PATVIRTINTA
VšĮ „Vaivorykštės tako“ gimnazijos
direktorės Džiuljetos Gečienės
2025 m. balandžio 18 d., įsakymu
Nr.V4-15

VŠĮ „VAIVORYKŠTĖS TAKO" GIMNAZIJOS DUOMENŲ TVARKYMO INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1.1. Vykdyti Planą privaloma įvykus elektroninės informacijos saugos incidentui, kai gali kilti pavojus IS duomenų konfidencialumui, vientisumui ir prieinamumui (toliau - Incidentai).
1.2. 1.2. Veiksmų, kurie būtų atliekami įvykus Incidentui, vykdymo eiliškumas yra nurodomas šiame Plane.

II SKYRIUS
VEIKLOS VALDYMO IR ATKŪRIMO PRINCIPAI

2.1. Pagrindiniai Incidentų valdymo principai prioriteto tvarka:
- Darbuotojų gyvybės ir sveikatos apsaugos užtikrinimas;
- IS veiklos atkūrimas, visų pirma atkuriant kritiškiausias funkcijas;
- Darbuotojų informavimas ir mokymas apie incidentus ir atsakomybes.

2.2. IS, ryšių ir infrastruktūros atkūrimo reikalavimai:
- Kritiškiausių funkcijų atkūrimo prioritetas;
- Techninės įrangos, ryšių ir infrastruktūros funkcionavimo atkūrimas;
- Veiklos tęstinumas turi būti atkurtas per 8 val. darbo metu;
- Alternatyvių kompiuterių suradimo laikas – 2 darbo dienos;
- Toleruotinas duomenų praradimo kiekis – ne didesnis nei 24 val.

III SKYRIUS
ORGANIZACINĖS NUOSTATOS

3.1. IT specialistas atsakingas už IS veiklos tęstinumą, nebent šios funkcijos perduotos paslaugų teikėjui.
3.2. IT specialistas, koordinuodamas IS veiklos tęstinumą:
- analizuoja ir priima sprendimus dėl IS veiklos atkūrimo;
- bendrauja su atsakingais asmenimis ir institucijomis;
- prižiūri reikalingų išteklių naudojimą;
- koordinuoja fizinę saugą Incidento metu.

3.3. Atkūrimo metu IT specialistas:
- atkuria duomenis;
- atkuria taikomąsias programas;
- atkuria naudotojų kompiuterių veikimą.

3.4. Incidento metu IT specialistas informuoja įstaigos vadovą kas 2 val. apie atkūrimo eigą.
3.5. IS naudotojai reaguoja į Incidentus vadovaudamiesi 1 priede nurodytais veiksmais.
3.6. IT specialistas Incidentus valdo pagal 2 priede nurodytą tvarką.

IV SKYRIUS
APRAŠOMOSIOS NUOSTATOS

4.1. Tęstinumui užtikrinti turi būti surinkta ir naudojama aktuali informacija, būtina IS atkūrimui.
4.2. Šią informaciją organizuoja ir atnaujina IT specialistas.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

5.1. IS veikla laikoma atkurta, kai naudotojai gali atlikti savo funkcijas įprastiniu būdu.
5.2. Darbuotojai, pažeidę Plano ar teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

PRIEDAS NR. 1

VEIKSMAI INCIDENTO METU IS NAUDOTOJAMS

Situacija	Rekomenduojami veiksmai
Pavojus sveikatai/gyvybei (gaisras, griūtis)	1. Nedelsdami išeikite iš patalpų. 2. Praneškite apie pavojų avarinėms tarnyboms. 3. Praneškite apie pavojų Įstaigos vadovui.
Kompiuteris neįsijungia (elektra yra)	1.Patikrinkite, ar elektros laidai yra tvarkingai prijungti prie kompiuterio. 2. Informuokite IT specialistą. 3. Jei yra galimybė, tęskite darbą, perėję prie laisvos kompiuterizuotos darbo vietos. 4. Tęskite darbus rankiniu būdu.
Dingo elektra	1.Nedelsdami išjunkite kompiuterį. 2. Informuokite savo tiesioginį vadovą. 3. Palaukite 10 minučių. 4. Jei patalpoje yra pakankamas apšvietimas, tęskite darbus rankiniu būdu. 5. Jei patalpoje apšvietimas yra nepakankamas, pratęskite darbus tuomet, kai atsinaujins elektros tiekimas.
IS neveikia arba labai lėta	1.Informuokite IT specialistą. 2. Palaukite 10 minučių. 3. Jei sistema nepradeda normaliai veikti, tęskite darbus rankiniu būdu

PRIEDAS NR. 2

INCIDENTŲ VALDYMO IR VEIKLOS ATKŪRIMO VEIKSMAI

Incidentas	Atsakomieji veiksmai
Patalpų pažeidimas	1. Darbuotojų evakuacija. 2. Avarinių tarnybų informavimas, atsižvelgiant į iškilusio pavojaus pobūdį. 3. Žalos įvertinimas. 4. Pažeistų patalpų remonto, renovacijos, atstatymo darbų organizavimas. 5. Pažeistų ryšio linijų ir sugadintos techninės įrangos atstatymo ir duomenų atkūrimo organizavimas. 6. Įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.
Elektros tiekimo sutrikimai	1.Elektros tiekimo sutrikimo masto ir kritiškumo įvertinimas. 2. Kreipimasis į elektros energijos tiekimo Įstaigą dėl sutrikimo pašalinimo trukmės prognozės. 3. Įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.
Ryšio sutrikimai	1. Kritiškumo įvertinimas. 2. Ryšio sutrikimo priežasties nustatymas. 3. Kreipimasis į ryšio paslaugų teikėją dėl sutrikimo pašalinimo trukmės prognozės. 4. Įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.
Programinės įrangos sugadinimas	1.Kritiškumo įvertinimas. 2. Sugadintos programinės įrangos atstatymas iš kopijų. 3. Įvykusios situacijos išanalizavimas ir, esant reikalui, plano pakeitimas, siekiant išvengti panašių situacijų ateityje.
Duomenų praradimas/atskleidimas	1.Kritiškumo įvertinimas. 2. Neteisėto duomenų sugadinimo arba atskleidimo atvejais teisėsaugos tarnybų informavimas ir jų nurodymų vykdymas. 3. IS veiklos sutrikimo dėl duomenų sugadinimo ar praradimo atvejais duomenų atstatymas iš kopijų. 4. Įvykusios situacijos išanalizavimas, siekiant išvengti panašių situacijų ateityje.
Kibernetinė ataka	1. Nutraukti IS naudojimą ir informuoti Darbuotojus apie veiklos sutrikimus dėl esamų ar įtariamų kibernetinių atakų. 2. Nustatyti, jei įmanoma, trikdžių šaltinį. 3. Pranešti elektroninių ryšių ir informacijos saugumo incidentų tyrimo tarnyboms, suteikiant reikiamą informaciją apie įvykį Įstaigos nustatyta tvarka. 4. Patikrinti, ar neprarasti arba nesugadinti IS esantys duomenys. 5. Atkurti duomenis iš atsarginių kopijų. 6. Pašalinti trikdžius, atkurti IS darbingumą. 7. Prevenciškai yra prašoma trečiųjų asmenų, kad būtų testuojamas sistemos saugumas.
Kompiuterių gedimas	1.Pakeisti arba naudoti pakaitinį kompiuterį (-ius) kompiuterio gedimo laikotarpiu; 2. Sugedus kompiuteriui arba programinei įrangai, kasdienių funkcijų vykdymui ir tęstiniam darbui palaikyti naudojami nuomojami kompiuteriai arba kiti įrenginiai.