenų, identifikuoti tinkamiausią atsarginę kopiją, įvertinti galimą poveikį veiklai.
- 6.2. **Atkūrimo veiksmai.** Atsakingas IT specialistas parenka tinkamą atsarginę kopiją, atkuria duomenis į gamybinę arba testinę aplinką, patikrina atkūrimo užbaigimą, užtikrina, kad atkūrimo metu nebūtų pažeistas duomenų vientisumas.
- 6.3. **Atkūrimo prioritetai.** Esant kelių sistemų sutrikimams šia prioritetine seka pirmiausia atkuriamos kritinės informacinės sistemos, autentifikavimo ir prieigos valdymo sistemos, duomenų bazės, tarnybinės stotys, kitos sistemos.

7. Atkūrimo rezultatų tikrinimas

Po atkūrimo turi būti atliekamas:

- 7.1. Techninis tikrinimas, kurio metu patikrinama, ar sistema paleidžiama be klaidų, ar prieinami visi reikalingi duomenys, ar veikia integracijos, ar nėra sugadintų failų.
- 7.2. Funkcinis tikrinimas, kurio metu sistemos savininkas arba paskirtas naudotojas patvirtina atkurtų duomenų išsamumą ir tikslumą, sistemos tinkamumą naudojimui.

8. Atkūrimo dokumentavimas

Kiekvienas atliktas atkūrimas registruojamas Akademijos Informacijos saugos politikos Priede Nr. 1 patvirtinto registro formoje. Atkūrimo įrašė nurodoma atkūrimo data ir laikas, atsakingas darbuotojas, atkurti duomenys arba sistema, naudotos atsarginės kopijos data, atkūrimo priežastis, atkūrimo trukmė, atkūrimo rezultatas, nustatytos problemos. Atkūrimo įrašų registras saugomas ne trumpiau kaip 2 metus.

9. Atsarginių kopijų atkūrimo testavimas

- 9.1. **Periodinis testavimas.** Atsarginių kopijų atkūrimo bandymai turi būti atliekami ne rečiau kaip kartą per metus.
- 9.2. **Kritinės sistemos.** Kritinėms sistemoms atkūrimo testai atliekami ne rečiau kaip kartą per 6 mėnesius.
- 9.3. Testavimo metu turi būti vertinama ar galima atkurti duomenis, ar laikmenose saugomos kopijos nėra pažeistos, atkūrimo trukmė, atkurtų duomenų vientisumas, nustatytų RTO ir RPO reikalavimų pasiekimas.
- 9.4. Testavimo rezultatai protokoluojami. Protokolai saugomi ne trumpiau nei 2 metus.

10. Neatitikčių valdymas

Jeigu bandymo arba realaus atkūrimo metu nustatoma, kad, atsarginė kopija sugadinta, duomenys neatkuriami, atkūrimo laikas viršija nustatytus rodiklius, neatkuriami visi reikalingi duomenys, už testavimo vykdymą atsakingas darbuotojas privalo registruoti neatitiktį, informuoti IT padalinio vadovą, kuris organizuoja korekcinius veiksmus ir prireikus atnaujiną atsarginių kopijų sudarymo tvarką.

11. Informacijos saugumas

- 11.1. Atsarginės kopijos ir jų laikmenos turi būti apsaugotos nuo neteisėtos prieigos.
- 11.2. Atkūrimo darbus gali atlikti tik įgalioti darbuotojai.
- 11.3. Atkūrimo metu naudojami duomenys turi būti tvarkomi laikantis konfidencialumo reikalavimų.
- 11.4. Atkuriant specialių kategorijų asmens duomenis turi būti užtikrinamos papildomos prieigos kontrolės priemonės.

12. Procedūros peržiūra

Procedūra peržiūrima ne rečiau kaip kartą per metus arba pasikeitus IT infrastruktūrai, arba pasikeitus atsarginių kopijų technologijoms, arba po reikšmingo incidento, arba nustačius procedūros trūkumus.

ŽURNALINIŲ ĮRAŠŲ VALDYMO PROCEDŪRA

1. Tikslas

Vilniaus dailės akademijos Žurnalinių įrašų valdymo procedūros (toliau – Procedūra) tikslas yra nustatyti žurnalinių įrašų rinkimo, saugojimo, apsaugos, peržiūros, analizės ir naudojimo tvarką, siekiant užtikrinti informacinių sistemų naudotojų veiksmų atsekamumą, aptikti ir tirti informacijos saugumo incidentus, identifikuoti neteisėtus, klaidingus ar neįprastus veiksmus, užtikrinti Akademijos informacinių išteklių saugumą, sudaryti sąlygas įrodyti atliktus veiksmus ir vykdyti atitikties reikalavimus.

2. Taikymo sritis

Procedūros taikymo objektai yra šie:

- 2.1. informacinės sistemos;
- 2.2. tarnybinės stotys;
- 2.3. darbo vietų kompiuteriai;
- 2.4. tinklo ir tinklo saugos įranga;
- 2.5. debesijos paslaugos;
- 2.6. duomenų bazių valdymo sistemos;
- 2.7. tapatybės ir prieigos valdymo sistemos;
- 2.8. kitos informacinių technologijų priemonės, kuriose tvarkomi arba saugomi Akademijos duomenys.

3. Atsakomybės

- 3.1. IT padalinio vadovas organizuoja žurnalinių įrašų valdymą, užtikrina techninių priemonių veikimą; skiria atsakingus asmenis žurnalų peržiūrai ir analizei; užtikrina nustatytų pažeidimų šalinimą.
- 3.2. Įgaliotas IT specialistas administruoja žurnalų kaupimo sprendimus, vykdo žurnalų stebėseną ir analizę, dokumentuoja analizės rezultatus, praneša IT skyriaus vadovui apie nustatytus incidentus.
- 3.3. Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis, ar kitas Rektoriaus įsakymu už informacijos saugumą paskirtas atsakingas asmuo vertina gautą informaciją apie nustatytus nuokrypius, priima sprendimus dėl incidentų tyrimo, inicijuoja reagavimo priemones. Jei Kibernetinio saugumo vadovas ir (ar) saugos įgaliotinis nepaskirtas, šias funkcijas atlieka IT padalinio vadovas.

4. Registruojami įvykiai

Žurnaluose turi būti registruojami ne mažiau kaip šie įvykiai:

- 4.1. **Prisijungimo įvykiai:** sėkmingi prisijungimai, nesėkmingi prisijungimai, paskyrų užblokavimai, slaptažodžių keitimai, kelių faktorių autentifikacijos nesėkmės.
- 4.2. **Prieigos valdymo įvykiai:** naudotojų teisių suteikimas, naudotojų teisių keitimas, naudotojų teisių panaikinimas, privilegijuotų teisių suteikimas.
- 4.3. **Administratorių veiksmai.** Registruojami visi sistemų administratorių veiksmai, įskaitant: naudotojų kūrimą, naudotojų šalinimą, saugumo parametrų keitimą, sisteminių nustatymų keitimą, duomenų eksportą, atsarginių kopijų atkūrimą.

4.4. **Sistemos įvykiai:** sistemos paleidimas, sistemos sustabdymas, avarinis išjungimas, sistemos klaidos, programinės įrangos gedimai.

4.5. **Saugumo įvykiai:** aptikti kenkėjiškos programinės įrangos atvejai, ugniasienių blokavimo įvykiai, IDS/IPS perspėjimai, bandymai pakeisti ar ištrinti žurnalinius įrašus, kiti galimi saugumo pažeidimai.

5. Registruojama informacija

Kai techniškai įmanoma, kiekviename žurnalo įrašė turi būti registruojama įvykio data ir laikas, naudotojo identifikatorius, darbo vieta arba IP adresas, įvykio tipas, atliktas veiksmas, veiksmo rezultatas (sėkmingas / nesėkmingas), sistema arba išteklius, kuriam veiksmas buvo atliktas.

6. Laiko sinchronizavimas

6.1. Visi įrenginiai ir informacinės sistemos privalo naudoti bendrą laiko šaltinį.

6.2. Darbuotojams turi būti draudžiama savarankiškai keisti darbo vietų sisteminių laiką.

6.3. Laiko sinchronizavimo paslauga turi būti reguliariai tikrinama.

7. Žurnalų apsauga

7.1. Žurnaliniai įrašai turi būti saugomi centralizuotai arba kitu būdu, užtikrinančiu jų vientisumą.

7.2. Turi būti užkirstas kelias neteisėtam žurnalų keitimui, trynimui, sugadinimui, nuslėpimui.

7.3. Prieiga prie žurnalinių įrašų suteikiama tik įgaliotiems asmenims.

7.4. Prieiga prie žurnalų turi būti registruojama.

8. Žurnalų saugojimo terminai

8.1. Žurnaliniai įrašai saugomi ne trumpiau kaip 3 mėnesius ir ne ilgiau kaip 12 mėnesių, jeigu teisės aktai nenustato ilgesnio saugojimo termino.

8.2. Incidento tyrimo atveju susiję žurnalai gali būti saugomi ilgiau iki tyrimo pabaigos.

9. Žurnalų peržiūra ir analizė

9.1. Žurnalinių įrašų duomenys turi būti peržiūrimi ir analizuojami ne rečiau kaip kartą per mėnesį.

9.2. Analizę vykdo IT padalinio vadovas arba jo įgaliotas asmuo.

9.3. Analizės metu vertinama: nesėkmingų prisijungimų statistika, privilegijuotų paskyrų naudojimas, administratorių atlikti veiksmai, neįprasti naudotojų veiksmai, sistemos klaidos, saugumo incidentų požymiai, bandymai keisti ar ištrinti žurnalus.

9.4. Analizės rezultatai dokumentuojami.

9.5. Nustačius reikšmingus nuokrypius, anomalijas, galimus informacijos saugumo incidentus ar kitus saugumo rizikos požymius, apie juos nedelsiant informuojamas IT padalinio vadovas apie tai nedelsiant informuoja Akademijos rektorių.

10. Stebėseną ir perspėjimai

10.1. Jei procedūros taikymo objektuose naudojamos automatinės stebėsenos priemonės, jos turi analizuoti žurnalinius įrašus, generuoti įspėjimus, rengti būklės ataskaitas, padėti identifikuoti galimus saugumo incidentus.

10.2. Akademijos kritinės svarbos informacinėse sistemose turi būti naudojamos automatizuotos stebėsenos priemonės, leidžiančios identifikuoti neįprastą veiklą realiuoju laiku.

11. Incidentų valdymas

11.1. Nustačius galimą saugumo incidentą incidentas registruojamas, išsaugomi susiję žurnalų įrašai, atliekamas incidento tyrimas, prireikus aktyvuojamos incidentų valdymo procedūros.

11.2. Žurnalu duomenys gali būti naudojami kaip įrodymai atliekant vidinius tyrimus ar teisės aktų numatytus veiksmus.

12. Kontrolė ir peržiūra

Ši Procedūra peržiūrima ne rečiau kaip kartą per metus arba pasikeitus teisės aktams, technologinei infrastruktūrai, įvykus reikšmingam informacijos saugumo incidentui ar nustačius procedūros trūkumus.
