Apstiprināts Jāzepa Vītola Latvijas Mūzikas akadēmijas
2020. gada 28. oktobrī Senāta sēdē, protokols nr. 5

Informācijas drošības politika

Izdota saskaņā ar
Valsts pārvaldes iekārtas likuma
72. panta pirmās daļas 1. punktu,
Informācijas tehnoloģiju drošības likuma 8. pantu un
2015.gada 28.jūlija Ministru kabineta noteikumiem nr. 442
"Kārtība, kādā tiek nodrošināta informācijas un
komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām"

1. Lietoto terminu definīcijas

Akadēmija - Jāzepa Vītola Latvijas Mūzikas akadēmija, Reģ.Nr.90000028796, Krišjāņa Barona iela 1, Rīga, LV-1050, kas nodarbina personas uz darba, uzņēmuma vai autoratlīdzības līguma pamata.

Tiešais vadītājs - Akadēmijas pārstāvis, kurš ir norādīts attiecīgā līgumā vai iecelts ar Akadēmijas rīkojumu kā Darbinieka tiešais vadītājs.

Darbinieks - Akadēmijā nodarbināta fiziska persona.

Vadība - Jebkura cita persona Akadēmijā, kurai piešķirtas vadības funkcijas un pilnvaras.
Politika - Šī Informācijas drošības politika.

Trešā puse - Fiziska persona, juridiska persona vai cita persona, kas nav saistīta ar Akadēmiju.

2. Mērķis un apjoms

2.1. Akadēmijas informācijas drošības sistēmas mērķis ir pasargāt Akadēmijas darbiniekus, sadarbības partnerus un studentus no nelikumīgām vai kaitējošām personu tiešām vai netiešām, apzinātām vai neapzinātām darbībām, apstrādājot informāciju un datus, kas nonāk attiecīgo personu rīcībā, kā arī lietojot noteiktu aprīkojumu savu darba pienākumu izpildes vajadzībām.

2.2. Politika regulē informācijas apstrādi jebkādās sistēmās vai jebkādos nesējos, kas iesaistīti datu/informācijas apstrādē Akadēmijā, neatkarīgi no tā, vai datu/informācijas apstrāde ir saistīta ar Akadēmijas iekšējām procedūrām, vai Akadēmijas ārējām attiecībām ar jebkādām trešajām pusēm.

2.3. Šī Politika regulē arī to, kā Akadēmijas Darbinieki lieto viņiem pieejamo aprīkojumu un rīkus, savu darba pienākumu veikšanas ietvaros.

2.4. Politika var būt piemērojama kopā ar jebkādām citām politikām, noteikumiem, procedūrām un/vai vadlīnijām, ko periodiski pieņem un ievieš Akadēmiju.

2.5. Par visiem informācijas drošības sistēmas jautājumiem, kas nav atrunāti šajā Politikā, jāvēršas pie IT daļas vadītāja.

2.6. Ar šiem noteikumiem ir rakstveidā jāiepazīstina visi darbinieki un jāpārliecinās, ka noteikumi ir pilnībā izprasti. Nepieciešamības gadījumā ir jāorganizē darbinieku apmācība vienotas un pareizas izpratnes radīšanai par IT un personas datu aizsardzības jautājumiem.

3. Informācijas klasifikācija

3.1. Jebkādus datus/informāciju, kas ir saistīta ar Akadēmijas studentu, darbinieku vai sadarbības partneru personas datiem, un, kas kļūst pieejama Darbiniekiem, veicot savus darba pienākumus, tiek uzskatīta par Akadēmijai piederošu un konfidenciālu informāciju, ko, līdz ar to, aizsargā atbilstoši piemērojamie normatīvie akti par personas datu aizsardzību.

3.2. Lai nodrošinātu pienācīgu informācijas un datu aizsardzību, Akadēmija veic iekšējo informācijas klasifikāciju. Datus/informāciju aizsargā neatkarīgi no tā, vai šāda informācija ir nonākusi Darbinieka rīcībā drukātu materiālu veidā, jebkādās datu uzglabāšanas ierīcēs, audio/video materiālu veidā vai jebkādā citā veidā.

3.3. Akadēmija lieto informācijas klasifikāciju, atbilstoši rektora rīkojumam par ierobežotas pieejamības informācijas statusa noteikšanu.

4. Datu/informācijas apstrādē iesaistītās sistēmas

4.1. Ikvienam Darbiniekam ir pienākums lietot šādu tehnisko aprīkojumu un rīkus ar pienācīgu rūpību un uzmanību un tikai ar Akadēmijas darbību saistītiem mērķiem. Vienīgais izņēmums ir gadījumi, kad Akadēmija ir piešķīrusi Darbiniekam tehnisko aprīkojumu (piemēram, mobilā tālruņa ierīci), sniedzot skaidru piekrišanu to lietot arī personīgām vajadzībām.

5. Darbinieku pienākumi

5.1. Jebkādi dati/informācija, kas nonāk Darbinieka rīcībā, pildot savus darba pienākumus, uzskatāma lietojama kā ierobežotas pieejamības informācija, ievērojot tās aizsardzību saskaņā ar šo Politiku, un datus/informāciju neizpauž nekādām trešajām pusēm, kamēr un ja vien Vadība nepaziņo, ka šāda informācija ir kļuvusi publiska vai ir kā citādi pārklasificēta par informāciju, kas vairs netiek aizsargāta šajā Politikā paredzētajā kārtībā.

5.2. Visus personas datus un citu informāciju, ar kuras palīdzību var identificēt fizisku personu, ievāc un apstrādā tikai, ja tas ir nepieciešams un ciktāl tas ir nepieciešams Darbinieka darba pienākumu veikšanas nolūkā, ar nosacījumu, ka šādas darbības tiek veiktas Darbiniekam piešķirto pilnvaru robežās un saskaņā ar likumā paredzētajām datu aizsardzības prasībām, jo īpaši, saskaņā ar **Vispārīgo datu aizsardzības regulu.**

5.3. Jebkādus datu pieprasījumus un/vai pieprasījumus par datu apstrādi, ko Darbinieks, veicot savus darba pienākumus, ir saņēmis no datu īpašniekiem – fiziskām personām, nekavējoties pārsūta turpmākai izskatīšanai Vadība un Datu aizsardzības speciālistam.

5.4. Ikvienam Darbiniekam ir pienākums ievērot šo Politiku, kā arī pildīt spēkā esošo vietējo, reģionālo vai starptautisko normatīvo aktu prasības, kas paredz datu/informācijas apstrādes un aizsardzības nosacījumus. Politikas neievērošanu uzskata par būtisku noteiktās darba kārtības pārkāpumu un tā rezultātā pēc Akadēmijas ieskatiem Darbiniekam var piemērot disciplinārsodu vai atlaist Darbinieku no darba. Tas tāpat var izraisīt arī pārkāpumu pieļāvušā Darbinieka saukšanu pie administratīvās vai kriminālās atbildības.

6. Piekļuves un aizsardzības pārvaldība

6.1. Darbinieki var piekļūt jebkādām Darbiniekiem pieejamām ierīcēm, ja tas nepieciešams attiecīgo Darbinieku darba pienākumu veikšanas vajadzībām, atbildības ietvaros un uz zinātvajadzības pamata. Piekļuves tiesības jebkādai sistēmai nenozīmē, ka Darbinieks ir pilnvarots apskatīt vai lietot visu attiecīgajā sistēmā esošo informāciju.

6.2. Izmantotie lietotāja ID ir unikāli un identificē konkrētu Darbinieku. Ikviens Darbinieks atbild par visām darbībām, kas saistītas ar viņa personīgo ID kontu, līdz ar to, primārais pienākums ir nodrošināt, lai Darbinieka ID nebūtu pieejams nekādām trešajām pusēm un pat ne citiem Darbiniekiem, ja vien Akadēmija nav noteikusi citu kārtību.

6.3. Sistēmas drošības paroles izveido ar pienācīgu rūpību, ar nosacījumu, ka tās nevar viegli atminēt. Tās sastāv vismaz no 9 simboliem (t.sk., lielajiem un mazajiem burtiem, cipariem, kā arī speciālajiem simboliem). Paroles neietver personas datus un tās tiek regulāri mainītas (vismaz reizi 3 (trīs) mēnešos). Ikviens Darbinieks personīgi atbild par savas drošības paroles atbilstību šai Politikai un jebkādiem citiem Akadēmijas noteikumiem.

6.4. Darbinieks piekļūst ierobežotas pieejamības informācijai, tikai tad, ja šādas pilnvaras ir paredzētas attiecīgā līgumā, vai tas izriet no Darbinieka amata pienākumiem.

7. Drošības pasākumi

7.1. Visiem jebkādā formā (drukātā, elektroniskā, u.tml.) ievāktiem un apstrādātiem datiem un informācijai piemērojamas šīs Politikas un jebkāda normatīvā regulējuma prasības attiecībā uz datu/informācijas ievākšanu, apstrādi, aizsardzību un uzglabāšanu, un šādus dokumentus uzglabā Akadēmijas norādītā, drošā vietā ar tādu uzglabāšanas termiņu, kādu paredz piemērojamie likumi un/vai norāda Akadēmija.

7.2. Darbiniekiem aizliegts glabāt jebkādu konfidenciālu informāciju savās ierīcēs, izņemot informāciju, kas ir īslaicīgi nepieciešama konkrētai, ar darbu saistītai darbībai. Visa nepieciešamā konfidenciālā un personīgi identificējamā informācija jāuzglabā tikai Akadēmijas IT personāla apstiprinātā mākoņa krātuvē un Akadēmijas iekštīklā. Ir jāizvairās no jebkādas šādu datu lejupielādēšanas vietējās ierīcēs un tas jādara tikai, ja tas ir pamatoti nepieciešams saistībā ar informācijas apstrādi darba vajadzībām.

7.3. Jebkurām mobilajām, portatīvajām ierīcēm (tostarp, klēpjdatoriem, planšetēm, viedtālruņiem un citām plaukstdatoru ierīcēm), kā arī jebkādām mākoņa informācijas uzglabāšanas vietām jābūt apstiprinātām no Akadēmijas IT personāla puses un pienācīgi aizsargātām, lai novērstu neautorizētu piekļuvi Akadēmijas datu bāzēm un uz serveriem esošajiem resursiem.

7.4. Akadēmijā lietotajā aprīkojumā un rīkos var instalēt un lietot tikai licencētas un autorizētas sistēmas un programmatūru. Pirms jebkādas programmatūras lejupielādēšanas vai instalēšanas Darbiniekiem piederošās un lietotās ierīcēs šajā Politikā aprakstītajiem mērķiem, ir jāsaņem IT personāla atļauja.

7.5. Gadījumos, kad Darbinieki lieto personīgās (mājas) ierīces, lai piekļūtu Akadēmijas korporatīvajiem resursiem (piemēram, elektroniskais pasts, tiešsaistes/mākoņa datubāzes), Darbiniekiem ir pienākums ievērot šīs Politikas prasības tieši tāpat kā, ja viņi lietotu Akadēmijas nodrošināto aprīkojumu.

7.6. Jebkurā gadījumā ir stingri aizliegts izmantot publiskas piekļuves ierīces (piemēram, interneta kafejnīcās, bibliotēkās, u.tml.), ja vien tas nav kritiski un steidzami nepieciešams saistībā ar darbu, un Darbinieka Tiešais vadītājs ir sniedzis skaidru rakstveida piekrišanu šādai darbībai.

7.7. Gadījumā, ja Darbiniekam tiek piešķirtas tiesības piekļūt Akadēmijas sadarbības partnera datņu glabāšanas sistēmai, Darbiniekam ir pienākums lietot piešķirtos piekļuves rīkus un ievērot sniegtos norādījumus par drošas datu/informācijas apstrādes prasībām (tostarp, šifrēšanas sistēma, paroļu lietošana, datu lietošanas ierobežojumi, īpaši paredzētu atrašanās vietu lietošana, u.tml.).

7.8. Tiklīdz, pēc Akadēmijas ieskatiem aizsargātie dati/informācija vairs nav nepieciešama Akadēmijas darbībai, šādus datus/informāciju dzēš, iznīcina visas to kopijas un attiecīgo datu /informācijas apstrādē iesaistītos Darbiniekus attiecīgi informē par viņu pienākumu dzēst/iznīcināt vai nodot atpakaļ Akadēmijai datus/informāciju, kas viņiem vairs nav nepieciešami savu darba pienākumu veikšanai, un, jo īpaši, atdot atpakaļ Akadēmijai, dzēst un iznīcināt datu/informācijas kopijas, ja ar attiecīgo Darbinieku tiek izbeigtas darba tiesiskās attiecības.

7.9. Nekādus šajā Politikā minētos datus/informāciju nenosūta, nepārsūta un nekādā citā veidā neiesniedz Trešajai pusei, ja vien tas nav nepieciešams Darbinieka darba pienākumu izpildei, un tikai tiktāl tas ir nepieciešams šādu pienākumu izpildei. Gadījumā, ja datus pārsūta vai iesniedz Trešajām pusēm, ir noteikti jānodrošina datu aizsardzība un jāveic visi atbilstošie drošības pasākumi.

7.10. Akadēmija auditē datu/informācijas apstrādē pielietotās sistēmas, lai kontrolētu nepārtrauktu atbilstību šai Politikai un piemērojamajām normatīvajām prasībām.

7.11. Atbildīgajam IT speciālistam ir jāveic informācijas sistēmu risku analīze (gan pirms šīs sistēmu ekspluatācijas sākšanas, gan regulāri - vismaz reizi gadā). Riska analīze ir jādokumentē.

7.12. Atbildīgajam IT speciālistam ir jānodrošina regulāra informācijas sistēmas notikumu reģistrēšana un monitorēšana.

8. Aizliegtās darbības

8.1. Izņemot īpaši paredzētus izņēmumus, nekādu Akadēmijai, tā studentiem vai sadarbības partneriem piederošu aprīkojumu, sistēmas vai rīkus nekādā gadījumā un nekādos apstākļos nedrīkst izmantot ar Darbinieka darba pienākumiem vai ar Akadēmijas darbību nesaistītiem mērķiem.

8.2. Turpmāk minētās darbības ir stingri aizliegtas, bez izņēmumiem:

a) Jebkuras personas ar intelektuālā īpašuma tiesībām aizsargātu tiesību pārkāpšana, tostarp, bet ne tikai, jebkādu nelegālu programmatūru, tiešsaistes platformu, jebkādu citu elektronisko saturu, kurus Akadēmija nav licencēta lietot, uzstādīšana, kopēšana, izplatīšana vai uzglabāšana jebkādās Akadēmijas sistēmās vai aprīkojumā.
b) Ar autortiesībām aizsargātu materiālu neautorizēta kopēšana.
c) Jebkuras personas tiesību aizskaršana, pārmērīgi un bez vajadzības ievācot un apstrādājot attiecīgā subjekta personas datus.
d) Piekļuve datiem, serverim vai kontam tādiem mērķiem, kas nav saistīti ar Akadēmijas darbību vai attiecīgā Darbinieka darba pienākumu veikšanu.
e) Programmatūras, tehniskās informācijas, šifrēšanas programmatūras vai tehnoloģijas eksportēšana, pārkāpjot piemērojamos starptautiskos vai nacionālos normatīvos aktus un/vai Akadēmijas norādījumus.
f) Jebkādu datu vai informācijas, kurai ir īpašuma un/vai konfidenciāla vērtība, eksportēšana, ja šāda eksportēšana nav nepieciešama Akadēmijas darbības vai Darbinieka darba pienākumu veikšanas gaitā, un/vai, ja tā pārkāpj Akadēmijas iekšējos noteikumus, piemērojamos normatīvos aktus.
g) Darbinieka konta paroles atklāšana citām personām un citu personu pielaišana lietot šādu kontu (tostarp, bet ne tikai, ar Darbinieka ģimenes locekļiem).
h) Krāpniecisku produkcijas, preču vai pakalpojumu piedāvājumu izveide, izmantojot Akadēmijas kontu.
i) Jebkādas programmas/skripta/komandas lietošana vai jebkāda veida ziņojuma nosūtīšana, ar nolūku ar jebkādiem līdzekļiem traucēt vai atspējot lietotāja darba sesiju.
j) Ar Akadēmiju saistītu e-pasta adrešu veidošana bez saskaņošanas ar IT nodaļu.

9. Rezerves kopijas un datu šifrēšana

9.1. Lietotāja līmeņa informācijai (piemēram, lietotāja ievadītie dati) Akadēmija veido regulāras rezerves kopijas.

9.2. Sistēmas līmeņa informācijai, tehnisko resursu konfigurācijai un Sistēmas dokumentācijai iestāde veido regulāras rezerves kopijas.

9.3. Rezerves kopijas tiek uzglabātas ģeogrāfiski attālinātā vietā.

9.4. IT departamenta vadītājs, nepieciešamības gadījumā piesaistot Informācijas resursu un Tehnisko resursu valdītāju, izstrādā rezerves kopiju izgatavošanas un Sistēmas atjaunošanas kārtību, kurā nosaka rezerves kopiju veikšanas biežumu, apjomu, uzglabāšanas kārtību.

9.5. Atbildīgais par Sistēmas drošības pārvaldību, nepieciešamības gadījumā piesaistot Informācijas resursu un Tehnisko resursu valdītāju, izstrādā pārsūtāmo personas datu šifrēšanas kārtību.

9.6. IT speciālists ne retāk kā reizi ceturksnī veic rezerves kopiju lasīšanas pārbaudi, kā arī pilnu Sistēmas informācijas atjaunošanas testu.

9.7. IT speciālists nodrošina rezerves kopiju aizsardzību pret neautorizētu piekļuvi.

10. Ziņošana par drošības incidentiem

10.1. Par visiem datu/informācijas apstrādes drošības incidentiem vai iespējamiem incidentiem nekavējoties ir jāziņo Vadībai, kura, attiecīgi, veic visus pasākumus iespējamā kaitējuma novēršanai, radītā kaitējuma seku likvidēšanai un iepriekšējā drošības stāvokļa atjaunošanai.

10.2. Akadēmijas Vadībai personas datu aizsardzības pārkāpuma gadījumā ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms, paziņo par personas datu aizsardzības pārkāpumu uzraudzības iestādei, izņemot gadījumus, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām.

10.3. Akadēmija dokumentē visus personas datu aizsardzības pārkāpumus, norādot faktus, kas saistīti ar personas datu pārkāpumu, tā sekas un veiktās koriģējošās darbības, kā arī veic nepieciešamās darbības atklāto trūkumu novēršanai, nepieciešamības gadījumā piesaistot ekspertus no Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas CERT.LV, modernizējot programmatūru, kā arī organizējot darbinieku apmācības IT jautājumos.

Senāta priekšsēdētājs profesors Normunds Vīksne