APSTIPRINĀTS
ar Murjāņu sporta ģimnāzijas direktora
24.09.2026. rīkojumu Nr. RV-31

MURJĀŅU SPORTA ĢIMNĀZIJA
INFORMĀCIJAS DROŠĪBAS POLITIKA

1. MĒRĶIS UN DARBĪBAS JOMA

1.1. Murjāņu sporta ģimnāzijas (turpmāk – MSĢ) Informācijas drošības politikas (turpmāk – Politika) mērķis ir aizsargāt iestādes informācijas aktīvus, informācijas sistēmas un tehnoloģiskos resursus pret jebkādiem iekšējiem vai ārējiem, tīšiem vai nejaušiem drošības apdraudējumiem.

1.2. Politika ir izstrādāta saskaņā ar Nacionālo kiberdrošības likumu, 2025. gada 25. jūnija Ministru kabineta noteikumiem Nr. 397 "Minimālās kiberdrošības prasības" (turpmāk – MK noteikumi Nr. 397), Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (Vispārīgā datu aizsardzības regula, turpmāk – GDPR) un Fizisko personu datu apstrādes likumu.

1.3. Šie noteikumi ir saistoši visiem MSĢ darbiniekiem, skolēniem, kuri izmanto MSĢ IKT resursus, un trešajām personām, kuras līgumattiecību ietvaros izmanto MSĢ IKT resursus vai ir piekļuve MSĢ apstrādātajai informācijai.

1.4. Politika attiecas uz visiem MSĢ īpašumā vai valdījumā esošajiem informācijas aktīviem, tīkliem, informācijas sistēmām un IKT ierīcēm neatkarīgi no to atrašanās vietas, kā arī uz privātajām ierīcēm, ja tās tiek izmantotas darba vajadzībām.

1.5. Politika ir MSĢ kiberdrošības pārvaldības dokumentu kopuma daļa. Uz Politikas pamata var tikt izstrādātas detalizētākas instrukcijas un procedūras (piemēram, incidentu vadības kārtība, rezerves kopiju atjaunošanas kārtība, piekļuves tiesību pārvaldības kārtība u.c.).

2. TERMINI

2.1. Politikā lietoti šādi termini:

- **IKT resursi** – MSĢ informācijas sistēmas, tīkli, datori, serveri, mobilās ierīces, datu nesēji, programmatūra un pakalpojumi, ko MSĢ izmanto darbā;
- **informācijas aktīvi** – jebkura MSĢ apstrādājamā informācija (elektroniskā vai papīra formā), kā arī sistēmas un resursi, kas to apstrādā;
- **kiberdrošības pārvaldnieks** – MSĢ direktora noteikta persona, kas atbild par kiberdrošības pārvaldību un normatīvo aktu prasību izpildi;
- **drošības incidents** – notikums, kas apdraud vai var apdraudēt informācijas aktīvu konfidencialitāti, integritāti vai pieejamību;
- **personas datu aizsardzības pārkāpums** – drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga personas datu iznīcināšana, zaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem;
- **privileģētais konts** – lietotāja konts ar paplašinātām (administratora) tiesībām.

3. ATBILDĪBA UN LOMAS

3.1. **MSĢ direktors** apstiprina Politiku, nodrošina tās izpildei nepieciešamos resursus un atbild par Politikas ievērošanas uzraudzību.

3.2. **Kiberdrošības pārvaldnieks** koordinē kiberdrošības pārvaldību MSĢ, atbild par atbilstību Nacionālā kiberdrošības likuma un MK noteikumu Nr. 397 prasībām, periodiski iesniedzamā pašvērtējuma ziņojuma sagatavošanu, sadarbību ar Nacionālo kiberdrošības centru un CERT.lv, kā arī par drošības incidentu ziņošanu.

3.3. **IT speciālists** atbild par IKT resursu tehnisko drošību, lietotāju kontu administrēšanu, datu dublēšanu un atjaunošanu, drošības atjauninājumu uzstādīšanu, drošības incidentu reģistrēšanu un neatliekamo pasākumu veikšanu.

3.4. **Datu aizsardzības speciālists** uzrauga personas datu apstrādes atbilstību GDPR un konsultē MSĢ datu aizsardzības jautājumos.

3.5. **Struktūrvienību vadītāji** nodrošina, ka viņu pakļautībā esošie darbinieki ievēro Politiku, un savlaicīgi informē IT speciālistu par izmaiņām darbinieku amatos, pienākumos vai darba tiesisko attiecību izbeigšanu.

3.6. **Katrs lietotājs** ir atbildīgs par Politikas ievērošanu, sava lietotāja konta un piešķirto IKT resursu drošu izmantošanu un par nekavējošu ziņošanu par drošības incidentiem.

4. RISKU PĀRVALDĪBA UN INFORMĀCIJAS KLASIFIKĀCIJA

4.1. MSĢ apzina informācijas aktīvus, informācijas sistēmas un IKT resursus un uztur to uzskaiti.

4.2. Kiberdrošības riskus novērtē ne retāk kā reizi gadā, kā arī pēc būtiskām izmaiņām IKT vidē, izvērtējot apdraudējumus, ievainojamības un iespējamo ietekmi uz izglītības procesu, skolēnu personas datu drošību un MSĢ darbību.

4.3. Informāciju klasificē pēc pieejamības ierobežojuma līmeņiem: vispārpieejama informācija; iekšējai lietošanai paredzēta informācija; ierobežotas pieejamības informācija (tostarp personas dati, īpašu kategoriju personas dati, piemēram, dati par skolēnu veselību, un informācija dienesta vajadzībām).

4.4. MSĢ nosaka informācijas sistēmu un datu kritiskumu, dublēšanas regularitāti, aizsardzības pasākumus un atjaunošanas prioritātes.

5. LIETOTĀJU PIEKĻUVES KONTROLE UN PAROĻU PRASĪBAS

5.1. Katram darbiniekam piekļuvei MSĢ informācijas sistēmām (e-pasts, e-klase, VIIS, VPS, darba aizsardzības, grāmatvedības sistēmām HoP un Horizon, Office 365, u.c.) tiek piešķirts individuāls lietotāja konts. Kopīgu vai universālu kontu izmantošana ikdienas darbā ir aizliegta.

5.2. Piekļuves tiesības piešķir atbilstoši amata pienākumiem, pēc principa "vajadzīgs zināt" un ar minimāli nepieciešamajām tiesībām, pamatojoties uz struktūrvienības vadītāja pieprasījumu. Piekļuves tiesību piešķiršanu un izmaiņas reģistrē.

5.3. Piekļuves tiesības atceļ vai groza darba tiesisko attiecību izbeigšanas, pārcelšanas citā amatā vai ilgstošas prombūtnes gadījumā ne vēlāk kā pēdējā darba dienā. Darbinieks nodod MSĢ piešķirtās IKT ierīces, datu nesējus un piekļuves līdzekļus.

5.4. IT speciālists ne retāk kā reizi gadā pārskata lietotāju un privileģēto kontu sarakstu un piekļuves tiesību atbilstību amata pienākumiem. Neizmantotus kontus bloķē.

5.5. Privileģētos kontus izmanto tikai administrēšanas uzdevumiem, tie ir atdalīti no ikdienas lietotāja konta un ir reģistrēti.

5.6. Daudzfaktoru autentifikāciju piemēro e-pastam, attālinātai piekļuvei, privileģētajiem kontiem un sistēmām, kurās tiek apstrādāta ierobežotas pieejamības informācija, ja sistēma to atbalsta.

5.7. Autentifikācijas parolēm ir jāatbilst šādām minimālajām drošības prasībām:

- minimālais garums: 12 zīmes;
- sastāvs: jāsatur lielie burti, mazie burti, cipari un speciālie simboli;
- mainīšanas biežums: nekavējoties, ja rodas aizdomas par paroles noplūdi, un ne retāk kā reizi 12 mēnešos;
- vienu paroli nedrīkst izmantot vairākās sistēmās, kā arī nedrīkst izmantot viegli uzminamas paroles (vārdus, dzimšanas datumus, vienkāršas secības);
- sākotnējo (uzņēmuma piešķirto) paroli maina pirmajā pieslēgšanās reizē.

5.8. Paroļu nodošana trešajām personām vai to uzglabāšana trešajām personām redzamā/pieejamā vietā ir stingri aizliegta.

6. IKT RESURSU LIETOŠANA UN TEHNISKĀ AIZSARDZĪBA

6.1. MSĢ IKT resursus izmanto darba pienākumu veikšanai. Personiska lietošana pieļaujama tikai tādā apjomā, kas neapdraud informācijas drošību un netraucē darba pienākumu izpildi.

6.2. Uz visām darba stacijām un serveriem tiek uzturēta pretvīrusu aizsardzība, savlaicīgi uzstādīti operētājsistēmas un programmatūras drošības atjauninājumi. Programmatūru, kurai vairs netiek nodrošināti drošības atjauninājumi, nelieto vai izolē no pārējā tīkla.

6.3. Programmatūru uzstāda tikai IT speciālists vai ar viņa atļauju.

6.4. MSĢ tīklā tiek nodrošināta tīkla aizsardzība (ugunsmūris), viesu un skolēnu bezvadu tīkli tiek nodalīti no administratīvā tīkla.

6.5. Nozīmīgu informācijas sistēmu un tīkla notikumu žurnālfailus glabā 6 mēnešus. Tie ir aizsargāti pret neatļautām izmaiņām un pieejami IT speciālistam un kiberdrošības pārvaldniekam.

6.6. Portatīvie datori un pārnēsājamie datu nesēji, kuros tiek glabāta ierobežotas pieejamības informācija, tiek šifrēti. Ierobežotas pieejamības informāciju elektroniski nosūta tikai drošos kanālos (šifrēts e-pasts vai drošs failu apmaiņas risinājums).

6.7. Privātās un mobilās ierīces darba vajadzībām drīkst izmantot tikai ar IT speciālista atļauju. Tām jābūt aizsargātām ar ekrāna bloķēšanu un atjauninātai programmatūrai. Ierobežotas pieejamības informāciju šādās ierīcēs bez šifrēšanas glabāt aizliegts. Ierīces zuduma gadījumā nekavējoties ziņo IT speciālistam.

6.8. Attālinātā darba laikā izmanto tikai aizsargātas ierīces un drošu savienojumu VPN vai IT speciālista uzstādītu līdzvērtīgu risinājumu. Publiskos bezvadu tīklus bez papildu aizsardzības darba vajadzībām nelieto.

6.9. Aizliegts atvērt aizdomīgas saites vai pielikumus, kā arī pārsūtīt darba informāciju uz privātiem e-pasta kontiem vai neapstiprinātiem mākoņpakalpojumiem.

6.10. Pārnēsājamos datu nesējus (USB u.c.) pirms lietošanas pārbauda ar pretvīrusu programmatūru. Pirms datu nesēju nodošanas citai personai vai utilizācijas datus neatgriezeniski dzēš vai nesēju fiziski iznīcina.

7. DATU DUBLĒŠANA (BACKUP) UN AIZSARDZĪBA

7.1. Par kritisko sistēmu un datu regulāru dublēšanu ir atbildīgs iestādes IT speciālists.

7.2. Rezerves kopiju veidošanas regularitāte tiek noteikta atbilstoši datu kritiskumam (piemēram, grāmatvedības un lietvedības datiem – katru darba dienu).

7.3. Ne retāk kā reizi gadā IT speciālists veic rezerves kopiju atjaunošanas testēšanu, lai pārliecinātos par datu integritāti un sistēmu atjaunojamību krīzes situācijā. Testēšanas rezultātus dokumentē.

7.4. Rezerves kopijas jāuzglabā fiziski vai loģiski izolēti no pamata tīkla (piemēram, bezsaistes vai nemaināmā veidā), lai pasargātu tās no izspiedējvīrusu uzbrukumiem. Rezerves kopijas, kas satur ierobežotas pieejamības informāciju, tiek šifrētas.

7.5. Katrai kritiskajai sistēmai nosaka mērķa atjaunošanas laiku (RTO) un pieļaujamo datu zudumu (RPO).

8. FIZISKĀ DROŠĪBA UN VIDEONOVĒROŠANA

8.1. Telpām, kurās atrodas MSĢ tīkla infrastruktūras mezgli vai serveri, jābūt pastāvīgi aizslēgtām. Piekļuve šīm telpām ir atļauta tikai IT speciālistam un pilnvarotām personām.

8.2. Videonovērošana skolas teritorijā tiek veikta likumīga mērķa (personu un mantas drošības nodrošināšana) sasniegšanai saskaņā ar GDPR un Fizisko personu datu apstrādes likumu. Videonovērošanas dati ir personas dati un uzskatāmi par ierobežotas pieejamības informāciju. Par videonovērošanu informē ar brīdinājuma zīmēm, kurās norādīta informācija par datu pārzini.

8.3. Piekļuve videonovērošanas arhīvam un vadības paneļiem tiek stingri kontrolēta un piešķirta tikai saskaņā ar direktora rīkojumu. Piekļuves gadījumus reģistrē.

8.4. Videoierakstus glabā ne ilgāk kā 30 dienas, ja tie nav nepieciešami konkrēta incidenta izmeklēšanai. Pēc termiņa beigām ierakstus dzēš.

8.5. Visiem darbiniekiem, atstājot darba vietu, ir pienākums bloķēt datora ekrānu (Windows taustiņš + L) un nodrošināt, ka sensitīvi dokumenti neatrodas uz galda trešajām personām redzamā veidā. Dokumentus ar ierobežotas pieejamības informāciju pēc darba glabā slēdzamā vietā, bet izdrukas no printeriem izņem nekavējoties.

8.6. Trešās personas telpās, kurās atrodas IKT resursi vai ierobežotas pieejamības informācija, uzturas MSĢ darbinieka pavadībā.

9. PERSONAS DATU AIZSARDZĪBA

9.1. MSĢ personas datus, tostarp skolēnu (nepilngadīgo) datus un īpašu kategoriju datus (piemēram, veselības datus), apstrādā tikai likumīga mērķa sasniegšanai, minimālā nepieciešamajā apjomā un atbilstoši GDPR un Fizisko personu datu apstrādes likumam.

9.2. Personas datu apstrādes darbības tiek dokumentētas datu apstrādes darbību reģistrā.

9.3. Personas datus glabā ne ilgāk, kā nepieciešams apstrādes mērķim, ņemot vērā MSĢ lietu nomenklatūru un normatīvajos aktos noteiktos glabāšanas termiņus.

9.4. Personas datu aizsardzības pārkāpuma gadījumā MSĢ bez nepamatotas kavēšanās un, ja iespējams, 72 stundu laikā pēc tam, kad par to kļuvis zināms, ziņo Datu valsts inspekcijai, ja vien pārkāpums neradīs risku fizisko personu tiesībām un brīvībām. Ja

pārkāpums var radīt augstu risku, MSĢ informē arī datu subjektus (GDPR 33. un 34. pants). Visus pārkāpumus dokumentē neatkarīgi no ziņošanas pienākuma.

10. ĀRPAKALPOJUMA SNIEDZĒJI UN TREŠĀS PERSONAS

10.1. Līgumos ar IKT pakalpojumu sniedzējiem (tostarp mākoņpakalpojumu un sistēmu uzturētājiem) iekļauj drošības prasības: konfidencialitāti, piekļuves kontroli, pienākumu bez kavēšanās paziņot MSĢ par drošības incidentiem, tiesības pārbaudīt drošības prasību izpildi un datu atgriešanu vai dzēšanu pēc līguma beigām.

10.2. Ja pakalpojumu sniedzējs apstrādā personas datus MSĢ vārdā, slēdz datu apstrādes līgumu atbilstoši GDPR 28. pantam.

10.3. Pirms ārpakalpojuma sniedzēja piesaistes, kas apstrādās ierobežotas pieejamības informāciju, izvērtē tā spēju nodrošināt atbilstošu drošības līmeni.

10.4. Trešo personu piekļuvi MSĢ IKT resursiem atļauj tikai ar direktora vai IT speciālista atļauju, uz noteiktu laiku, ar individuālu kontu un to reģistrējot.

11. DROŠĪBAS INCIDENTU VADĪBA UN ZIŅOŠANA

11.1. Par jebkuru aizdomīgu aktivitāti (piemēram, pēkšņiem sistēmas darbības traucējumiem, aizdomīgiem e-pastiem ar saitēm vai failiem, datortehnikas zudumu) darbiniekam ir nekavējoties jāziņo IT speciālistam. Darbinieks līdz IT speciālista norādījumiem neveic patstāvīgas darbības, kas var iznīcināt incidenta pierādījumus.

11.2. IT speciālists reģistrē incidentu MSĢ datu drošības incidentu reģistrā (datums un laiks, apraksts, ietekmētie resursi, veiktie pasākumi, cēloņi) un veic neatliekamos pasākumus tā seku likvidēšanai.

11.3. IT speciālists nekavējoties informē kiberdrošības pārvaldnieku un direktoru un incidentu klasificē atbilstoši MK noteikumos Nr. 397 noteiktajai klasifikācijai.

11.4. Būtisku IKT drošības incidentu gadījumā kiberdrošības pārvaldnieks sadarbībā ar vadību nodrošina ziņošanu valsts IT drošības incidentu novēršanas institūcijai CERT.lv un kompetentajai uzraudzības iestādei Nacionālajā kiberdrošības likumā un MK noteikumos Nr. 397 noteiktajos termiņos un formā, izmantojot noteikumu pielikumos iekļautās veidlapas.

11.5. Ja incidents ir arī personas datu aizsardzības pārkāpums, piemēro šīs Politikas 9.4. punktu.

11.6. Pēc katra būtiska incidenta veic tā cēloņu analīzi un, ja nepieciešams, uzlabo drošības pasākumus un šo Politiku.

12. DARBĪBAS NEPĀRTRAUKTĪBA UN ATJAUNOŠANA

12.1. MSĢ izstrādā un uztur kritisko informācijas sistēmu atjaunošanas plānu, kurā norāda atbildīgās personas, atjaunošanas prioritātes, mērķa atjaunošanas laikus (RTO) un pieļaujamo datu zudumu (RPO).

12.2. Atjaunošanas plānu pārbauda ne retāk kā reizi gadā kopā ar rezerves kopiju atjaunošanas testēšanu (7.3. punkts).

12.3. Ilgstoša informācijas sistēmu atteikuma gadījumā nodrošina kritisko procesu (piemēram, mācību procesa un skolēnu drošības nodrošināšanas) turpināšanu ar alternatīviem darba paņēmieniem.

13. APMĀCĪBA UN INFORMĒTĪBA

13.1. Ar Politiku iepazīstina katru darbinieku pirms piekļuves piešķiršanas MSĢ informācijas sistēmām. Iepazīšanos apliecina ar parakstu (Politikas pielikums).

13.2. Kiberhigiēnas un informācijas drošības apmācības darbiniekiem organizē ne retāk kā reizi gadā, tajās iekļaujot drošas paroles, pikšķerēšanas atpazīšanu, datu aizsardzības prasības un incidentu ziņošanas kārtību.

13.3. Kiberdrošības pārvaldnieka un IT speciālista kvalifikāciju uztur atbilstoši normatīvo aktu prasībām.

13.4. Skolēnus par drošu un atbildīgu IKT lietošanu informē izglītības procesa ietvaros.

14. ATBILDĪBA, PĀRSKATĪŠANA UN NOSLĒGUMA JAUTĀJUMI

14.1. Politikas neievērošana var būt pamats darba tiesiskai atbildībai saskaņā ar Darba likumu un MSĢ iekšējiem noteikumiem, kā arī citai normatīvajos aktos noteiktai atbildībai.

14.2. Politiku pārskata ne retāk kā reizi gadā, kā arī pēc būtiskiem drošības incidentiem, izmaiņām normatīvajos aktos vai MSĢ IKT vidē. Par pārskatīšanu atbild kiberdrošības pārvaldnieks.

14.3. Grozījumus Politikā apstiprina MSĢ direktors ar rīkojumu.

Direktors: _____ Sergejs Čevers

Datums:

Informācijas drošības politikas
pielikums

IEPAZĪŠANĀS LAPA

Ar MSĢ Informācijas drošības politiku esmu iepazinies/-usies un apņemos to ievērot.

Vārds, Uzvārds	Amats	Datums	Paraksts