Asmens duomenų tvarkymo taisyklių
Priedas Nr. 8

ŠIAULIŲ DAINŲ PROGIMNAZIJOS DUOMENŲ TVARKYMO INFORMACINĖS SISTEMOS VEIKLOS TĘSTINUMO VALDYMO PLANAS

Įstaigos Duomenų tvarkymo informacinės sistemos veiklos tęstinumo valdymo plane (toliau - **Planas**) vartojamos sąvokos turi reikšmę, nurodytą Įstaigos Asmens duomenų tvarkymo taisyklėse.

Planas reglamentuoja Įstaigos informacinių sistemų, kuriose tvarkomi asmens duomenys (toliau - **IS**) ir jos teikiamų funkcijų nepertraukiamos veiklos užtikrinimą.

1. Bendrosios nuostatos

1.1. Vykdyti Planą privaloma įvykus elektroninės informacijos saugos incidentui[1], kai gali kilti pavojus IS duomenų konfidencialumui, vientisumui ir prieinamumui (toliau - **Incidentai**).

1.2. Veiksmų, kurie būtų atliekami įvykus Incidentui, vykdymo eiliškumas yra nurodomas šiame Plane.

2. Veiklos valdymo ir atkūrimo principai

2.1. Pagrindiniai Incidentų valdymo principai prioriteto tvarka yra šie:

2.1.1. Įstaigos Darbuotojų gyvybės ir sveikatos apsaugos užtikrinimas. Būtina užtikrinti visų Darbuotojų gyvybės ir sveikatos apsaugą, kol trunka ekstremali situacija[2] ir likviduojami jos padariniai;

2.1.2. IS veiklos atkūrimas; paskelbus ekstremalią situaciją, jei būtina, organizuojama IS fizinė sauga ir jos veiklos atkūrimas; visų pirma turi būti atkurtos kritiškiausios IS funkcijos ir užtikrintas jų prieinamumas;

2.1.3. Įstaigos Darbuotojų mokymas; Darbuotojai nedelsiant turi būti informuojami apie susidariusią situaciją ir privalo būti iš anksto supažindinti su Planu ir kitais teisės aktais, nustatančiais asmeninę kiekvieno Įstaigos Darbuotojo atsakomybę, kai įvyksta Incidentas.

2.2. Pagrindiniai IS, ryšių ir infrastruktūros atkūrimo principai ir reikalavimai yra šie:

2.2.1. IS veikimui būtinos infrastruktūros atkūrimo pirmumas; pirmiausia būtina atkurti kritiškiausių IS sistemų kritiškiausias funkcijas;

2.2.2. IS sudarančios techninės įrangos, ryšių ir infrastruktūros funkcionavimas;

2.2.3. IS veiklos tęstinumas privalo būti atkurtas per 8 val. darbo metu, jei sutartyje su paslaugų teikėju nenumatytas trumpesnis laikotarpis;

2.2.4. Kompiuterių gedimo atveju, alternatyvių kompiuterių suradimo laikas – 2 darbo dienos.

2.2.5. Toleruotinas duomenų praradimo kiekis – ne didesnis negu 24h.

---

[1] Elektroninės informacijos saugos incidentas - įvykis ar veiksmas, kuris gali sudaryti neteisėto prisijungimo prie IS galimybę, sutrikdyti ar pakeisti IS 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] Ekstremali situacija - situacija, kuri skelbiama Įstaigos vadovo, Įstaigoje įvykus elektroninės informacijos saugos incidentui.

3. Organizacinės nuostatos

3.1. Įstaigos IT specialistas yra atsakingas už IS veiklos tęstinumą ir veiklos atkūrimą, jei šios funkcijos nėra perduotos paslaugų teikėjui, su kuriuo Įstaiga yra sudariusi duomenų tvarkymo sutartį. Prireikus, IT specialistas pasitelkia Saugumo specialistą į pagalbą ir visada konsultuojasi su DAP. Valdant Asmens duomenų saugumo pažeidimą taip pat vadovaujamasi Asmens duomenų saugumo pažeidimų reagavimo tvarkos aprašu (Priedas Nr. 6 prie Taisyklių). Jei kyla prieštaravimų tarp pastarojo dokumento ir Plano, vadovaujamasi Asmens duomenų saugumo pažeidimų reagavimo tvarkos aprašu.

3.2. Koordinuodamas IS veiklos tęstinumą, IT specialistas atlieka šias funkcijas:

3.2.1. analizuoja ir priima sprendimus dėl IS veiklos tęstinumo;
3.2.2. bendrauja su Saugumo specialistu, DAP, Darbuotojais, rangovais, teisėsauga ir kitomis institucijomis;
3.2.3. prižiūri finansinių ir kitų išteklių, reikalingų IS veiklai atkurti, įvykus Incidentui, naudojimą;
3.2.4. koordinuoja elektroninės informacijos fizinę saugą Incidento metu.

3.3. Atkurdamas IS veiklos tęstinumą, IT specialistas atlieka šias funkcijas:

3.3.1. IS duomenų atkūrimas;
3.3.2. taikomųjų programų tinkamas atkūrimas;
3.3.3. IS naudotojų kompiuterių veikimo atkūrimas.

3.4. Įvykus Incidentui, IT specialistas turi informuoti Įstaigos vadovą kas 2 valandas apie IS atkūrimo eigą.

3.5. IS naudotojai turi reaguoti į Incidentus, vadovaudamiesi 1 priede nurodytais veiksmais.

3.6. IT specialistas turi reaguoti ir valdyti Incidentus, vadovaujantis 2 priede nurodytais veiksmais.

4. Aprašomosios nuostatos

4.1. Veiklos tęstinumo vykdymo užtikrinimui turi būti surinkta ir naudojama detali bei aktuali informacija, būtina IS veiklos atkūrimui.

4.2. Veiklos tęstinumo vykdymui reikalingos detalios informacijos rengimą ir atnaujinimą organizuoja IT specialistas.

5. Baigiamosios nuostatos

5.1. IS veikla yra laikoma atkurta tuomet, kai IS naudotojai vėl gali atlikti savo darbines funkcijas įprastiniu būdu.

5.2. Darbuotojai, pažeidę Plano ir kitų veiklos tęstinumą reglamentuojančių teisės aktų nuostatas, atsako įstatymų nustatyta tvarka.

_____

Duomenų tvarkymo informacinės sistemos
veiklos tęstinumo valdymo plano
Priedas Nr. 1

VEIKSMAI INCIDENTO METU
IS NAUDOTOJAMS

Situacija	Rekomenduojami veiksmai
Iškyla pavojus jūsų sveikatai arba gyvybei (gaisras, pastato griūtis ir pan.).	1. Nedelsdami išeikite iš patalpų. 2. Praneškite apie pavojų avarinėms tarnyboms. 3. Praneškite apie pavojų Įstaigos vadovui.
Neįsijungia kompiuteris (patalpose 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.
Patalpose dingo elektros maitinimas (taip pat ir apšvietimas).	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 jos veikla sulėtėjo taip, kad neįmanoma atlikti darbų.	1. Informuokite IT specialistą. 2. Palaukite 10 minučių. 3. Jei sistema nepradeda normaliai veikti, tęskite darbus rankiniu būdu.

Duomenų tvarkymo informacinės sistemos
veiklos tęstinumo valdymo plano
Priedas Nr. 2

INCIDENTŲ VALDYMO IR VEIKLOS ATKŪRIMO ORGANIZAVIMO VEIKSMAI

Incidentas	Atsakomieji veiksmai
Patalpų pažeidimas arba praradimas	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 sugadinimas praradimas arba 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.
IS veiklos sutrikdymas dėl kibernetinių atakų	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.