Šiaulių Medelyno progimnazijos asmens duomenų tvarkymo taisyklių
Priedas Nr. 6

PATVIRTINTA
Šiaulių Medelyno progimnazijos
direktoriaus 2022 m. lapkričio 7 d.
įsakymu Nr. V-302

ŠIAULIŲ MEDELYNO PROGIMNAZIJOS ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ REAGAVIMO TVARKOS APRAŠAS

I SKYRIUS
1. BENDROSIOS NUOSTATOS

1.1. Asmens duomenų saugumo pažeidimų reagavimo tvarkos apraše (toliau - **Aprašas**) didžiąja raide vartojamos sąvokos, turi reikšmę, nurodytą Įstaigos Asmens duomenų tvarkymo taisyklėse.

1.2. Šio Aprašo tikslas nustatyti Įstaigos procedūras, atliekamas siekiant tinkamai valdyti bet kokius Asmens duomenų saugumo pažeidimus.

1.3. Aprašas yra privalomas visiems Įstaigos Darbuotojams. Darbuotojai supažindinami su šia Tvarka pasirašytinai.

II SKYRIUS
2. ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAS

2.1. Asmens duomenų saugumo pažeidimas yra tuomet, kai atsitiktinai ar neteisėtai atliekamas bet kuris iš šių veiksmų:

2.1.1. atskleidžiama ar suteikiama prieiga prie Įstaigos tvarkomų Asmens duomenų (konfidencialumo pažeidimas);

2.1.2. prarandama prieiga prie Asmens duomenų arba jie sunaikinami (prieinamumo pažeidimas);

2.1.3. pakeičiami Asmens duomenys (vientisumo pažeidimas).

(toliau – bet kuris iš 2.1 p. nurodytų veiksmų – **ADSP**)

2.2. ADSP be kita ko apima šiuos atvejus:

2.2.1. netyčinis asmens duomenų atskleidimas asmenims, neturintiems teisės juos gauti;

2.2.2. duomenų arba įrangos, kuriuose saugomi duomenys ar yra prieiga prie jų, praradimas ar vagystė;

2.2.3. popierinių įrašų praradimas ar vagystė;

2.2.4. įrašai pakeičiami arba ištrinami be leidimo;

2.2.5. fizinio saugumo pažeidimai, pvz., fizinis ar elektroninis durų ar langų pažeidimas patalpose, kuriose laikomi asmens duomenys;

2.2.6. asmens duomenų palikimas laisvai su asmens duomenimis neturintiems teisės susipažinti asmenims prieinamose vietose;

2.2.7. IT įrangos palikimas be priežiūros, kai prisijungiama prie vartotojo abonemento, neužblokuojamas ekranas;

2.2.8. sustabdoma įgaliotų asmenų prieiga prie informacijos;

2.2.9. el. laiškai, kuriuose yra asmens duomenys, klaidingai išsiunčiami neteisingam gavėjui ir kt.

III SKYRIUS

3. ADSP PRIELAIDOS

3.1. Pagrindiniai šaltiniai, kuriais naudojantis gali būti sukeltas ADSP ir sutrikdyta Įstaigos infrastruktūra, yra:

3.1.1. išorinės kompiuterinės laikmenos;

3.1.2. internetas;

3.1.3. interneto svetainių pagrindu veikianti programinė įranga;

3.1.4. paprasta įranga;

3.1.5. kiti ADSP šaltiniai.

3.2. Informacija apie galimą ADSP gali būti gaunama iš įvairių informacijos šaltinių:

3.2.1. IT paslaugų teikėjo, kuris atlieka ADSP stebėseną;

3.2.2. Asmens duomenų tvarkytojų;

3.2.3. kompetentingų valstybės institucijų;

3.2.4. tarptautinių organizacijų arba institucijų, atliekančių Asmens duomenų saugumo užtikrinimo funkcijas;

3.2.5. kitų juridinių ar fizinių asmenų.

3.3. Bet kuris Darbuotojas, gavęs informacijos apie galimą ADSP, nedelsiant praneša savo skyriaus vadovui ir IT specialistui, o pastarasis Saugumo specialistui ir DAP.

3.4. Reaguojant į galimą ADSP, atliekami tokie veiksmai (žr. lentelę apačioje):

3.4.1. ADSP nustatymas;

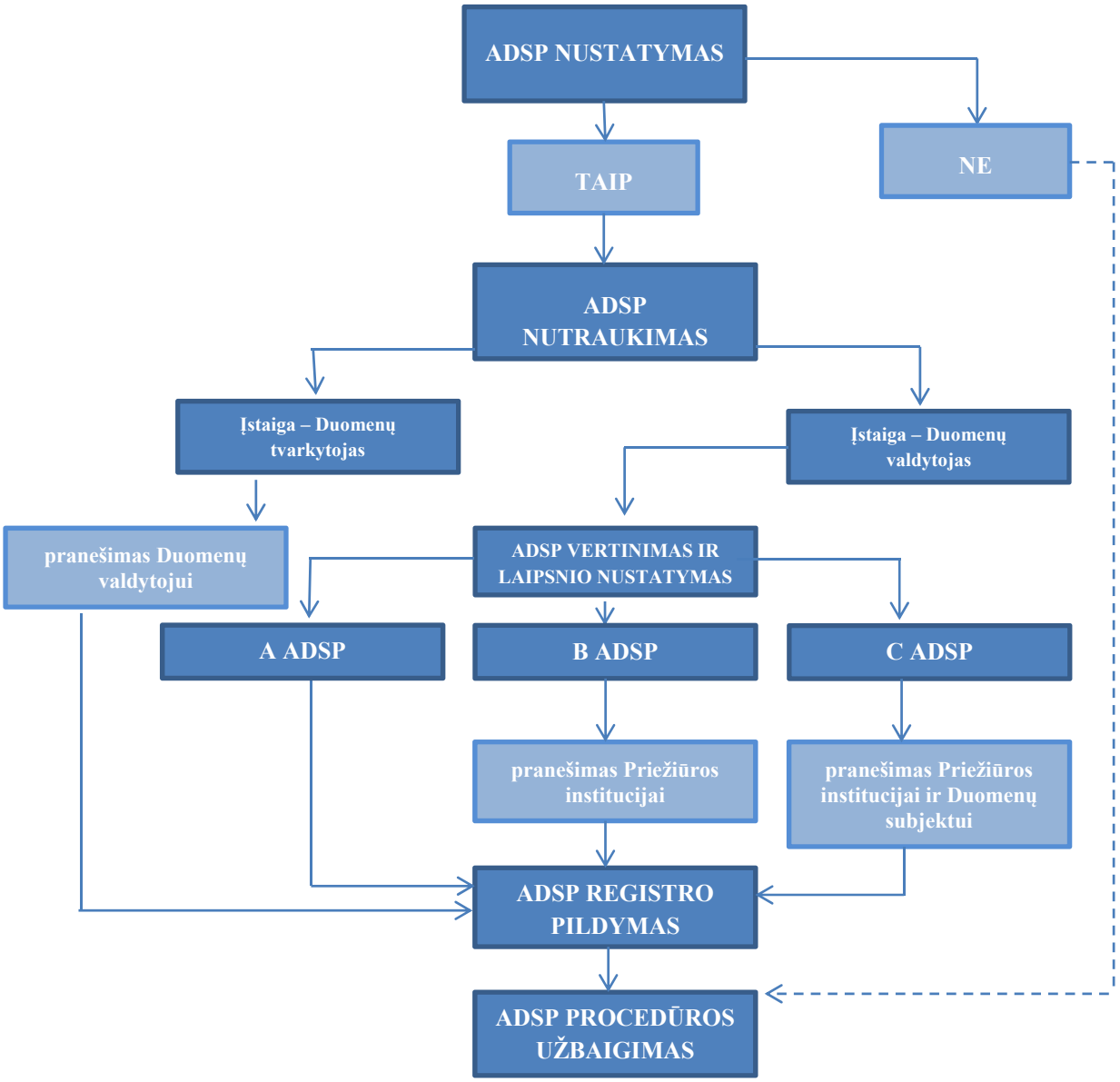
3.4.2. ADSP nutraukimas ir Asmens duomenų atkūrimas;

3.4.3. ADSP laipsnio vertinimas ir nustatymas;

3.4.4. pranešimas apie ADSP;

3.4.5. ADSP registro pildymas;

3.4.6. ADSP procedūros užbaigimas.



IV SKYRIUS

4. ADSP NUSTATYMAS

4.1. Saugumo specialistas įvertina gautą informaciją apie galimą ADSP pagal Tvarkos 2.1, 2.2 p. nurodytus kriterijus, konsultuojasi su DAP ir patvirtina arba paneigia ADSP nustatymo faktą. Kilus abejonių ar incidentas laikomas ADSP, Saugumo pareigūnas konsultuojasi su Valstybine duomenų apsaugos inspekcija (toliau – **Priežiūros institucija**).

4.2. Saugumo specialistas, patvirtinęs ADSP nustatymo faktą, per kuo trumpesnį laiką praneša Įstaigos vadovui apie ADSP. Jei reikia, sudaroma ADSP valdymo komanda (toliau – **Valdymo komanda**), į kurios sudėtį įeina Saugumo specialistas, IT specialistas, DAP, taip pat gali įeiti kiti Darbuotojai ar paslaugų teikėjai.

4.3. Atsižvelgiant į ADSP pobūdį, atliekant asmens duomenų saugumo pažeidimo tyrimą turi būti išsaugomi visi esamos situacijos įrodymai bei vėliau naudojamos visos tinkamos techninės ir organizacinės priemonės, pvz., prisijungimų analizės įrankiai bei kt.

4.4. Nustatoma, ar ADSP susijęs su Asmens duomenimis, kuriuos tvarkydama Įstaiga veikia kaip Duomenų valdytojas, ar kaip Duomenų tvarkytojas. Įstaigos pasitelktas duomenų tvarkytojas

apie įvykusį ADSP Įstaigą informuoja su ja sudarytoje Asmens duomenų tvarkymo sutartyje nustatytais terminais ir tvarka.

V SKYRIUS

5. PAŽEIDIMO NUTRAUKIMAS IR PADĖTIES ATKŪRIMAS

5.1. Saugumo specialistas ir IT specialistas nedelsiant imasi visų įmanomų priemonių ADSP nutraukti ir padėčiai atstatyti. Jei būtina, pasitelkiami kiti Įstaigos Darbuotojai, IT paslaugų teikėjai, Valdymo komanda.

5.2. Saugumo specialistas, veikdamas kartu su IT specialistu arba/ir Valdymo komanda, pagal kompetenciją, priklausomai nuo situacijos įvertina Įstaigos informacinės infrastruktūros būklę, nustato pažeistas jos dalis ir per kuo trumpesnį laiką imasi veiksmų pažeistoms dalims atkurti arba pakeisti ir (arba) teikia Įstaigos IT infrastuktūros paslaugos teikėjams siūlymus dėl pažeistų dalių atkūrimo arba pakeitimo, jeigu to negalima padaryti savo jėgomis.

5.3. Prieš atkurdami Įstaigos informacinės infrastruktūros veiklą, Saugumo specialistas ir IT specialistas, privalo įsitikinti, ar pašalintas pažeidžiamumas, dėl kurio įvyko ADSP.

5.4. Pagrindiniai kriterijai, kuriais vadovaujantis priimamas sprendimas dėl ADSP valdymo priemonių:

5.4.1. numatytas galimas poveikis ir žala;

5.4.2. ADSP įrašų išsaugojimo, jų patikimumo, vientisumo ir pasiekiamumo užtikrinimas;

5.4.3. informacinės infrastruktūros neveikimo terminas;

5.4.4. ADSP valdymo sprendimui įgyvendinti reikalingas laikas ir ištekliai;

5.4.5. numatoma kita žala, kurią gali padaryti ADSP, priėmus jo valdymo sprendimą.

5.5. Konkretūs veiksmai, siekiant nutraukti ADSP ir atstatyti padėtį galėtų būti tokie:

5.5.1. Asmens duomenų ištrynimas nuotoliniu būdu iš pamesto ar pavogto įrenginio;

5.5.2. kuo skubesnis kreipimasis į asmenį, kuriam per klaidą buvo išsiųsti Asmens duomenys, su prašymu neatidarinėti atsiųstų duomenų ir juos ištrinti be galimybės atkurti;

5.5.3. Tretiesiems asmenims atskleisto prisijungimo prie duomenų bazės slaptažodžio pakeitimas;

5.5.4. prarastų Asmens duomenų atkūrimas iš turimos atsarginės kopijos.

5.6. Vykdant šią procedūrą reikia imtis atsargumo priemonių tam, kad būtų užtikrinta, jog būtų surinkti kiek įmanoma tikslesni duomenys bei įrodymai apie įvykusį ADSP (pavyzdžiui, užfiksuojama, kas, kada ir iš kokio įrenginio jungėsi prie duomenų bazės, kam konkrečiai buvo per klaidą išsiųsti Asmens duomenys, kokiomis aplinkybėmis buvo prarastas įrenginys su Asmens duomenimis).

5.7. Suvaldant ADSP taip pat vadovaujamasi Įstaigos Duomenų tvarkymo informacinės sistemos veiklos tęstinumo valdymo planu (Priedas Nr. 8 prie Taisyklių).

VI SKYRIUS

6. PAŽEIDIMO LAIPSNIO VERTINIMAS

6.1. Saugumo specialistas nedelsiant, bet ne vėliau, kaip per 4 val. nuo ADSP, kuris susijęs su Asmens duomenimis, kuriuos Įstaiga tvarko kaip Duomenų valdytojas, nustatymo, išsiaiškina ADSP aplinkybes ir kartu su IT specialistu ir DAP įvertina ADSP sunkumą, suteikiant ADSP vieną iš šių laipsnių: A – tikėtina, kad rizikos asmenims dėl ADSP nėra (toliau - **A ADSP**); B – dėl ADSP kyla rizika asmenims (toliau - **B ADSP**); C – dėl ADSP yra didelė rizika asmenims (toliau - **C ADSP**). Konkretus ADSP sunkumo laipsnis nustatomas pagal žemiau

nurodytus kriterijus. Konkretų ADSP laipsnį patvirtina Įstaigos vadovas pagal Saugumo specialisto rekomendaciją.

6.2. A ADSP laipsnis nustatomas tada, kai patiriamas ADSP, dėl kurio neturėtų kilti pavojaus fizinių asmenų teisėms ir laisvėms, kurių Asmens duomenys tvarkomi. A ADSP gali būti, pavyzdžiui, kai nustatoma, kad paliktas kompiuteris neužrakintu ekranu, tačiau prieiga prie asmens duomenų apsaugota šifravimu.

6.3. B ADSP laipsnis nustatomas tada, kai patiriamas ADSP, kuris kelia pavojų Duomenų subjektams (pavojų keliančiu laikytinas toks pažeidimas, dėl kurio asmuo galėtų patirti materialinę ar nematerialinę žalą, teisių apribojimą, diskriminaciją, galėtų būti pavogta ar suklastota asmens tapatybė, asmeniui padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta asmens reputacijai, prarasti Asmens duomenys, kurie laikomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala). Tokie atvejai galėtų būti, pavyzdžiui, laikmenos praradimas su kelių klientų fizinių asmenų kontaktais ir klientų finansiniais duomenimis.

6.4. C ADSP nustatomas tada, kai dėl ADSP gali kilti didelis pavojus fizinių Duomenų subjektų teisėms ir laisvėms (didelį pavojų keliančiu ADSP laikytinas bet kuris 6.3. punkte nurodytų pasekmių riziką keliantis ADSP tada, jei tokios pažeidimo pasekmės yra labai tikėtinos, tvarkomi jautrūs Asmens duomenys (pavyzdžiui, duomenys apie sveikatą, atlyginimus), pažeidimas turi neigiamą poveikį dideliam Duomenų subjektų skaičiui ir pan.). Pavyzdžiui, pametamas nešiojamasis kompiuteris, kuriame yra sutartys su klientais fiziniais asmenimis, ir prieiga prie jų nėra šifruota ar kitaip apsaugota dėl ko duomenys negali būti perskaitomi.

6.5. Vertinant ADSP laipsnį, gali būti vadovaujamasi Asmens duomenų pažeidimo sunkumo vertinimo metodika, patvirtinta Europos Sąjungos kibernetinio saugumo agentūros (*ENISA Personal Data Breach Severity Assessment Methodology*)[1]; 29 straipsnio darbo grupės 2017-10-03 Pranešimo apie asmens duomenų saugumo pažeidimo gairėmis pagal reglamentą 2016/679[2] ir Europos duomenų apsaugos valdybos 2021-12-14 Gairėmis dėl pranešimo apie asmens duomenų saugumo pažeidimus pavyzdžius[3].

VII SKYRIUS

7. PRANEŠIMAS APIE ADSP

7.1. Patvirtinus A ADSP, pranešimas nei Priežiūros institucijai, nei Duomenų subjektams nėra teikiamas, išskyrus atvejus, kai pats duomenų subjektas informuoja apie galimai įvykusį ADSP. ADSP dokumentuojama, kaip nurodyta Priede Nr. 1 ir užbaigiama ADSP procedūra.

7.2. Nustačius B ADSP, Saugumo specialistas ne vėliau kaip per 72 valandas nuo ADSP patvirtinimo momento Priežiūros institucijai pateikia reikiamą informaciją, užpildydamas Pranešimo formą, pateiktą Priede Nr. 2. Pranešimas Duomenų subjektams nėra teikiamas, išskyrus atvejus, kai pats duomenų subjektas informuoja apie galimai įvykusį ADSP.

7.3. Pranešimas Priežiūros institucijai teikiamas per interneto svetainę www.vdai.lrv.lt naudojantis elektronine paslaugų sistema; nesant tokios galimybės, pranešimas teikiamas elektroninio pašto adresu ada@ada.lt; nesant tokių galimybių, Valstybinė duomenų apsaugos inspekcija informuojama telefono ryšio numeriu, kuris skelbiamas www.vdai.lrv.lt ir nedelsiant informacija išsiunčiama registruotu laišku.

7.4. Jei Priežiūros institucijai apie ADSP nepranešama per 72 valandas, prie pranešimo privalo pateikti vėlavimo priežastis.

---

[1] https://www.enisa.europa.eu/publications/dbn-severity
[2] file:///C:/Users/D1CBC~1.TAM/AppData/Local/Temp/7zO84C7289A/wp250rev01_lt.pdf
[3] Guidelines 01/2021 on Examples regarding Personal Data Breach Notification

7.4.1. Kai ir jeigu informacijos apie ADSP neįmanoma pateikti visa apimtimi tuo pačiu metu, informacija toliau nepagrįstai nedelsiant gali būti teikiama etapais.

7.4.2. Jei Priežiūros institucija paprašo patikslinti arba papildyti informaciją apie ADSP, Saugumo specialistas organizuoja papildomos informacijos surinkimą ir pateikimą Priežiūros institucijai jos nustatytu laiku.

7.5. Patvirtinus C ADSP, Saugumo specialistas praneša Priežiūros institucijai (tokia pačia tvarka, kaip pranešama apie B ADSP) ir nepagrįstai nedelsdamas praneša apie ADSP Duomenų subjektams. Saugumo specialistas Duomenų subjektams turi pateikti aiškią ir suprantamą informaciją, suderintą su DAP kurioje turi būti bent ši informacija:

7.5.1. ADSP apibūdinimas;

7.5.2. tikėtinų padarinių, kurie jau atsirado arba gali atsirasti ateityje, sąrašas;

7.5.3. priemonių, kurių buvo imtasi ir/ar bus imtasi norint sustabdyti ADSP bei pašalinti atsiradusius arba atsirasiančius padarinius, priemonių galimoms neigiamoms pasekmėms sumažinti sąrašas;

7.5.4. Saugumo specialisto ir DAP kontaktai. DAP komunikuoja su Priežiūros institucija ir kitomis institucijomis, tiriančioms ADSP.

7.6. 7.5. punkte nurodytas pranešimas Duomenų subjektams gali būti neteikiamas, jei egzistuoja bet kuri iš šių aplinkybių:

7.6.1. Įstaiga įgyvendino tinkamas technines ir organizacines apsaugos priemones ir tos priemonės taikytos Asmens duomenims, kuriems ADSP turėjo poveikį, kurios užtikrina, kad Asmens duomenys būtų nesuprantami, pavyzdžiui, šifravimo priemonės;

7.6.2. Įstaiga vėliau ėmėsi priemonių, kuriomis užtikrinama, kad ateityje negalėtų kilti didelis pavojus Duomenų subjektų teisėms ir laisvėms;

7.6.3. tiesioginis komunikavimas pareikalautų neproporcingai daug pastangų; tokiu atveju apie įvykusį ADSP Įstaigos vadovui patvirtinus, paskelbiama viešai arba taikoma panaši priemonė, kuria Duomenų subjektai būtų informuojami taip pat efektyviai. Šiuo atveju pateikiama šio Priedo 7.5.1 – 7.5.4 punktuose nurodyta informacija.

7.7. Saugumo specialistas, įvertinęs gautą informaciją apie ADSP, pasitaręs su DAP, esant Įstaigos vadovo sutikimui, nedelsdamas informuoja apie ADSP nustatymo faktą ne tik Priežiūros instituciją ar Duomenų subjektą (kai reikia), bet ir policiją - nustačius, kad ADSP gali turėti nusikalstamos veikos požymių ir atitinkamais atvejais Nacionalinį kibernetinio saugumo centrą. Šiuo atveju vykdant pranešimų apie ADSP prievolę, turi būti atsižvelgiama į teisėsaugos institucijų interesus, kai ankstyvas informacijos atskleidimas galėtų bereikalingai pakenkti ADSP aplinkybių tyrimui.

7.8. Jei nustatoma, kad ADSP susijęs su Asmens duomenimis, kuriuos Įstaiga tvarko kaip duomenų tvarkytojas, apie įvykusį ADSP informuoja duomenų valdytoją (pvz., Švietimo, mokslo ir sporto ministeriją) teisės aktų, kuriais Įstaiga paskirta duomenų tvarkytoju, ar Asmens duomenų tvarkymo sutartyse su duomenų valdytoju nustatyta tvarka.

VIII SKYRIUS

8. ADSP REGISTRO PILDYMAS

8.1. Visi veiksmai, kurių imamasi ADSP valdymo procedūros metu, turi būti aprašomi ir visi susiję įrašai apie ADSP peržiūrimi tam, kad būtų užtikrintas jų išbaigtumas, tikslumas ir atitiktis atitinkamam teisiniam reguliavimui. Šiam tikslui pasiekti turi būti vedamas ADSP žurnalas,

kuriame tiksliai aprašomi veiksmai, kurių buvo imtasi įgyvendinant ADSP valdymo procedūrą.

8.2. ADSP žurnalo elektroninė forma yra pateikta Priede Nr. 1. Elektroninį ADSP registrą pildo Saugumo specialistas, pasikonsultavęs su DAP. ADSP žurnale saugomi ne senesni, nei 10 metų, įrašai.

8.3. ADSP žurnale esantys įrašai peržiūrimi Saugumo specialisto ne rečiau kaip kartą per kalendorinį ketvirtį. ADSP išanalizuojami ne vėliau kaip per vieną kalendorinį mėnesį nuo jų nustatymo. Saugumo specialistas kartu su DAP, IT specialistu išanalizuoja ADSP ir pateikia ataskaitą su išvadomis bei rekomenduojamomis įgyvendinti prevencijos priemonėmis Įstaigos vadovui. Prevencijos priemonės įgyvendinamos ataskaitoje pasiūlytais ir vadovo patvirtintais terminais. IT specialistas ir DAP kontroliuoja kaip įgyvendinamos ADSP prevencijos priemonės.

IX SKYRIUS

9. ADSP PROCEDŪROS UŽBAIGIMAS

9.1. Suvaldžius ADSP, Saugumo specialistas apie ADSP suvaldymo rezultatus informuoja Įstaigos vadovą.

9.2. Saugumo specialistas, gavęs supažindinto su ADSP ir jo pašalinimo aplinkybėmis Įstaigos vadovo pritarimą, priima sprendimą užbaigti ADSP valdymo procedūrą tada, kai ADSP laikytinas likviduotu, o visoms reikalingoms šalims apie ADSP yra pranešta.