UGNIAGESIŲ GELBĖTOJŲ MOKYKLOS
VIRŠININKAS

ĮSAKYMAS
DĖL UGNIAGESIŲ GELBĖTOJŲ MOKYKLOS INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKOS PATVIRTINIMO

2023 m. d. Nr. 4-
Vilnius

Vadovaudamasis Ugniagesių gelbėtojų mokyklos nuostatų, patvirtintų Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2003 m. balandžio 25 d. įsakymu Nr. 68 „Dėl Ugniagesių gelbėtojų mokyklos nuostatų patvirtinimo“, 36.1 ir 36.8 papunkčiais ir siekdamas užtikrinti efektyvų Ugniagesių gelbėtojų mokyklos informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą:

1. T v i r t i n u Ugniagesių gelbėtojų mokyklos informacijos ir kibernetinio saugumo politiką (pridedama).

2. N u r o d a u Ugniagesių gelbėtojų mokyklos Administracinio skyriaus vyresniajai specialistei Eglei Petrovskienei supažindinti su įsakymu Mokyklos darbuotojus.

Viršininkas
vidaus tarnybos pulkininkas Kęstutis Agintas

PATVIRTINTA
Ugniagesių gelbėtojų mokyklos
viršininko
2023 m. gegužės d. įsakymu Nr. 4-

UGNIAGESIŲ GELBĖTOJŲ MOKYKLOS INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKA

I. TIKSLAS

Informacijos ir kibernetinio saugumo politika (toliau – Politika) apibrėžia Ugniagesių gelbėtojų mokyklos (toliau – Mokykla) vadovybės poziciją ir atsakomybę informacijos ir kibernetinio saugumo srityje bei yra skirta pateikti vieningus saugumo valdymo principus bei užtikrinti efektyvų Mokyklos informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.

II. TAIKYMO SRITIS IR PRIORITETAI

Ši Politika privaloma Mokyklos vadovybei, visiems Mokyklos darbuotojams, kursantams, klausytojams, visoms suinteresuotoms šalims, įskaitant trečiųjų šalių darbuotojus. Politika taikoma kiekviename Mokyklos veiklos procese, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, nepriklausomai nuo jos formos ir saugojimo būdo.

Informacija laikoma prioritetiniu Mokyklos veiklos ištekliu, todėl elektroninės, rašytinės, žodinės informacijos saugumas yra esminis siekis, norint užtikrinti Mokyklos patikimumą, veiklos tęstinumą ir suinteresuotų šalių reikalavimų vykdymą.

III. PAGRINDINIAI TEISĖS AKTAI

Kibernetinio saugumo politikos tikslus, prioritetus ir jiems pasiekti būtinas priemones nustato Lietuvos Respublikos Vyriausybė, kibernetinio saugumo politika formuoja, jos įgyvendinimą organizuoja, kontroliuoja ir koordinuoja Lietuvos Respublikos krašto apsaugos ministerija, o kibernetinio saugumo politiką įgyvendina Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija ir kitos institucijos, kurių funkcijos yra susijusios su kibernetiniu saugumu.

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos – pagrindinė Lietuvos kibernetinio saugumo institucija, įgyvendinanti nacionalinę kibernetinio saugumo politiką (www.nksc.lt).

Pagrindiniai teisės aktai, kuriais vadovaujantis Mokykloje diegiamos organizacinės ir techninės duomenų saugumo priemonės:

Asmens duomenų teisinės apsaugos įstatymas
Baudžiamasis kodeksas
Elektroninių ryšių įstatymas
Valstybės informacinių išteklių valdymo įstatymas
Kibernetinio saugumo įstatymas
Administracinių nusižengimų kodeksas
Nutarimas dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo

IV. POLITIKOS UŽTIKRINIMO KRYPTYS

Pagrindinės informacijos ir kibernetinio saugumo Mokyklos užtikrinimo kryptys:

1. užtikrinti saugią ir patikimą informacinę ir kibernetinę Mokyklos aplinką;
2. užtikrinti informacijos saugumą – informacijos konfidencialumą, vientisumą ir prieinamumą;
3. užtikrinti veiklos tęstinumą – elektroninių ryšių tinklų, informacinių sistemų, techninės ir programinės įrangos nepertraukiamą veiklą, informacijos saugumo ir kibernetinių incidentų valdymą ir savalaikį veiklos atstatymą;
4. užtikrinti ir valdyti atitikimą, informacijos ir kibernetinį saugumą bei asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimams.

V. PAGRINDINIAI PRINCIPAI IR ĮSIPAREIGOJIMAI

Mokykla siekdama užtikrinti informacijos ir kibernetinį saugumą, nustato šiuos informacijos ir kibernetinio saugumo valdymo principus:

Padidintas dėmesys informacijos ir kibernetinio saugumo kultūros vystymui ir palaikymui.

Darbuotojai turi tinkamai suvokti informacijos ir saugumo svarbą, galimą neigiamą poveikį Mokyklos veiklai, keliamų strateginių tikslų įgyvendinimui. Nuolatos didinamas visų Mokyklos darbuotojų atsparumas kibernetinėms grėsmėms periodiškai organizuojant mokymus ar (arba) vykdant nuolatinę komunikaciją apie aktualias grėsmes ir priemones, leidžiančias išvengti incidentų.

Rizikos vertinimas ir valdymas.

Mokyklos svarbiausių veiklos procesų, informacijos ir kibernetinio saugumo grėsmių rizika vertinama atsiradus poreikiui (kuriant naujas ar keičiant esamas informacines sistemas ar veiklos procesus). Identifikuota rizika mažinama iki toleruojamo rizikos lygio.

Atitiktis.

Užtikrinti atitiktį teisės aktuose nustatytiems informacijos ir kibernetinio saugumo reikalavimams, Mokyklos sutartiniams įsipareigojimams su trečiosiomis šalimis, taikant rizikos vertinimu pagrįstas informacijos ir kibernetinio saugumo priemones.

Sistemingas ir nuoseklus incidentų ir pažeidžiamumų valdymas.

Valdant informacijos saugumo ir kibernetinius incidentus, užtikrinamas reikiamas reagavimas, suvaldymas ir mokymasis iš incidentų, siekiant išvengti jų pasikartojimo ar pažeidžiamumų išnaudojimo.

Siekdama įgyvendinti nustatytus informacijos ir kibernetinio saugumo valdymo principus, Mokykla įsipareigoja:

1. laikytis visų kibernetinio ir informacijos saugumo įsipareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartyse, prižiūrėti ir nuolat tobulinti informacijos saugumo valdymo sistemos efektyvumą;
2. skatinti ir propaguoti incidentų prevenciją užtikrinančias priemones bei vystyti Mokyklos darbuotojų informacijos saugumo kultūrą ir kibernetinę higieną (sąmoningumą);
3. užtikrinti efektyvų informacijos saugumo valdymo sistemos aprūpinimą reikiamais ištekliais, sudaryti sąlygas Mokyklos darbuotojams tobulinti žinias informacijos ir kibernetinio saugumo bei asmens duomenų saugumo srityse.

VI. TAIKOMOS PRIEMONĖS

Žmonių saugumo priemonės. Darbuotojų kompetencijai keliami reikalavimai nustatyti darbuotojų pareigybių aprašymuose. Darbuotojų atsakomybės, įgaliojimai ir įsipareigojimai nustatyti procesų aprašuose, tvarkose bei instrukcijose.

Fizinės saugumo priemonės apima patalpų (pvz., perimetro, įėjimo kontrolė, apsauga nuo išorinių grėsmių ir kt.) ir įrangos apsaugą nuo praradimo, sugadinimo ar vagystės. Vykdoma nuolatinė stebėsena.

Techninės priemonės: tinklo perimetro apsauga, techninės ir programinės įrangos saugus konfigūravimas, apsauga nuo kenksmingų priemonių, išorinio įsilaužimo prevencija, pažeidžiamumų vertinimas, elektroninio pašto ir naršyklės apsauga ir kt.

VII. ATSAKOMYBĖ

Bet koks informacijos saugumo normų pažeidimas laikomas informacijos saugumo incidentu, kuris gali daryti neigiamą įtaką Mokyklos veiklos tęstinumui, sugadinti ir pakenkti Mokyklos įvaizdžiui visuomenėje. Kiekvienas Mokyklos darbuotojas, pastebėjęs Mokyklos informacinių sistemų veiklos sutrikimą ar saugumo incidentą, kibernetinio saugumo spragą ar silpnąją vietą, nedelsiant privalo informuoti Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos Informacinių technologijų ir ryšių skyriaus specialistus el. paštu itrs@vpgt.lt.

Mokyklos darbuotojams ir trečiosioms šalims, pažeidusiems informacijos saugumo reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose, Mokyklos vidaus teisės aktuose bei sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose numatytos poveikio priemonės.

VIII. POLITIKOS PERŽIŪRA IR SKLAIDA

Politika tvirtinama, keičiama ar naikinama Mokyklos viršininko įsakymu. Politika yra skelbiama viešai Mokyklos interneto svetainėje ugm.lrv.lt ir prieinama visoms suinteresuotoms šalims. Šios Politikos nuostatos detalizuojamos ir įgyvendinamos priimant Mokyklos vidaus teisės aktus, derančius su Mokyklos strateginiais tikslais, teisiniais reikalavimais, tarptautiniais informacijos saugumo standartais ir gerosiomis praktikomis.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Ugniagesių gelbėtojų mokykla 111962021, Rolando Jankausko g. 2, LT-04310 Vilnius
Dokumento pavadinimas (antraštė)	DĖL UGNIAGESIŲ GELBĖTOJŲ MOKYKLOS INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKOS PATVIRTINIMO
Dokumento registracijos data ir numeris	2023-05-10 Nr. 4-51 (1.3 E)
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Kęstutis Agintas, Viršininkas
Sertifikatas išduotas	KĘSTUTIS AGINTAS LT
Parašo sukūrimo data ir laikas	2023-05-10 13:03:53 (GMT+03:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2023-05-10 13:03:58 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	RCSC IssuingCA, VI Registru centras - i.k. 124110246 LT
Sertifikato galiojimo laikas	2023-01-26 14:07:37 – 2025-01-25 14:07:37
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Eglė Petrovskienė, Vyresnysis specialistas, Administracinis skyrius
Sertifikatas išduotas	EGLĖ PETROVSKIENĖ LT
Parašo sukūrimo data ir laikas	2023-05-10 13:17:28 (GMT+03:00)
Parašo formatas	XAdES-EPES
Laiko žymoje nurodytas laikas	–
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2022-06-29 15:26:16 – 2027-06-28 23:59:59
Parašo paskirtis	Susipažinimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Žydrė Kaškevičiūtė, Vyriausiasis specialistas, Administracinis skyrius
Sertifikatas išduotas	ŽYDRĖ KAŠKEVIČIŪTĖ LT
Parašo sukūrimo data ir laikas	2023-05-10 13:24:51 (GMT+03:00)
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2023-05-10 13:25:06 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2022-08-04 18:00:18 – 2027-08-03 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	–
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	–
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	DBSIS, versija 3.5.72.2
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2023-05-10 14:20:38)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2023-05-10 14:20:39 DBSIS