

Jelgavā

APSTIPRINĀTS
Jelgavas Mūzikas vidusskolas
direktors Artūrs Puķītis

2019. gada 23. augustā

Jelgavas Mūzikas vidusskolas Informācijas sistēmas drošības noteikumi

I. Vispārīgie jautājumi

1. Informācijas sistēmas drošības noteikumi ietver kārtību, kādā Jelgavas Mūzikas vidusskola (turpmāk – Iestāde) nodrošina Iestādē izmantotās informācijas sistēmas aizsardzību.

2. Noteikumos lietotie termini:

2.1. **Informācijas sistēma** – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta Iestādes izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.

2.2. **Jelgavas Mūzikas vidusskola** – iestāde, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.

2.3. **Informācijas sistēmas lietotājs** – persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.

2.4. **IT speciālists** – Iestādes vai ārpalpojuma darbinieki, kā arī Kultūras ministrijas Informācijas un tehnoloģiju atbalsta nodaļas speciālisti, kuri Iestādes normatīvajos aktos noteiktā kārtībā veic nepieciešamos datortehnikas apkalpošanas darbus. Ārpalpojuma gadījumā veicamo darbu apjomu un pienākumus nosaka ārpalpojuma sniedzēja līguma nosacījumi.

3. Informācijas sistēmas drošības noteikumi ir saistoši Informāciju sistēmu lietotājiem un IT speciālistam. IT speciālista funkcijas pilnībā vai daļēji var tikt nodotas ārpalpojumā. Ja tās tiek nodotas daļēji, tad Iestādei ir pienākums parūpēties par pārējo noteikumu ievērošanu citā veidā, piemēram, deleģējot šos pienākumus citam iekšējam darbiniekam. Nododot IT speciālista funkcijas ārpalpojumā, tiek nodotas arī atbilstošas pilnvaras.

II. Informācijas loģiskā aizsardzība

4. Iestādes datortīklu, datoru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu veic IT speciālists.

5. IT speciālists ir atbildīgs par piemērotu un efektīvu aizsardzības sistēmas izveidi, lietojot atbilstošu maršrutēšanas un ugunsdmūra sistēmu, kā arī nodrošinot pretvīrusu programmatūras

uzstādīšanu un uzturēšanu uz Iestādes datoriem. Darbstaciju konfigurēšana notiek automātiski, izmantojot speciāli šim nolūkam izstrādāto programnodrošinājumu, kuru darbību kontrolē IT speciālists.

6. IT speciālistam ir pienākums regulāri sekot līdzi ugunsdūmu paziņojumiem un reaģēt uz vīrusu uzbrukumiem, nodrošinot konstatēto vīrusu iznīcināšanu un būtisko incidentu reģistrēšanu.

7. Gadījumā, ja tiek konstatēti ielaušanās mēģinājumi vai būtiski incidenti, IT speciālists veic to reģistrēšanu un izmeklēšanu, kā arī par tās rezultātiem informē Drošības incidentu novēršanas institūciju (CERT.lv).

8. Vīrusu darbības novēršanai veic šādus pasākumus:

8.1. IT speciālists veic pasākumus datoru vīrusu darbības novēršanai tehniskajos resursos, izmantojot šim nolūkam paredzētu programmatūru;

8.2. IT speciālists veic antivīrusu programmu pārraudzību, lai pārliecinātos par to darbību un jaunāko vīrusu definīciju failu esamību.

9. Direktors ar rīkojumu norīko/anulē darbinieku tiesības konkrētajās informācijas sistēmās. Pēc minētā rīkojuma izdošanas, tiek nosūtīts direktora parakstīts pieprasījums attiecīgās informācijas sistēmu uzturētājam, par piekļuves tiesību piešķiršanu/anulēšanu darbiniekam. Nepieciešamības gadījumā IT speciālists izveido, veic izmaiņas un anulē Informācijas sistēmas lietotāju tiesības pēc direktora pieprasījuma. Minētais attiecas uz Iestādes piederošajām informācijas sistēmām.

10. Informācijas sistēmas lietotājiem, kuri ir Iestādes darbinieki, autorizēšanās rekvizītus (lietotājvārdu un paroli) izsniedz IT speciālists vai arī atbilstošās informācijas sistēmas pakalpojumu sniedzējs.

11. Nepieciešamības gadījumā Informācijas sistēmas lietotājiem, kuri nav Iestādes darbinieki, autorizēšanās rekvizītus (lietotājvārdu un paroli) izsniedz IT speciālists pēc direktora pieprasījuma.

12. Ja Informācijas sistēmas lietotājs, kas ir Iestādes darbinieks, ir aizmirsis savu lietotāja paroli, par to Informācijas sistēmas lietotājs personīgi vai telefoniski informē IT speciālistu vai ārpakalpojumu sniedzēju. IT speciālists vai ārpakalpojumu sniedzējs identificē atbilstošo informācijas sistēmas lietotāju, izveido jaunu paroli un izsniedz atbilstošajam Informācijas sistēmas lietotājam.

13. Paroles politika ir noteikta Iestādes Informācijas sistēmas lietošanas noteikumos.

14. Informācijas sistēmas lietotāja parole pie ievades nedrīkst parādīties uz ekrāna.

15. IT speciālists nodrošina auditācijas pierakstu veidošanu datortīkla autorizācijai un par informācijas sistēmām, kas ir izvietotas uz Iestādes resursiem vai kuras ir Iestādes īpašumā. Auditācijas pierakstos iekļauj visus veiksmīgus un neveiksmīgus pieslēgšanās gadījumus, to datumus un laiku, kā arī šo lietotāju (t.sk. administratora) vārdus vai citu autentifikācijas līdzekli. IT speciālists nodrošina auditācijas pierakstu integritāti un regulāri veido auditācijas pierakstu datu rezerves kopijas.

16. Ja Iestāde ievieš savas informācijas sistēmas, tā nodrošina, ka pirms jaunas sistēmas pieņemšanas ekspluatācijā tai ir veikti ielaušanās testi. Ielaušanās testus veic juridiska persona vai Iestādes darbinieki, kuri nav piedalījušies sistēmas izstrādē. Lielākā daļa Iestādē lietotās

informācijas sistēmas tiek instalētas automātiski ar Kultūras ministrijas ieviesto programmnodrošinājumu, kuru pieņemšanu un lēmumu par uzinstalēšanu pieņem ekspluatācijā augstāk stāvošā iestāde.

17. IT speciālists veic auditācijas pierakstu analīzi šādos gadījumos:

- 17.1. Informācijas sistēmas lietotāja atkārtota neveiksmīga pieslēgšanās informācijas sistēmai;
- 17.2. Informācijas sistēmas lietotāja pieslēgšanās informācijas sistēmai ārpus darba laika;
- 17.3. mēģinājumi piekļūt informācijas resursiem, kuriem IT speciālists nav pilnvarojis piekļūt;
- 17.4. atkārtoti mēģinājumi lietot lietotāja rekvizītus, kuri jau ir atcelti;
- 17.5. nesankcionētas programmatūras konfigurācijas maiņas un neatļautas programmatūras uzstādīšana.

18. IT speciālistam ir pienākums informēt Iestādes vadību un Kultūras ministrijas Informācijas un tehnoloģiju atbalsta nodaļu, konstatējot iespējamās problēmas ar Iestādē lietojamās programmatūras licencēm, kā arī to, ja tuvākā mēneša laikā tā beigsies un pēc nepieciešamības sniegt arī priekšlikumus un konsultācijas saistībā ar jaunas programmatūras iegādi.

19. Reģistru par iegādātiem un uzstādītiem informācijas tehniskajiem resursiem (t.sk. par darba stacijām, serveriem un perifērijas iekārtām) veic Iestādes grāmatvedība. Vismaz reizi gadā tiek veikta šo resursu inventarizācija, pārliecinoties, ka šis reģistrs ir korekts.

20. IT speciālists, tā pilnvarota persona vai ārējs konsultants nodrošina Iestādes Informācijas sistēmas lietotāju apmācību informācijas sistēmu drošības jomā, izskaidrojot tiem Informācijas sistēmas drošības politikas pamatprincipus un būtiskākos drošības pasākumus datu drošībai.

Iestādē tiek nodrošināta datortīkla / informācijas sistēmas atbilstība šādām aizsardzības prasībām:

- 21.1. iekšējo datortīklu nodala no interneta ar ugunsūra palīdzību;
- 21.2. ja tehniskais risinājums to pieļauj, nodrošina datortīkla / informācijas sistēmas pretvīrusa aizsardzību;
- 21.3. nodrošina nepārtrauktu datortīkla / informācijas sistēmas darba vides drošības apdraudējumu novēršanu, izmantojot ielaušanās mēģinājumu noteikšanu un aizsardzības sistēmu;
- 21.4. izmantojot tikai šifrētu pieslēgumu un ja iespējams, tad daudzfaktoru autentifikāciju, nodrošina attālinātas piekļuves ierobežošanu datortīkla / informācijas sistēmas administrēšanai;
- 21.5. sistēmu testēšanai organizē uz servera loģiskā vai fiziskā līmenī individuāli nodalītu testēšanas vidi;
- 21.6. piekļuvi datortīkla / informācijas sistēmas administrēšanas un pārvaldības funkcionalitātei nodrošina tikai tām personām, kurām datortīkla / informācijas sistēmas esošā informācija atbilstošā apmērā ir nepieciešama darba pienākumu veikšanai;
- 21.7. sistēmas lietotāji, kas veic sistēmas administrēšanas darbu, izmanto īpašus lietotāju kontus (piemēram, sistēmas administratora konts), kas netiek izmantoti ikdienas darbību veikšanai;
- 21.8. sistēmās vēlams nodrošināt, lai katrs lietotāja konts ir saistīts ar konkrētu fizisko personu. Ja sistēmā tiek izmantoti konti, kas nav piesaistāmi konkrētai fiziskai personai, tad sistēmā jābūt iestrādātiem tehniskiem līdzekļiem, kas novērš iespēju lietotājiem izmantot šādus kontus;

- 21.9. sistēmas lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī lietotāja autentifikācijas procesa ietvaros;
- 21.10. sistēmas lietotāja parole ievadīšanas brīdī lietotājam netiek pilnībā attēlota;
- 21.11. sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir lietojama vienu reizi un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas;
- 21.12. sistēmā nav pieļaujama funkcionalitāte, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;
- 21.13. iekārtām, tai skaitā infrastruktūras iekārtām, kas nodrošina sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles;
- 21.14. tiek nodrošināta sistēmas auditācijas pierakstu (turpmāk – sistēmas pieraksti) veidošana un uzglabāšana vismaz sešus mēnešus pēc ieraksta izdarīšanas;
- 21.15. jebkura piekļuve sistēmai ir izsekojama līdz konkrētam sistēmas lietotāja kontam vai interneta protokola (IP) adresei;
- 21.16. sistēmai jābūt uzliktiem visiem pieejamiem programmatūras atjauninājumiem, iepriekš izvērtējot to nepieciešamību;
- 21.17. visās Iestādes valdījumā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, jābūt iekļautai pretvīrusu funkcionalitātei;
- 21.18. sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamām tiesībām;
- 21.19. piecas secīgas reizes nepareizi ievadot sistēmas lietotāja konta paroli, šis konts (izņemot sistēmas administratora kontu) nekavējoties tiek bloķēts;
- 21.20. ar sistēmas administratora kontu piekļūt sistēmai, izmantojot iekārtas, kas atrodas ārpus Iestādes telpām, kā arī iekārtas, kas neatrodas Iestādes valdījumā, iespējams, tikai izmantojot daudzfaktoru autentifikāciju;
- 21.21. fiziski piekļūt iekārtām, kas nodrošina sistēmas darbību, atļauts vienīgi Iestādes pilnvarotām personām;
- 21.22. Iestādes iekšēji izstrādātajām sistēmām lietotājiem redzami kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai sistēmas lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību atrisinātu kļūdu;
- 21.23. plūsma starp sistēmu un tās lietotājiem, kā arī starp sistēmu un citām sistēmām tiek kontrolēta, piemēram, izmantojot ugunsūri;
- 21.24. datortīkla pakalpojumi, kas netiek izmantoti sistēmas darbības nodrošināšanai, ir atslēgti;
- 21.25. veicot sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu sistēmā glabāto datu integritātei;
- 21.26. sistēmas izvietošana ārpalpojuma sniedzēja nodrošinātos resursos atļauta tikai tad, ja pakalpojuma sniedzējs ir juridiska persona, kas reģistrēta Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, un sistēmā glabātā informācija atrodas vienīgi Eiropas Savienības vai Eiropas Ekonomikas zonas valstu teritorijā.

22. Iestāde nodrošina, ka vismaz reizi gadā tiek veikta informācijas tehnoloģiju drošības pārbaude (t.i. Iestādes izmantotās informācijas sistēmas drošības dokumentācijas un pasākumu atbilstības pārbaude) un atbilstoši tās rezultātiem tiek organizēta atklāto trūkumu novēršana.

23. Iestāde nodrošina, ka vismaz reizi gadā IT speciālists apmeklē Drošības incidentu novēršanas institūcijas organizētu apmācību informācijas tehnoloģiju drošības jautājumos.

24. Iestāde nodrošina, ka ne retāk kā reizi gadā tiek veikta institūcijas darbinieku instruktāžu informācijas tehnoloģiju drošības jautājumos.

III. Informācijas fiziskā aizsardzība

25. Informācijas sistēmu serveri, datortīkla un ar to saistīts aprīkojums tiek ekspluatēts ierobežotas pieejas telpās vai slēgtajos skapjos (turpmāk - serveru telpas), kuriem iespēja piekļūt ir tikai direktoram un IT speciālistam, nodrošinot aizsardzību pret neautorizētu personu iespēju serverus izslēgt, pārvietot, bojāt un nesankcionēti mainīt to konfigurāciju.

27. Nepiederošas personas, t.sk. ārpakalpojumu sniedzēji, serveru telpām drīkst piekļūt tikai direktora vai IT speciālista klātbūtnē.

28. Pazūdot elektrībai serveru telpās, IT speciālistam ir pienākums maksimāli īsā laikā novērst elektrības padeves traucējumus un nodrošināt pieslēgumu no cita enerģijas avota vai arī, ja tas nav iespējams un serveriem nav nodrošināta izslēgšanās automātiski, uzsākt manuālu serveru izslēgšanu.

29. Darbinieku datoriem jābūt uzstādītam nepārtrauktas barošanas avotam (UPS), ja Iestādes elektroenerģijas padeves traucējumu risks ir iespējams, lai elektrības noraustīšanās gadījumā dators neizslēgtos un attiecīgi datorā nesaglabātā informācija netiktu pazaudēta.

30. Datu nesēju (t.sk. CD, DVD, USB Flash, ārējais cietais disks vai tml.) fizisko aizsardzību nodrošina katrs Informācijas sistēmas lietotājs, nodrošinot, ka tie tiek glabāti drošās vietās, lai novērstu jebkādu nepilnvaroto personu piekļuvi.

IV. Ārpakalpojumu iesaiste

31. Ja Iestādes sistēmas uzturēšanai slēdz ārpakalpojuma līgumu ar pakalpojuma sniedzēju, līguma izpildi uzrauga atbildīgā persona un līgumā iekļauj vismaz šādas drošības prasības:

31.1. saņēmamā ārpakalpojuma aprakstu;

31.2. precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;

31.3. Iestādes un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā:

31.3.1. Iestādes tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi;

31.3.2. Iestādes tiesības iesniegt ārpakalpojuma sniedzējam pamatotu rakstisku pieprasījumu nekavējoties izbeigt ārpakalpojuma līgumu, ja Iestāde konstatējusi, ka ārpakalpojumu sniedzējs nepilda ārpakalpojuma līgumā noteiktās prasības attiecībā uz ārpakalpojuma apjomu vai kvalitāti;

31.3.3. ārpakalpojuma sniedzēja pienākumu nodrošināt Iestādei iespēju pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti;

31.4. iekļaujot pušu atbildību, atbilstoši jaunās datu regulas prasībām, nodrošinot, ka datu saņēmējs/uzglabātājs uzņemas pilnu atbildību par personu datu drošību un apstrādi;

31.5. nepieciešamās izmaiņas lietotāju kontos piesakāmas tikai caur vienu atbildīgo personu, šī persona tiek noteikta.

32. Ja Iestāde uzsāk iepirkumu par esošas ārpakalpojumu sistēmas uzlabojumiem vai iegādi, tas nodrošina, ka iepriekš minētās ārpakalpojumu iesaistes drošības prasības tiek iekļautas iepirkuma specifikācijā.

33. Ja Iestāde uzsāk iepirkumu par jaunas sistēmas izstrādi, tā iepirkuma specifikācijā iekļauj prasības, paredzot:

33.1. noteiktu sistēmas uzturēšanas un atbalsta nodrošināšanas (tai skaitā sistēmas drošības nepilnību novēršanas) laikposmu;

33.2. sistēmas datorprogrammu pirmkoda un tā izmantošanas tiesību nodošanu Iestādei ne vēlāk kā pēc noteiktā laikposma beigām, kā arī pēc katru izmaiņu vai uzlabojumu veikšanas tajā;

33.3. iespēju noteiktajā laikposmā turpināt sistēmas ekspluatēšanu ar sistēmas funkcionēšanai obligāti nepieciešamā programmnodrošinājuma (piemēram, operētājsistēma, datubāzu vadības sistēma, interpretators) jaunākām versijām.

V. Rezerves kopiju veidošanas kārtība

34. IT speciālists nodrošina Iestādes informācijas resursu rezerves kopiju veidošanu tām informācijas sistēmām / resursiem, kas ir izvietoti uz Iestādes serveriem / darba stacijām.

35. Rezerves kopiju ārējos datu nesējus glabā attālināti no oriģinālajiem datiem, lai novērstu oriģināla un kopijas vienlaicīgas bojāejas iespēju liela apjoma negadījuma situācijā.

36. IT speciālists nosaka vietu, kur tiks glabātas rezerves kopijas uz ārējā datu nesēja.

37. IT speciālists nodrošina Iestādes informācijas resursu atjaunošanu no rezerves kopijām.

38. IT speciālistam ir pienākums vismaz reizi gadā veikt pārbaudi par informācijas sistēmu atjaunošanas iespējām no rezerves kopijām.

VI. Elektronisko datu nesēju iznīcināšanas procedūra

39. Iestādes darbinieki datu nesējus, kuri satur fiziskas personas datus un kuri paredzēti iznīcināšanai, nogādā IT speciālistam. IT speciālists nodrošina minēto datu nesēju drošu iznīcināšanu šādā kārtībā:

39.1. CD, Blue Ray vai DVD matricas tiek iznīcinātas speciālā griezējā, sasmalcinot tos tā, ka nav iespējams atjaunot;

39.2. USB un SD atmiņu kartes atkārtotai lietošanai tiek pārrakstītas ar „0” un „1”, vai - ar defektiem - tiek fiziski iznīcinātas;

39.3. Datoru cietie diski (gan iekšējie, gan ārējie) tiek formatēti un pēc tam pārrakstīti ar „0” un „1” vai - ar defektiem - tiek fiziski iznīcināti.