PATVIRTINTA
Vilniaus Pranciškaus Skorinos
gimnazijos direktoriaus 2026 m.
sausio 28 d. įsakymu Nr. 23/V

VILNIAUS PRANCIŠKAUS SKORINOS GIMNAZIJOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šis informacinės sistemos veiklos tęstinumo valdymo planas (toliau tekste – **Planas**) parengtas įgyvendinant 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau tekste – **BDAR**), taip pat vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (toliau tekste – **ADTAĮ**), 2020 m. birželio 18 d. Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairėmis duomenų valdytojams ir duomenų tvarkytojams bei kitais asmens duomenų apsaugą reglamentuojančiais teisės aktais ir jų išaiškinimais.
2. Apraše naudojamos sąvokos:
2.1. **Įmonė –** Vilniaus Pranciškaus Skorinos gimnazija, įmonės kodas 191722390.
2.2. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius;
2.3. **Duomenų tvarkymas** – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas;
2.4. **IT specialistas** – asmuo, paskirtas atsakingu įmonėje už visus su informacinėmis technologijomis bei jų sauga susijusius klausimus;
2.5. **Duomenų apsaugos pareigūnas –** asmuo, įmonėje paskirtas atsakingu už duomenų apsaugą ir kurio statusą reglamentuoja BDAR 37-39 straipsniai;
2.6. **Elektroninė informacija** – informacinėje sistemoje tvarkomi duomenys, dokumentai ir informacija;
2.7. **Elektroninės informacijos sauga** – elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;
2.8. **Elektroninės informacijos saugos incidentas** – įvykis ar veiksmas, kurie gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti

galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti;

2.9. **Ekstremali situacija** – situacija, kuomet įmonėje įvyksta elektroninės informacijos saugos incidentas.

3. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos BDAR bei kituose asmens duomenų tvarkymą ir apsaugą reglamentuojančiuose teisės aktuose.

II SKYRIUS
PAGRINDINIAI INCIDENTŲ VALDYMO PRINCIPAI

4. *Informavimo* – įmonės darbuotojai privalo būti raštu supažindinami su šiuo Planu, jiems už mokymus atsakingas asmuo privalo pravesti instruktavimą, kaip reikėtų elgtis, jeigu įmonėje įvyktų elektroninės informacijos saugos incidentas.

5. *Konsultavimo* – kiekvienas įmonės darbuotojas turi turėti realią galimybę pasikonsultuoti su įmonėje atsakingu asmeniu už duomenų ar informacinių technologijų saugą.

6. *Gyvybės ir sveikatos užtikrinimo* – privalu užtikrinti visų įmonės darbuotojų sveikatą ir gyvybę, kol įmonėje trunka ekstremali situacija, iki būtų likviduojami jos padariniai.

7. *Informacinės sistemos veiklos atkūrimo* – kuomet įvyksta ekstremali situacija, pirmiausia privalu, kad būtų atkurtos svarbiausios informacinės sistemos funkcijos bei užtikrinama prieiga prie jų, taip pat, esant reikalui, organizuojama informacinės sistemos fizinė sauga.

III SKYRIUS
INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO PROCEDŪRŲ TIKSLAI

8. Pilnai panaikinti arba, jeigu neįmanoma panaikinti, sumažinti kiekvieno incidento padaromą žalą, Plane nusimatant organizacinius veiksmus, kurie padėtų tinkamai reaguoti į kiekvieną įvykusį incidentą.

9. Sustabdyti atitinkamą sistemos veiklą, jeigu tai yra būtina, kad būtų pašalintas elektroninės informacijos saugos incidentas, Plane nusimatant šio sustabdymo veiksmus.

10. Atlikti visus būtinuosius veiksmus, siekiant atstatyti informacinės sistemos veiklą per kuo įmanomą trumpesnį laiką, prireikus pasitelkti atitinkamų specialistų pagalbą, jeigu vienu ar kitu atveju būtų naudojamasi išorinių paslaugų teikėjų paslaugomis.

11. Siekiant sumažinti bet kokių galimų klaidų tikimybę, Plane aiškiai išdėstyti atsakingus asmenis už informacinės sistemos atkūrimą bei su tuo susijusius tolimesnius veiklos tęstinumo užtikrinimo procesus.

IV SKYRIUS
IT SPECIALISTO IR DUOMENŲ APSAUGOS PAREIGŪNO FUNKCIJOS

12. Įmonės IT specialistas, valdant incidentus, atlieka šias funkcijas:

12.1. koordinuoja elektroninės informacijos saugą incidento metu;

12.2. kontaktuoja su įmonės duomenų apsaugos pareigūnu bei, esant poreikiui, kitais įmonės darbuotojais, įskaitant įmonės direktorių, kuomet yra sprendžiamas elektroninės informacijos saugos incidentas;

12.3. prižiūri ir informuoja įmonės direktorių apie finansinius išteklius, kurių galėtų prireikti sprendžiant įvykusį elektroninės informacijos saugos incidentą;

12.4. vertina ir pasitaręs su įmonės direktoriumi nusprendžia kokiu būdu optimaliausia būtų išspręsti įvykusį elektroninės informacijos saugos incidentą;

12.5. pateikia pasiūlymus ir rekomendacijas įmonės direktoriui, kurie galėtų padėti išvengti tokio incidento nutikimo ateityje.

13. Įmonės duomenų apsaugos pareigūnas, valdant incidentus, atlieka šias funkcijas:

13.1. kontaktuoja su įmonės IT specialistu sprendžiant įvykusį elektroninės informacijos saugos incidentą, suteikia jam informacijos ar kitaip pagal esamą poreikį padeda jam spręsti nutikusį incidentą;

13.2. informuoja įmonės darbuotojus apie nutikusį incidentą (jeigu tam yra poreikis), nurodo kokių veiksmų reiktų imtis ar nuo kokių susilaikyti, kad incidentas būtų sustabdytas ar bent būtų sumažinta jo daroma žala;

13.3. esant poreikiui, koreguoja Planą, tokiu būdu darant prevenciją bei apsisaugant nuo incidentų nutikimo ateityje;

13.4. dokumentuoja visus įvykusius incidentus asmens duomenų saugumo pažeidimų registravimo žurnale.

V SKYRIUS
ORGANIZACINĖS NUOSTATOS

14. Įvykus elektroninės informacijos saugos incidentui, bet kuris įmonės darbuotojas jį pastebėjęs ar numanantis, kad toks įvyko, privalo nedelsdamas apie jį informuoti įmonės IT specialistą bei įmonės duomenų apsaugos pareigūną.

15. Jeigu elektroninės informacijos saugos incidentas įvyksta ne įmonės darbo laiku, tuomet tą pačią (jeigu kažkas pastebi) arba kitą dieną, įvykusį incidentą pastebėjęs darbuotojas, apie jį turi pranešti įmonės IT specialistui bei įmonės duomenų apsaugos pareigūnui.

16. Kiekvienas įmonės darbuotojas supranta, kad jeigu dėl jo kaltų veiksmų įvyksta elektroninės informacijos saugos incidentas, tai galėtų būti prielaida ateityje iš jo pareikalauti nuostolių atlyginimo.

17. Jeigu įmonės darbuotojas nepraneša apie įmonėje įvykusi elektroninės informacijos saugos incidentą ir dėl ko rezultate įmonė patiria žalos, tai vėlgi galėtų būti prielaida ateityje iš jo pareikalauti nuostolių atlyginimo (neteisėtas neveikimas).

18. Įmonės IT specialistas ar duomenų apsaugos pareigūnas, gavę informacijos apie įmonėje nutikusį elektroninės informacijos saugos incidentą ar patys jį pastebėję, privalo nedelsdami apie tai informuoti įmonės direktorių bei palaikyti su juo ryšį viso incidento sprendimo metu.

19. Po sužinojimo apie įvykusį elektroninės informacijos saugos incidentą, įmonės IT specialistas privalo nedelsdamas reaguoti ir informuoti įmonės duomenų apsaugos pareigūną kokių tolimesnių veiksmų bus imtasi ar kokių veiksmų reiktų vengti, nebent pagal Priede numatytą planą tai būtų duomenų apsaugos pareigūno kompetencija (tuomet jisai atlieka atitinkamus veiksmus bei informuoja ar konsultuojasi su IT specialistu, jeigu yra to poreikis), tai galėtų būti:

19.1. informacinės sistemos veikimo laikinas sustabdymas;

19.2. darbuotojų, dirbančių informacinės sistemos aplinkoje, visų ar dalies laikinas atjungimas, jų teisių sustabdymas naudotis sistema;

19.3. informacinės sistemos tarnybinių stočių veiklos atkūrimo organizavimas;

19.4. kompiuterių tinklo veikimo atkūrimo organizavimas;

19.5. informacinės sistemos taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

19.6. darbo kompiuterių veikimo atkūrimo ir prisijungimo prie kompiuterių tinklo organizavimas;

19.7. daiktų fizinės saugos organizavimas;

19.8. logistikos organizavimas (daiktų perkėlimas, žmonių pasikeitimas, kiti veiksmai);

19.9. kitos reikalingos priemonės.

20. Jeigu elektroninės informacijos saugos incidentas įvyksta dėl įvykdytos nusikalstamos veikos, tuomet įmonės duomenų apsaugos pareigūnas apie tokią nusikalstamą veiką privalo pranešti įmonės direktoriui. Įmonės direktorius priima sprendimą ar iš tiesų buvo įvykdyta nusikalstama veika įmonės atžvilgiu ir ar apie ją pranešti teisėsaugos institucijoms.

21. Bet kuriam veiksmui, kuriam yra reikalinga pasinaudoti įmonės finansiniais ištekliais siekiant išspręsti įvykusį elektroninės informacijos saugos incidentą, dėl šio finansavimo poreikio įmonės IT specialistas ir/arba duomenų apsaugos pareigūnas privalo informuoti įmonės direktorių. Įmonės direktorius priima sprendimą dėl lėšų skyrimo incidento sprendimui.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

22. Informacinės sistemos veikla yra laikoma atkurta tuomet, kai įmonės darbuotojai gali vėl atlikti savo pareigas, naudojantis šia sistema.
23. Įmonės darbuotojai, pažeidę Plano nuostatas, atsako įstatymų nustatyta tvarka.
24. Įmonės Planas turi būti peržiūrimas ne rečiau nei kartą per 2 metus arba dažniau, jeigu esama tokio poreikio.

PRIEDAI:

1. Incidentų valdymo būdai ir priemonės.

PATVIRTINTA
Vilniaus Pranciškaus Skorinos gimnazijos direktoriaus 2025 m. spalio 29 d. įsakymu Nr. 310/V

VILNIAUS PRANCIŠKAUS SKORINOS GIMNAZIJOS INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANO PRIEDAS NR. 1
INCIDENTŲ VALDYMO BŪDAI IR PRIEMONĖS

Nutikęs incidentas	**Priemonės**
Ryšio sutrikimas	1. Kritiškumo įvertinimas 2. Ryšio sutrikimo priežasties nustatymas 3. Kreipimasis į ryšio paslaugų teikėją ir pasiaiškinimas sutrikimo priežasčių, jeigu manoma, kad ryšys prarastas dėl paslaugų teikėjo kaltės 4. Peržiūrimos sistemos, įvertinama ar ryšio sutrikimams galėjo turėti įtakos virusai ar kitos priežastys 5. Situacijos analizė ir priemonių nustatymas, kad panašios situacijos nepasikartotų ateityje
Programinės įrangos gedimai	1. Kritiškumo įvertinimas 2. Atstatymas programinės įrangos iš turimų kopijų arba įsigijimas naujos, jeigu nustatoma, kad ji buvo sugadinta nepataisomai 3. Situacijos analizė ir priemonių nustatymas, kad panašios situacijos nepasikartotų ateityje
Elektros tiekimo sutrikimas	1. Kritiškumo įvertinimas 2. Kreipimasis į elektros paslaugų tiekėją ir pasiaiškinimas, ar nebuvo nustatyta gedimų pas paslaugų teikėją 3. Jeigu gedimas ne pas paslaugų teikėją, tuomet peržiūrimi elektros prietaisai įmonės viduje, pasitelkiant specialistų pagalbą 4. Situacijos analizė ir priemonių nustatymas, kad panašios situacijos nepasikartotų ateityje
Patalpų pažeidimas	1. Kritiškumo įvertinimas 2. Avarinių tarnybų informavimas apie prarastą galimybę naudotis patalpomis 3. Prarandant patalpas ar galimybę naudotis jomis dėl nusikalstamos veikos, informavimas teisėsaugos institucijų 4. Situacijos analizė ir priemonių nustatymas, kad panašios situacijos nepasikartotų ateityje
Duomenų sunaikinimas, atskleidimas ar praradimas	1. Kritiškumo įvertinimas 2. Nustatymas dėl kokių priežasčių duomenys buvo prarasti, sunaikinti ar atskleisti 3. Esant darbuotojo kaltei, daroma situacijos analizė ir pasitelkiamos priemonės, kad informacija būtų atkurta ar apsaugotas jos konfidencialumas, o vėliau priėmimas sprendimo dėl darbuotojo atsakomybės bei ar konkrečiu atveju apie tai privalu pranešti VDAI bei duomenų subjektui 4. Esant trečiųjų šalių kaltei (padarius nusikalstamą veiką),

	daroma situacijos analizė ir pasitelkiamos priemonės, kad informacija būtų atkurta ar apsaugotas jos konfidencialumas, o vėliau priėmimas sprendimo ar konkrečiu atveju apie tai privalu pranešti VDAI bei duomenų subjektui
Informacinės sistemos veiklos sutrikdymas, nulemtas kibernetinių atakų	1. Kritiškumo įvertinimas 2. Įvertinimas trikdžių pobūdžio bei šaltinio 3. Esant privalomumui, nutraukimas naudojimosi informacinės sistemos, iki kol būtų pašalinti virusai ar sustabdytos kibernetinės atakos 4. Patikrinama ar nebuvo sugadinti ar prarasti duomenys 5. Patikrinama informacinės sistemos veikla 6. Situacijos analizė ir priemonių nustatymas, kad panašios situacijos nepasikartotų ateityje