VILNIAUS UNIVERSITETO

INFORMACINIŲ TECHNOLOGIJŲ PASLAUGŲ CENTRAS

Į S A K Y M A S

DĖL ITPC TVARKOMŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS KRITINIŲ INCIDENTŲ TYRIMO TVARKOS APRAŠO PATVIRTINIMO

2018 m. gruodžio 18 d. Nr. (1.1) 640000-DV-16

1. T v i r t i n u VU ITPC tvarkomų informacinių sistemų elektroninės informacijos saugos kritinių incidentų tyrimo tvarkos aprašą.
2. 2015 m. liepos 14 d. ITTC direktoriaus įsakymą Nr. 520000-DI-16 -(5201.DĮ) laikyti negaliojančiu.

Informacinių technologijų paslaugų centro direktorius Arūnas Stašionis

PATVIRTINTA
ITPC direktoriaus įsakymu
2018-12-18 Nr. 640000-DV-16

VILNIAUS UNIVERSITETO ITPC TVARKOMŲ INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS, KIBERNETINIŲ IR ASMENS DUOMENŲ SAUGOS KRITINIŲ INCIDENTŲ TYRIMO TVARKOS APRAŠAS

I. BENDROSIOS NUOSTATOS

1. Vilniaus universiteto ITPC tvarkomų informacinių sistemų (toliau – IS) ir IT paslaugų elektroninės informacijos, kibernetinių ir asmens duomenų kritinių saugos incidentų (toliau – kritinių incidentų) tyrimo tvarkos aprašas (toliau – Aprašas) nustato VU ITPC tvarkomų informacinių sistemų (išskyrus, kai tai kitaip numatyta tų sistemų elektroninės informacijos saugos dokumentuose) ir IT paslaugų naudotojų, administratorių, sistemų saugos įgaliotinių ir informacinių sistemų saugos incidentų tyrimo grupės narių (toliau – Grupės) ir kompiuterių tinklų veiksmus, tiriant informacinių sistemų techninės ir programinės įrangos funkcionavimo, duomenų tvarkymo bei teikimo sutrikimus įvykus kritiniams incidentams, kai jie nustatomi įvertinus veiklos tęstinumo plane nustatytus kriterijus.
2. Apraše apibrėžiamos sąvokos:
   2.1. Eskalavimas – incidento kategorijos perkvalifikavimas ir/arba didesnius įgaliojimus turinčių padalinio vadovų ir/arba tarnybų įtraukimas į incidento sprendimą.
   2.2. Informacinė sistema – VU ITPC tvarkomų informacinių technologijų išteklių ir programinės įrangos visuma, skirta vieno ar kelių veiklos procesų informaciniam ir techniniam aprūpinimui.
   2.3. Informacinių technologijų paslaugos (toliau – IT paslaugos) – ITPC teikiamos informacinės bei duomenų perdavimo paslaugos Universiteto bendruomenei, Lietuvos švietimo ir mokslo bei kitoms Lietuvos ar užsienio institucijoms.
   2.4. Sistemos administratorius – tai darbuotojas, atsakingas už informacinei sistemai skirtų infrastruktūros išteklių naudojimą ir techninėmis priemonėmis užtikrinantis jų veikimą bei elektroninės informacijos saugą;
   2.5. Kritinis incidentas – įvykis ar veikla kibernetinėje erdvėje, sudarantis ar galintis sudaryti galimybę ar sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, įskaitant bet neapsiribojant asmens duomenimis, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims ir įvykio padariniai atitinka incidento kritiškumo vertinimo kriterijus, įvardintus ITPC veiklos tęstinumo valdymo plane.
   2.6. Kitos šiame Apraše vartojamos sąvokos apibrėžtos Aprašo 3 punkte nurodytuose teisės aktuose.
3. Kritiniai incidentai valdomi vadovaujantis:
   3.1. Lietuvos Respublikos elektroninių ryšių įstatymu;
   3.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

3.3. Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymu;
3.4.Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“;
3.5. Lietuvos Respublikos Valstybinės duomenų apsaugos inspekcijos direktoriaus 2018 m. gegužės 24 d. įsakymu Nr. 1T-53(1.12.) „Dėl pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamos formos patvirtinimo“;
3.6. Lietuvos Respublikos Krašto apsaugos ministro 2016 m. sausio 6 d. įsakymu Nr. V-11 „Dėl Nacionalinio kibernetinio saugumo centro reagavimo į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose tvarkos aprašo“;
3.7. Vilniaus universiteto kanclerio 2017 m. birželio 20 d. įsakymu Nr. R-265 (Vilniaus universiteto kanclerio 2018 m. kovo 14 d. įsakymo Nr. R-145 redakcija) „Dėl ITPC nuostatų keitimo ir ITPC padalinių nuostatų tvirtinimo“;
3.8. Studijuojančiųjų asmens duomenų tvarkymo Vilniaus universitete taisyklėmis, patvirtintomis Vilniaus universiteto senato komisijos 2013 m. birželio 20 d. nutarimu Nr. SK-2013-8-7;
3.9. Asmens duomenų tvarkymo Vilniaus universitete tvarkos aprašu, patvirtintu 2018 gegužės 25 d. Vilniaus universiteto rektoriaus įsakymu Nr. R-316 „Dėl asmens duomenų tvarkymo Vilniaus universitete tvarkos aprašo patvirtinimo“;
3.10. Asmens duomenų tvarkymo mokslinio tyrimo tikslais Vilniaus universitete taisyklėmis, patvirtintomis 2015 m. lapkričio 23 d. Vilniaus universiteto rektoriaus įsakymu Nr. R-452 „Dėl Vilniaus universiteto asmens duomenų tvarkymo mokslinio tyrimo tikslais taisyklių patvirtinimo“;
3.11. Vilniaus universiteto darbo tvarkos taisyklėmis, patvirtintomis Vilniaus universiteto rektoriaus 2015 m. balandžio 20 d. įsakymu Nr. R-146;
3.12. Vilniaus universiteto studijų nuostatais, patvirtintais Vilniaus universiteto Senato komisijos 2012 m. birželio 21 d. nutarimu Nr. SK-2012-12-8;
3.13. Vilniaus universiteto ITPC veiklos tęstinumo valdymo planu, patvirtintu 2015-03-14 Rektoriaus įsakymu R-83;
3.14. VU kanclerio įsakymas Nr. R-335 „Dėl IT techninės įrangos prieglobos VU duomenų centre“, patvirtintu 2016 m. rugsėjo 9 d.;
3.15. IT įrangos prieglobos Vilniaus universiteto ITPC duomenų centre paslaugos aprašu, patvirtintu VU ITPC direktoriaus 2018-12-03 įsakymu (1.1) 640000-DV-14.

II. PRANEŠIMŲ APIE SAUGOS INCIDENTUS REGISTRAVIMAS IR NEATIDĖLIOTINI SAUGOS INCIDENTŲ PLĖTROS SUSTABDYMO VEIKSMAI

4. ITPC darbuotojas, arba bet kuris naudotojas, įtardamas saugos incidentą arba jo požymius, nedelsdamas praneša IT pagalbos elektroniniu paštu pagalba@itpc.vu.lt ir/arba telefonu 8 (5) 236 6200 (tarnybos darbo valandomis nuo 8 iki 17 val.).
5. Gautas pranešimas apie saugos incidentą pranešėjo vardu registruojamas IT pagalbos sistemoje adresu https://veiklos.vu.lt/projects/ITPC/issues ir priskiriamas:
5.1. sistemos administratoriui - incidentui spręsti;

5.2. atsakingo padalinio vadovui - incidentui stebėti, ir/arba toliau nustatytais atvejais - incidentui spręsti ir tirti;

5.3. susijusios informacinės sistemos duomenų saugos įgaliotiniui – incidentui stebėti ir/arba toliau nustatytais atvejais - incidentui tirti;

5.4. informacijos saugos vadovui - incidentui stebėti ir/arba toliau nustatytais atvejais - tirti.

6. IT pagalbos skyriaus darbuotojas, įvertinęs incidento kritiškumą ir sprendimo eigą turi teisę eskaluoti incidento sprendimą atsakingo už paslaugos teikimo skyriaus vadovui;

7. Atsakingo už incidento sprendimą padalinio vadovas privalo per 4 darbo valandas įvertinti, ar incidentas gali būti pašalintas per veiklos tęstinumo plano 6 priede incidento kategorijai numatytą terminą, ir eskaluoja incidentą sušaukdamas veiklos atkūrimo grupės pasitarimą, kai numanomi incidento padarinių šalinimo terminai galimai viršys nustatytus veiklos tęstinumo plane kriterijus.

8. Jei incidentas išsprendžiamas neviršijant numatytų minimalių veiklos tęstinumo plane incidento sprendimui terminų, atsakingo padalinio vadovas įvertina sprendimo eigą informacinėje sistemoje JRA ir priima sprendimą uždaryti incidentą.

9. Incidentai, kurių padariniai ir šalinimo aplinkybės atitinka kritinių incidentų kriterijus, turi būti tiriami toliau nustatyta tvarka.

10. Jei padalinio vadovas įvertina, kad incidentas gali turėti didesnių nei incidentas nepavyksta išspręsti per 24 valandas, incidentas eskaluojamas papildomai informuojant apie susidariusią padėtį veiklos atkūrimo valdymo grupės vadovą (ITPC direktorių ar jį pavaduojantį tuo metu asmenį).

11. Informacinės sistemos duomenų saugos įgaliotinis, o jei toks nepaskirtas, Informacijos saugos vadovas, gavęs pranešimą apie kritinį saugos incidentą ir įvertinęs jo aplinkybes, perklasifikuoja saugos incidentą, organizuoja tyrimui būtinos medžiagos surinkimą, informuoja kitus susijusius darbuotojus bei esant poreikiui, susijusias institucijas.

12. Įvykus incidentui, sistemos administratorius informuoja tiesioginį vadovą, arba jam nesant, pagalbos tarnybą su prašymu jį informuoti ir nedelsiant imasi visų deramų atsargumo priemonių ir, nesukeldamas žalos teikiamoms paslaugoms ir sistemoms:

12.1. atlieka neatidėliotinus administravimo veiksmus, skirtus saugos incidento plitimui sustabdyti;

12.2. įjungia administravimo veiksmų įrašų išsaugojimo režimą, o jei nėra tokios galimybės – kopijuoja administravimo komandas į tekstinę laikmeną, fiksuodamas veiksmų laiko žymas;

12.3. išsaugo esamas incidento metu įrangos duomenų, sisteminių įrašų ir konfigūracijos kopijas, reikiamas tyrimui;

12.4. pagal ITPC veiklos tęstinumo valdymo plano 6 priede aprašytus kriterijus įvertinęs, kad incidentas gali būti klasifikuojamas kritiniu, informuoja savo tiesioginį vadovą;

12.5. lokalizavęs incidentą ir sustabdęs jo plitimą, pateikia IT pagalbos sistemoje incidentui tirti reikiamus pagal sistemos kategoriją susijusius sisteminius įrašus. Perduodami registruoti tinklo įvykiai, asmens duomenų kopijavimo, jei jis darytas, ir atkūrimo jų avarinio praradimo atveju veiksmai (kada ir kas atliko šiuos veiksmus), ir informacija apie informacinėje sistemoje įrašomus duomenis, apie informacinės sistemos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis informacinėje sistemoje, visus informacinės sistemos naudotojų vykdomus veiksmus, kitus saugai svarbius įvykius (2013 spalio 4 d. Vidaus reikalų ministro įsakymo Nr. 1V-832 punkte 7.7 nurodyta informacija), Lietuvos Respublikos elektroninių ryšių įstatymo 1 priede nurodytą informaciją bei pagal galimybes kita tyrimui reikalinga informacija.

13. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią informacinės sistemos saugą, ITPC informacijos saugos vadovas nustatyta tvarka informuoja ITPC direktorių, informacinės(-ių) sistemos(-ų) valdytojo(-ų) atstovą (-us) ir, poreikiui esant, kompetentingas institucijas, tiriančias

elektroninių ryšių tinklų, asmens duomenų apsaugos, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais.

14. Įvertinus, kad kilo kritinis incidentas, tiesioginis administratoriaus vadovas informuoja veiklos tęstinumo plano valdymo grupės vadovą, kuris priima sprendimą dėl veiklos incidento padarinių šalinimo ir veiklos atkūrimo veiksmų.

III. SAUGOS INCIDENTŲ TYRIMAS

15. Jei incidentas nekritinis, saugos incidento tyrimą atlieka už prižiūrimą informacinę sistemą atsakingas skyriaus vadovas.

16. Atsakingo skyriaus vadovo nurodymu medžiagą tyrimui renka ir teikia susijusių sistemų administratoriai.

17. Jei incidentas kritinis, saugos incidento šalinimą organizuoja atsakingas skyriaus vadovas, tyrimą organizuoja sistemos duomenų saugos įgaliotinis, o nepašalinus incidento per 1 darbo dieną, incidento tyrimas perduodamas ITPC informacijos saugos vadovui.

18. Apie tyrimo eigą, pateikdamas informaciją prie užregistruoto incidento aprašo incidentų žurnale adresu https://veiklos.vu.lt/projects/ITPC/issues, administratorius privalo informuoti ne vėliau, kaip darbo dienos pabaigoje.

19. Esant poreikiui tyrimo užduotis skirti kitų VU padalinių darbuotojams, atsakingo skyriaus vadovas kreipiasi į reikiamo padalinio vadovą.

20. Darbuotojams atlikus pavestas užduotis, atsakingo skyriaus vadovas pildo incidento tyrimo ataskaitą ir perduoda informaciją ITPC informacijos saugos vadovui.

21. Nekritinio incidento tyrimo išvadas saugos incidentų žurnale patvirtina ir tyrimą uždaro atsakingo skyriaus vadovas.

22. Nustatęs, kad incidentas yra kritinis, ITPC informacijos saugos vadovas gali sudaryti saugos incidento tyrimo grupę (toliau – Grupė).

23. Kritinių incidentų tyrimai Grupėje atliekami 24-31 punktuose nustatyta tvarka.

24. Jei incidentas kritinis, ne vėliau kaip kitą darbo dieną nuo saugos incidento įregistravimo, incidentą šalinančio padalinio vadovas kviečia Grupės pasitarimą.

25. Grupės sudėtis tvirtinama ITPC direktoriaus įsakymu ir atnaujinama esant poreikiui.

26. Grupei vadovauja ir apie tyrimų eigą ITPC direktorių bei susijusių IS duomenų valdymo įgaliotinius informuoja ITPC informacijos saugos vadovas.

27. Siekdamas nustatyti saugos incidento aplinkybes, priežastis ir asmenis, dėl kurių galbūt neteisėtų veiksmų įvyko saugos incidentas, ITPC informacijos saugos vadovas Grupės nariams skiria saugos incidento tyrimo užduotis.

28. Grupės nariai turi teisę:

28.1. apžiūrėti saugos incidento vietą ir įrangą;

28.2. peržiūrėti su incidentu susijusius sistemų įrašus;

28.3. apklausti su saugos incidentu galimai susijusius naudotojus;

28.4. susipažinti su saugos incidento tyrimui reikalingais dokumentais;

28.5. gauti kitą, su saugos incidentu susijusią, informaciją;

28.6. siūlyti administracines ir technines elektroninės informacijos saugos priemones;

28.7. dalyvauti IS veiklos tęstinumo atstatymo veiklose.

29. Grupės nariai privalo:

29.1. vadovaudamiesi surinkta tyrimo medžiaga, surašyti saugos incidento tyrimo išvadą, kurioje išdėstomos saugos incidento aplinkybės, priežastys ir jas pagrindžiantys įrodymai, taip pat nurodomi asmenys, dėl kurių veiklos galimai įvyko saugos incidentas;

29.2. savo kompetencijos ribose sudaryti rizikos mažinimo veiksmų planus;

29.3. bendradarbiauti su telekomunikacijų tinklų kibernetinės saugos atsako grupėmis (CERT, CSIRT);

29.4. bendradarbiauti su žalą likviduojančiomis specialiosiomis tarnybomis ir kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais;

29.5. ITPC vadovo nurodymu rengti IS veiklos atkūrimo detaliojo plano ar IS saugą įgyvendinančių dokumentų pakeitimo ar papildymo projektus.

30. Gavęs Aprašo 12.5 punkte įvardintą kritinio incidento tyrimo medžiagą, ITPC informacijos saugos vadovas pateikia JIRA sistemoje apibendrinančią išvadą, pildo kritinių incidentų registravimo žurnalą (ITPC veiklos tęstinumo valdymo plano 2 priedas).

31. Tyrimo Grupei atlikus skirtas užduotis, ITPC informacijos saugos vadovas registruoja kritinio incidento tyrimo ataskaitą DVS „Avilyje“ ir informuoja ITPC direktorių bei tyrimo dalyvius.

IV. BAIGIAMOSIOS NUOSTATOS

32. Jei nustatyti darbuotojai ar studentai, dėl kurių nederamo veikimo arba neveikimo įvyko incidentas, šie asmenys privalo pateikti VU ITPC adresuotą aplinkybių, kuriomis įtakojo incidentą, paaiškinimą.

33. Darbuotojų galimai padaryti pažeidimai nagrinėjami 2017 spalio 13 d. Vilniaus universiteto kanclerio įsakymu Nr. 447 „Dėl Vilniaus universiteto darbuotojų darbo pareigų pažeidimų nagrinėjimo tvarkos aprašo tvirtinimo“ nustatyta tvarka.

34. Studentų galimai padaryti pažeidimai nagrinėjami Vilniaus universiteto studijų nuostatuose, patvirtintuose Vilniaus universiteto Senato komisijos 2012 m. birželio 21 d. nutarimu Nr. SK-2012-12-8 (Vilniaus universiteto senato 2018 m. gegužės 22 d. nutarimo Nr. S-2018-5-2 redakcija) ir susijusiose teisės aktuose nustatyta tvarka.

35. Apie darbuotojų galimai padarytus pažeidimus informuojami jų tiesioginiai vadovai, apie studentų ir klausytojų padarytus pažeidimus, informuojami atitinkamų kamieninių padalinių vadovai, apie kitų sutartinių santykių turinčių asmenų galimai padarytus pažeidimus informuojami sutartis sudariusių Universiteto padalinių vadovai.

36. Apie asmenų galimai padarytus pažeidimus, kai už juos Lietuvos Respublikos teisės aktuose numatyta atsakomybė, informuojamos institucijos pagal kompetenciją.

37. Šio Aprašo nurodyta tvarka priimti incidentą sprendžiančių darbuotojų, tyrimą vykdančių vadovų ir ITPC direktoriaus sprendimai laikomi priimtais nuo paskelbimo ir privalo būti dokumentuoti IT Pagalbos sistemoje.

38. Saugos incidentų tyrimo medžiaga saugoma ne trumpiau kaip 1 metus nekritiniams ir 3 metus kritiniams incidentams nuo saugos incidento registracijos dienos.

_____