Latvijas republikas Kultūras ministrija
Profesionālās izglītības kompetences centrs
"Ventspils mūzikas vidusskola"
Reģistrācijas Nr.3234303114
Lielais laukums 1, Ventspils, LV-3601
Tālrunis 63622220
elektroniskais pasts: ventspilsmv@inbox.lv, www.vmv@ventspils.lv

Ventspilī

APSTIPRINĀTS
Profesionālās izglītības kompetences centra
„Ventspils Mūzikas vidusskola"
direktors Andris Grigalis
_____
_____.gada _____.

Profesionālās izglītības kompetences centra „Ventspils Mūzikas vidusskola" Informācijas sistēmas drošības politika

I. Vispārīgie jautājumi

1. Informācijas sistēmas drošības politika nosaka politiku, kādā Profesionālās izglītības kompetences centrā „Ventspils Mūzikas vidusskola" (turpmāk – Iestāde) tiek nodrošināta izmantotās informācijas sistēmas aizsardzība pret ārējiem un iekšējiem riskiem un nodrošina informācijas sistēmas pieejamību, integritāti un konfidencialitāti saskaņā ar spēkā esošajiem normatīvajiem aktiem.

2. Informācijas sistēmas drošības politika attiecas uz Iestādes Informācijas sistēmas lietotājiem, kuriem ir pieeja kādai(-ām) no informāciju sistēmām.

3. Politikā lietotie termini:
   3.1. **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.
   3.2. **Profesionālās izglītības kompetences centrs „Ventspils Mūzikas vidusskola"** – Iestāde, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.
   3.3. **Informācijas sistēmas lietotājs** – persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.
   3.4. **IT speciālists** – Iestādes vai ārpakalpojuma darbinieks, kurš Iestādes normatīvajos aktos noteiktā kārtībā veic nepieciešamos datortehnikas apkalpošanas darbus. Ārpakalpojuma gadījumā veicamo darbu apjomu un pienākumus nosaka ārpakalpojuma sniedzēja līguma nosacījumi.

4. Informācijas sistēmas drošības politika ir izstrādāta saskaņā ar Informācijas tehnoloģiju drošības likumu, Valsts informācijas sistēmu likumu, Fizisko personu datu aizsardzības likumu, 2015.gada 28.jūlija MK noteikumu Nr.442 „Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8.punktu un citu LR normatīvo aktu prasībām, kā arī ievērojot Latvijas standartu LVS ISO/IEC 27001:2013" Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības".

II. Informācijas sistēmas drošības politikas mērķi un pamatnostādnes

5. Iestādes pienākums ir nodrošināt, lai to rīcībā esošā informācija tiktu apstrādāta, glabāta un pārvaldīta droši un pārbaudāmi, sniedzot tās darbiniekiem un lietotājiem skaidri noteiktas prasības informācijas sistēmas iekārtu un resursu izmantošanā, un nodrošinot Informācijas sistēmas aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem apdraudējumiem.

6. Informācijas sistēmas drošības politika attiecas uz visiem Iestādes Informācijas sistēmas lietotājiem, kuri veic darbības ar informācijas resursiem (piemēram, informācijas sistēmām, informāciju, kas tiek saņemta, apstrādāta, ievadīta, pārsūtīta vai uzglabāta) un tehniskajiem resursiem (piemēram, datoru sistēmām, datoru tīkliem), t.sk.:

6.1. pilna darba laika, nepilnas slodzes un līgumdarbiniekiem, kuri ir nodarbināti Iestādē;

6.2. lietotājiem, kuri ir noslēguši līgumu ar Iestādi par datu lietošanu vai kuri uz pieprasījuma pamata saņem datus no Iestādes izmantotām informācijas sistēmām;

6.3. ārpakalpojumu sniedzējiem vai konsultantiem, kuri strādā Iestādes labā.

7. Informācijas sistēmas lietotājs, kas ir nodarbināts Iestādē un ir Iestādes darbinieks (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), atbild par drošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šādos dokumentos:

7.1. Informācijas sistēmas drošības politikā;

7.2. Informācijas sistēmas lietošanas noteikumos.

8. Informācijas sistēmu lietotājs par iepazīšanos ar augstāk minētajiem dokumentiem un to ievērošanu paraksta 1.Pielikumu "Informācijas sistēmas lietotāja apliecinājums par "Informācijas sistēmas drošības politikas" prasību ievērošanu".

9. IT speciālists atbild par drošības politikas nosacījumu un prasību ievērošanu, kas ir minēti:

9.1. Informācijas sistēmas drošības politikā;

9.2. Informācijas sistēmas lietošanas noteikumos;

9.3. Informācijas sistēmas drošības noteikumos;

9.4. Informācijas sistēmas drošības riska pārvaldības plānā;

9.5. Informācijas sistēmu atjaunošanas plānā.

10. Iestādes direktors ir atbildīgs par viņa pakļautībā vai uzraudzībā esošajiem Informācijas sistēmas lietotājiem. Iestādes direktors nodrošina, ka personāls, uz kuru šī politika attiecas daļēji vai pilnā apmērā, ir informēts par politikas esamību un pilda savus darba pienākumus atbilstoši politikas nostādnēm.

11. Informācijas sistēmas drošība tiek nodrošināta šādu mērķu realizācijai:

11.1. nodrošinātu informācijas pieejamību;

11.2. nodrošinātu informācijas integritāti;

11.3. nodrošinātu informācijas konfidencialitāti;

11.4. aizsargātu sistēmas informācijas resursus;

11.5. aizsargātu sistēmas tehniskos resursus;

11.6. noteiktu sistēmas drošības apdraudējumu;

11.7. novērtētu sistēmas drošības risku;

11.8. atklātu sistēmas drošības incidentu;
11.9. atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.

12. Iestādē izmantotās informācijas sistēmām ir šādas drošības (pieejamības, integritātes un konfidencialitātes) klases:
12.1 C pieejamības klase - sistēmas nodrošinātā pakalpojuma neplānots pārtraukums sistēmas paredzētajā darba laikā drīkst būt ilgāks par 24 stundām mēnesī (summāri);
12.2. B integritātes klase - sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par 24 stundām (summāri) mēnesī, bet tas pieļaujams lielāks par četrām stundām (summāri) mēnesī;
12.3 A konfidencialitātes klase - sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par četrām stundām mēnesī (summāri), kā arī sistēmā tiek apstrādāti īpašās kategorijas (sensetīvi) personas dati vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde var radīt smagākas sekas nekā kaitējums Iestādes, citai Iestādei vai Latvijas Republikas reputācijai.

13. Iestādes būtiskākajās lietošanā esošajās informācijas sistēmās (Horizon, VIIS) tiek apstrādāti darbinieku un klientu personas dati.

14. Informācijas tehnoloģiju drošības pārvaldību un Informācijas sistēmas drošības politikas koordināciju Iestādē veic IT speciālists.

III. Informācijas sistēmas drošības organizācija

15. Informācijas sistēmas drošības organizatoriskās struktūras pamatu veido IT speciālists un Informācijas sistēmas lietotāji.

16. IT speciālists nodrošina informācijas sistēmas drošības politikas realizāciju, kā arī veic šādas darbības:
16.1. aktualizē drošības politiku, izstrādā ar informācijas sistēmas drošības saistīto iekšējo normatīvo aktu projektus un veic tās koordināciju;
16.2. aktualizē Informācijas sistēmas drošības politiku un to saistītos dokumentus vismaz vienu reizi gadā, kā arī šādos gadījumos:
16.2.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;
16.2.2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;
16.2.3. ja pēkšņi pieaug sistēmas drošības incidentu skaits vai ir noticis nozīmīgs sistēmas drošības incidents;
16.2.4. ja izmaiņas Iestādes organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju;
16.2.5. ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.
16.3. nodrošina informācijas sistēmās izmantojamās informācijas racionālu un pareizu izmantošanu;
16.4. izskata informācijas sistēmas lietotāju tiesību piešķiršanas un izmaiņu veikšanas pieteikumu autorizāciju saskaņā ar Informācijas sistēmas lietošanas noteikumiem;
16.5. piedalās Risku vadības procesā saskaņā ar Informācijas drošības riska pārvaldības plānu;
16.6. nodrošina atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši šīs politikas prasībām;
16.7. Iestādes direktors IT speciālista prombūtnes gadījumā ieceļ tā pienākumu aizvietotāju.

17. IT speciālista pienākums ir:

17.1. nodrošināt tehnisko resursu racionālu un pareizu izmantošanu;
17.2. nodrošināt tehnisko resursu fiziskās un loģiskās aizsardzības pasākumus saskaņā ar Informācijas sistēmas drošības noteikumiem;
17.3. veikt nepieciešamo tehnisko risinājumu uzstādīšanu un konfigurēšanu;
17.4. veikt Risku vadības procesa koordināciju Iestādē saskaņā ar Informācijas drošības riska pārvaldības plānu;
17.5. izmeklēt informācijas drošības incidentus;
17.6. veikt regulāras pārbaudes, lai pārliecinātos, ka tiek ievērotas Informācijas sistēmas drošības politikas un to saistošo dokumentu prasības;
17.7. nodrošināt informācijas sistēmas atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un informācijas sistēmas funkcionēšana traucēta vai neiespējama saskaņā ar Informācijas sistēmas drošības noteikumiem un Informācijas sistēmu atjaunošanas plānu;
17.8. nodrošināt atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši Informācijas sistēmas drošības politikas prasībām.

18. Informācijas sistēmas lietotāja pienākums ir racionāli un lietderīgi izmantot informācijas sistēmas un to datus sava darbu pienākumu veikšanai.

IV. Informācijas resursu klasifikācija

19. Visiem Iestādes informācijas resursiem (t.sk., darba stacijām, serveriem, perifērijas iekārtām, programmatūrai, Informācijas sistēmas datiem) ir jābūt uzskaitītiem un reģistrētiem, kā arī Informācijas sistēmas datiem ir jābūt klasificētiem.

20. Iestādes informācijas resursu klasificēšana tiek veikta atbilstoši Informācijas atklātības likumam un noteikta ar rīkojumu par ierobežotas pieejamības informācijas statusa noteikšanu.

V. Informācijas resursu riska analīze

21. Informācijas resursu riska analīzes mērķis ir nodrošināt atbilstošu Informācijas sistēmas vadību un kontroles sistēmas darbības efektivitāti, lai atklātu un novērstu kļūdas un nepreciziātes, un nepieciešamības gadījumā veiktu labojumus drošības sistēmā.

22. Iestādes informācijas resursu riska analīze tiek veikta atbilstoši Informācijas sistēmas drošības riska pārvaldības plānam.

VI. Informācijas resursu loģiskā drošība

23. Iestādes Informācijas sistēmas lietotājiem pieejas tiesību piešķiršana, izmainīšana un anulēšana tiek veikta atbilstoši Informācijas sistēmas lietošanas noteikumiem un Informācijas sistēmas drošības noteikumiem.

24. Informācijas sistēmas lietotāju pienākumi attiecībā uz informācijas resursu lietošanu, interneta izmantošanu un tehnisko resursu fizisko drošību ir iekļauti Informācijas sistēmas lietošanas noteikumos.

25. Iestādes datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu veic IT speciālists, kura pienākumi ir iekļauti Informācijas sistēmas drošības noteikumos.

VII. Tehnisko resursu fiziskā drošība

26. Iestādes datorsistēmas un tehnika (t.sk. datortīkli, programmatūra, informācijas sistēmas, serveri, datori) tiek aizsargāta ar piemērotu fizisko, tehnisko, organizatorisko un vides kontroļu kopumu.

27. Serveri un datori tiek novietoti aizslēgtās telpās, kurās pieeja ir tikai atbilstošām personām, nodrošinot fizisko aizsardzību no trešajām personām pret piekļūšanu šiem resursiem. Par serveru fizisko drošību Iestādē atbild IT speciālists, savukārt par atbilstošo datoru fizisko drošību atbild attiecīgais Informācijas sistēmas lietotājs.

28. Informācijas sistēmas lietotāju pienākumi attiecībā uz tehnisko resursu fizisko drošību ir iekļauti Informācijas sistēmas lietošanas noteikumos.

VIII. Darbības nepārtrauktības nodrošināšana

29. Iestādes informācijas sistēmām un elektroniskā veidā saglabātai informācijai regulāras rezerves kopijas veidošanu nodrošina IT speciālists atbilstoši Informācijas sistēmas drošības noteikumiem.

30. Katram Informācijas sistēmas lietotājam, kas ir nodarbināts Iestādē, ir jāveic un jānodrošina darbības nepārtrauktību tādā apjomā, kādā tā ir noteikta konkrētā darbinieka pienākumos un cik tas nepieciešams darbinieka tiešajiem darba pienākumiem.

31. Par visām avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaimes gadījumiem utt.) Informācijas sistēmas lietotājiem un IT speciālistam ir nekavējoties jāpaziņo Iestādes direktoram.

Pielikumā:

1. Profesionālās izglītības kompetences centra „Ventspils Mūzikas vidusskola" sistēmas lietotāja apliecinājums par "Informācijas sistēmas drošības politikas" prasību ievērošanu uz 1 lpp.