

## VISAGINO „VERDENĖS“ GIMNAZIJOS INFORMACINIŲ SISTEMŲ VEIKLOS TĖSTINUMO VALDYMO PLANAS

### I SKYRIUS

#### BENDROSIOS NUOSTATOS

1. Visagino „Verdenės“ gimnazijos informacinių sistemų veiklos tęstinumo valdymo plano (toliau – valdymo planas) tikslas – nustatyti Visagino „Verdenės“ gimnazijos (toliau – gimnazija) kompiuterijos inžinieriaus, informacinių sistemų naudotojų ir kitų asmenų veiksmus esant elektroninės informacijos saugos incidentui, kurio metu kyla pavojus informacinės sistemos duomenims, techninės, programinės įrangos funkcionavimui.

2. Valdymo planas parengtas vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, saugos dokumentų turinio gairių ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registų ir kitų informacinių sistemų klasifikavimo gairių, patvirtintų Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 ir Nacionalinių kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nacionalinis kibernetinių incidentų valdymo planas).

3. Valdymo plane vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše ir kituose Lietuvos Respublikos teisės aktuose vartojamas sąvokas.

4. Valdymo planas įsigalioja įvykus elektroninės informacijos saugos incidentui, jo vykdymas yra privalomas elektroninės informacijos saugos incidentų atveju, kurių metu gali kilti pavojus informacinių sistemų duomenims, informacinių sistemų techninės, programinės įrangos funkcionavimui.

5. Už valdymo plano įgyvendinimą atsakingi direktorius, kompiuterijos inžinierius, ūkio padalinio vadovas, direktoriaus pavaduotojas ugdymui, ir visi informacinių sistemų naudotojai.

6. Elektroninės informacijos saugos incidento metu patirti nuostoliai padengiami iš gimnazijos asignavimų ir kitų finansavimo šaltinių.

7. Informacinės sistemos veikla laikoma atkurta, jeigu bent 90 procentų yra atkurtas sistemos prieinamumas autorizuotų informacinės sistemos naudotojų atžvilgiu.

### II SKYRIUS

#### ORGANIZACINĖS NUOSTATOS

8. Veiklos tęstinumo valdymo grupės sudėtis:
  - 8.1. grupės vadovas – gimnazijos direktorius.
  - 8.2. Grupės nariai:
    - 8.2.1. kompiuterijos inžinierius;
    - 8.2.2. direktoriaus pavaduotojas ugdymui;
    - 8.2.3. ūkio padalinio vadovas;

8.2.4. informatikos mokytojas.

9. Veiklos tęstinumo valdymo grupės funkcijos:

- 9.1. analizuoti elektroninės informacijos saugos incidentus ir priimti sprendimus informacinės sistemos veiklos tęstinumo valdymo klausimais;
- 9.2. bendrauti su informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;
- 9.3. bendrauti su teisėsaugos ir kitomis institucijomis, atsakingomis už nacionalinių elektroninių ryšių tinklų ir informacijos saugumą;
- 9.4. kontroliuoti finansinių ir kitų išteklių, reikalingų informacinės sistemos veiklai atkurti įvykus elektroninės informacijos saugos incidentui, naudojimą;
- 9.5. užtikrinti elektroninės informacijos fizinę saugą įvykus saugos incidentui;
- 9.6. logistika (organizuoti darbuotojų, daiktų, įrangos gabenimą);
- 9.7. vykdyti informacinės sistemos veiklos atkūrimo priežiūrą ir koordinuoti veiklos atkūrimo veiksmus;
- 9.8. vykdyti kitas veiklos tęstinumo valdymo grupei pavestas funkcijas.
10. Įvykus elektroninės informacijos saugos incidentui patalpose, kuriose yra saugoma informacinės sistemos techninė ir programinė įranga, atliekami veiksmai.
11. Kompiuterijos inžinierius:
  - 11.1. apie elektroninės informacijos saugos incidentą nedelsdamas informuoja gimnazijos direktorių;
  - 11.2. informaciją įrašo į Elektroninės informacijos saugos incidentų registravimo žurnalą;
  - 11.3. pagal kompetenciją atkuria kompiuterių tinklo veiklą, duomenis, techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir apie tai informuoja gimnazijos direktorių.

### **III SKYRIUS**

#### **APRAŠOMOSIOS NUOSTATOS**

12. Gimnazija saugo:
  - 12.1. naudojimosi informacinės sistemos programine įranga sutartis gimnazijos dokumentų valdymo sistemoje;
  - 12.2. informacinės sistemos atsarginių duomenų kopijos saugomos serverinėje esančiuose serveriuose.
13. Už informacinės sistemos techninės ir programinės įrangos priežiūrą yra atsakingas direktoriaus įsakymu paskirtas asmuo.
14. Už informacinės sistemos atsarginių duomenų kopijų darymą, saugojimą, duomenų iš atsarginių kopijų atkūrimą atsakingas direktoriaus įsakymu paskirtas asmuo.
15. Gimnazijos direktorius, kompiuterijos inžinierius ir informatikos mokytojas kartą per kalendorinius metus įvertina informacinės sistemos naudotojų padaliniuose rizikos veiksmų galimybes, išnagrinėja gimnazijos informacinės sistemos nenumatytų situacijų registravimo žurnale padarytus įrašus, atlieka informacinės sistemos rizikos vertinimą..

### **IV SKYRIUS**

#### **KIBERNETINIŲ INCIDENTŲ VALDYMO PROCEDŪRA**

16. Kibernetinių incidentų valdymo procedūrų tikslas – aptikti, analizuoti kibernetinius incidentus ir reaguoti į juos, taip pat atkurti įprastinių ryšių ir informacinių sistemų veiklą.
17. Kibernetinio incidento valdymo organizavimas:
  - 17.1. informacinių sistemų naudotojas, pastebėjęs įvykį ar veiką kibernetinėje erdvėje, kurie gali sukelti grėsmę arba neigiamą poveikį ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui,

gali trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą, nedelsdamas apie tai informuoja kompiuterijos inžinierių ir (ar) direktorių;

17.2. gavęs informaciją apie minėtą įvykį ar veiką kibernetinėje erdvėje, kompiuterijos inžinierius:

17.2.1. nedelsdamas apie tai praneša gimnazijos direktoriui;

17.2.2. įvertina kibernetinį incidentą ir priskiria jį tam tikrai kategorijai remdamasis Nacionalinio kibernetinių incidentų valdymo plano (toliau – VP), patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, priede nustatyta tvarka;

17.2.3. informuoja Nacionalinio kibernetinio saugumo centrą apie didelio, vidutinio ir nereikšmingo poveikio kibernetinį incidentą VP nustatyta tvarka;

17.3. Nacionalinis kibernetinio saugumo centras, priskyres kibernetinį incidentą pavojingo kibernetinio incidento kategorijai ir nustatęs, kad kibernetinis incidentas gali turėti nusikalstamos veikos požymiu, informuoja Lietuvos policiją, o nustatęs, kad kibernetinis incidentas gali būti susijęs su asmens duomenų saugumo pažeidimais, – informuoja Valstybinę duomenų apsaugos inspekciją.

18. Kibernetinių incidentų tyrimas atliekamas vadovaujantis gimnazijoje patvirtintais kibernetinio saugumo teisės aktais tiek, kiek to nereglamentuoja VP, ir imamasi visų įmanomų priemonių, būtinų kibernetiniam incidentui suvaldyti ir įprastai ryšių ir informacinių sistemų veiklai atkurti.

---