**VILNIAUS UNIVERSITETO**
**REKTORIUS**

# ĮSAKYMAS
# DĖL VILNIAUS UNIVERSITETO REKTORIAUS 2015 M. GEGUŽĖS 4 D. ĮSAKYMO NR. R-169 „DĖL AUKŠTŲJŲ MOKYKLŲ STUDENTŲ IR ABSOLVENTŲ KARJEROS VALDYMO INFORMACINĖS SISTEMOS SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ PATVIRTINIMO“ PAKEITIMO

2019 m. gruodžio d. Nr. R-
Vilnius

Vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 30 straipsnio 2 ir 3 dalimis, 43 straipsnio 2 dalimi, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ 7 ir 8 punktais,

p a k e i č i u Vilniaus universiteto rektoriaus 2015 m. gegužės 4 d. įsakymu Nr. R-169 „Dėl Aukštųjų mokyklų studentų ir absolventų karjeros valdymo informacinės sistemos saugos politiką įgyvendinančių dokumentų patvirtinimo“:

1. Pakeičiu nurodytuoju įsakymu patvirtintas Saugaus elektroninės informacijos tvarkymo taisykles ir išdėstau jas nauja redakcija (pridedama);
2. Pakeičiu nurodytuoju įsakymu patvirtintą Veiklos tęstinumo valdymo planą ir išdėstau jį nauja redakcija (pridedama);
3. Pakeičiu nurodytuoju įsakymu patvirtintas Naudotojų administravimo taisykles ir išdėstau jas nauja redakcija (pridedama).

Rektorius prof. Artūras Žukauskas

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie KAM
2019-08-30 raštu Nr. (4.2 E) 6K-564

Parengė:
Vilniaus universiteto Informacinių technologijų paslaugų centro
informacijos saugos vadovas
Viktoras Bulavas

Aukštųjų mokyklų studentų ir absolventų
karjeros valdymo informacinės sistemos
veiklos tęstinumo valdymo plano
2 priedas

# AUKŠTŲJŲ MOKYKLŲ STUDENTŲ IR ABSOLVENTŲ KARJEROS VALDYMO INFORMACINĖS SISTEMOS ELEKTRONINĖS INFORMACIJOS SAUGOS IR KIBERNETINIŲ INCIDENTŲ VALDYMO TVARKOS APRAŠAS

## I SKYRIUS
## BENDROSIOS NUOSTATOS

1. Aukštųjų mokyklų studentų ir absolventų karjeros valdymo informacinės sistemos elektroninės informacijos saugos ir kibernetinių incidentų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja Aukštųjų mokyklų studentų ir absolventų karjeros valdymo informacinės sistemos (toliau – informacinė sistema) naudotojų, valdytojo ir tvarkytojo darbuotojų veiksmus, įvykus elektroninės informacijos saugos ir kibernetiniams incidentams (toliau – saugos incidentai) ir jų sprendimo bei tyrimo tvarką.

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

2. Informacinės sistemos naudotojas apie saugos incidentus darbo valandomis nedelsdamas praneša informacinės sistemos tvarkytojui IT pagalbos telefonu (8 5) 236 6200 ir elektroniniu paštu pagalba@itpc.vu.lt ne darbo valandomis.

3. IT pagalbos konsultantas pranešimą apie saugos incidentą registruoja IT pagalbos informacinės sistemos skiltyje „Saugos incidentai“ ir priskiria pagrindiniam informacinės sistemos administratoriui spręsti, informacinės sistemos priežiūrą vykdančio padalinio vadovui ir informacinės sistemos saugos įgaliotiniui stebėti.

4. Pagrindinis informacinės sistemos administratorius įvykus saugos incidentui:

4.1. atsižvelgdamas į incidento kategoriją informuoja kitus atsakingus asmenis (duomenų valdymo ir saugos įgaliotinius, IT pagalbos tarnybą, savo tiesioginį vadovą);

4.2. kartu su kitais administratoriais vykdo saugos incidento plėtros stabdymo veiksmus;

4.3. jei kitaip nenuspręsta, organizuoja veiklos atstatymo po saugos incidento veiką;

4.4. padedamas kitų administratorių, renka medžiagą saugos incidentui tirti;

4.5. informuoja atsakingus asmenis apie veiklos atstatymo eigą;

4.6. pagal poreikį perkvalifikuoja incidentą arba eskaluoja saugos incidento kategoriją;

4.7. išsprendus saugos incidentą, rengia rizikos mažinimo prevencinių priemonių planą;

4.8. vykdo įgaliotų asmenų nurodymus;

4.9. registruoja informaciją apie saugos incidento aplinkybes ir jo sprendimą IT pagalbos informacinėje sistemoje (prie pranešimo apie incidentą);

4.10. išsprendus saugos incidentą, pateikia išvadą tiesioginiam vadovui ir saugos įgaliotiniui žiniai;

4.11. priėmus sprendimą saugos incidentą uždaryti, administratorius informuoja pranešusį naudotoją apie sprendimą.

5. informacinės sistemos saugos įgaliotinis:

5.1. patvirtina saugos incidento kategoriją;

5.2. stebi saugos incidento šalinimą;

5.3. organizuoja saugos incidento tyrimą;

5.4. teikia privalomus vykdyti nurodymus sistemos ir infrastruktūros priežiūrą vykdantiems administratoriams ir tvarkytojo incidentų reagavimo grupei (toliau – CERT) dėl tyrimui reikalingos medžiagos pateikimo;

5.5. renka tyrimui reikalingą medžiagą;

5.6. bendradarbiauja su tvarkytojo ir kitų institucijų saugos incidentų tyrimo grupėmis ir kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos ir kibernetinius incidentus bei neteisėtas veiklas;

5.7. informuoja informacinės sistemos duomenų valdymo įgaliotinį apie saugos incidento tyrimo eigą;

5.8. teikia duomenų valdymo įgaliotiniui išvadą dėl prevencinių priemonių plano pakankamumo;

5.9. incidentų registracijos informacinėje sistemoje pateikia tyrimo metu nustatytą informaciją ir uždaro saugos incidentą, kai šis išsprendžiamas;

5.10. konsultuoja kitus tiriant saugos incidentus administratorius ir vidinius naudotojus.

6. Įtaręs neteisėtą veiklą, pažeidžiančią ar neišvengiamai pažeisiančią informacinės sistemos saugą, saugos įgaliotinis apie tai praneša informacinės sistemos duomenų valdymo įgaliotiniui ir kompetentingoms institucijoms, tiriančioms elektroninių ryšių tinklų, informacijos saugumo ir kibernetinius incidentus, neteisėtas veiklas, susijusias su elektroninės informacijos saugos incidentais.

## III SKYRIUS
## SAUGOS INCIDENTŲ TYRIMAS

7. Nereikšmingo poveikio saugos incidentų tyrimai neatliekami ir analizė Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos neteikiama. Tokiu atveju informacinės sistemos administratorius registruoja informaciją apie saugos incidento aplinkybes ir jo sprendimą IT pagalbos sistemos skiltyje „Saugos incidentai“ ir pateikia su išvada pagrindiniam administratoriui bei saugos įgaliotiniui žiniai.

8. Nereikšmingo poveikio saugos incidentų sprendimą sistemoje užbaigia tiesioginis padalinio, prižiūrinčio informacinę sistemą arba incidento paveiktą informacinei sistemai veikti būtiną infrastruktūrą, vadovas.

9. Saugos įgaliotinis turi teisę priimti sprendimą tirti sprendžiamą arba papildomai tirti jau išspręstą nereikšmingo poveikio saugos incidentą.

10. Saugos įgaliotinis, nustatęs aplinkybes, dėl kurių saugos incidentas gali turėti didesnių, nei manyta, padarinių, arba nustatęs, kad saugos incidento padariniai neatitinka numatytų kriterijų, turi teisę perkvalifikuoti saugos incidentą į kitą kategoriją.

11. Vidutinio ir didesnio poveikio saugos incidentų tyrimas:

11.1. Tiriant informacinės sistemos saugos incidentus, saugos įgaliotinis turi teisę gauti informaciją iš visų veiklos tęstinumo atstatyme dalyvavusių ir kitų galinčių turėti reikiamos informacijos darbuotojų bei incidentų reagavimo grupės (CERT).

11.2. Saugos incidentams tirti gali būti sudaromos specializuotos saugos incidentų tyrimo grupės (toliau – Tyrimo grupė).

11.3. Tyrimo grupės narius, saugos įgaliotinio siūlymu, skiria priežiūrą vykdančių padalinių vadovai arba tvarkytojo vadovas.

11.4. Tyrimo grupei vadovauja informacinės sistemos saugos įgaliotinis.

12. Siekdamas nustatyti saugos incidento aplinkybes, priežastis ir asmenis, dėl kurių galbūt neteisėtų veiksmų įvyko saugos incidentas, saugos įgaliotinis Tyrimo grupės nariams skiria saugos incidento tyrimo užduotis.

13. Tyrimo grupės nariai turi teisę:

13.1. apžiūrėti saugos incidento vietą;

13.2. apklausti su saugos incidentu galimai susijusius naudotojus;

13.3. susipažinti su saugos incidento tyrimui reikalingais dokumentais;

13.4. priimti sprendimą dėl saugos incidento kategorijos keitimo;

13.5. priima sprendimą dėl saugos incidento rizikos mažinimo plano tinkamumo;

13.6. gauti kitą, su saugos incidentu susijusią, informaciją.

14. Tyrimo grupės funkcijos ir atsakomybės:

14.1. vadovaudamasi informacinės sistemos duomenų saugos nuostatais ir kitais saugos dokumentais pagal savo kompetenciją tiria incidentą;

14.2. vadovaudamasi surinkta tyrimo medžiaga, surašo saugos incidento tyrimo išvadą, kurioje išdėsto saugos incidento aplinkybes ir jas pagrindžiančius faktus, taip pat nurodo asmenis, dėl kurių veiklos galimai įvyko saugos incidentas, ir šiuos duomenis teikia informacinės sistemos duomenų valdymo įgaliotiniui;

14.3. įtariant nusikalstamos veiklos požymių, priima sprendimą dėl atsakingos institucijos informavimo;

14.4. tyrimo grupės vadovo sprendimu bendradarbiauja su žalą likviduojančiomis specialiosiomis tarnybomis ir kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo ir kibernetinius incidentus, neteisėtas veiklas, susijusias su saugos incidentais;

14.5. atsižvelgdama į saugos incidento padarinius, atlieka liekamosios rizikos vertinimą;

14.6. atsižvelgdama į saugos incidento priežastis ir jo padarinius, prireikus nedelsdama rengia veiklos atkūrimo detaliojo plano ar saugą įgyvendinančių dokumentų pakeitimo ar papildymo projektą.

15. Tyrimo ataskaitoje turi būti pateikta bent ši informacija: incidento vieta, grėsmės kodas, incidento aprašymas, pradžia (data ir laikas), pabaiga (data ir laikas), tyrimą vykdžiusių darbuotojų duomenys.

16. Surinkęs tyrimo medžiagą, saugos įgaliotinis pateikia apibendrinančią išvadą ir priima sprendimą dėl incidento tyrimo pabaigos.

17. Saugos incidento tyrimo ataskaita registruojama dokumentų valdymo sistemoje, tyrimo medžiaga ir tyrimų ataskaitos pateikiami pagrindiniam tvarkytojui ir nustatyta tvarka Nacionaliniam kibernetinio saugumo centrui.

18. Tyrimo ataskaita ir medžiaga yra konfidenciali ir suteikiama tik turintiems teisę susipažinti su informacija asmenims, taip pat atitikties ir rizikos vertinimams vykdyti, bei kitais LR įstatymų numatytais atvejais.

19. Saugos incidentų žurnalo ir tyrimų medžiaga saugoma ne trumpiau kaip 1 metus nereikšmingo bei vidutinio poveikio saugos incidentams ir 3 metus didelio poveikio bei pavojingiems saugos incidentams, po ko gali būti naikinama per 3 mėnesius pasibaigus kalendoriniams saugojimo termino metams.

## IV SKYRIUS
## BAIGIAMOSIOS NUOSTATOS

20. Ši tvarka skelbiama ta pačia tvarka, kaip ir kiti informacinės sistemos dokumentai.

21. Asmenys, dėl kurių neteisėtų veiksmų ar neveikimo įvyko saugos incidentas, atsako teisės aktų nustatyta tvarka.

_____

| DETALŪS METADUOMENYS | |
|---|---|
| **Dokumento sudarytojas (-ai)** | Vilniaus universitetas 211950810, Universiteto g. 3, 01513 Vilnius |
| **Dokumento pavadinimas (antraštė)** | DĖL VILNIAUS UNIVERSITETO REKTORIAUS 2015 M. GEGUŽĖS 4 D. ĮSAKYMO NR. R-169 „DĖL AUKŠTŲJŲ MOKYKLŲ STUDENTŲ IR ABSOLVENTŲ KARJEROS VALDYMO INFORMACINĖS SISTEMOS SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ PATVIRTINIMO“ PAKEITIMO |
| **Dokumento registracijos data ir numeris** | 2019-12-09 Nr. R-621 |
| **Dokumento gavimo data ir dokumento gavimo registracijos numeris** | – |
| **Dokumento specifikacijos identifikavimo žymuo** | ADOC-V1.0 |
| **Parašo paskirtis** | Vizavimas |
| **Parašą sukūrusio asmens vardas, pavardė ir pareigos** | Arūnas Stašionis, Direktorius, Informacinių technologijų paslaugų centras |
| **Sertifikatas išduotas** | ARŪNAS,STAŠIONIS LT |
| **Parašo sukūrimo data ir laikas** | 2019-12-09 12:22:34 (GMT+02:00) |
| **Parašo formatas** | XAdES-EPES |
| **Laiko žymoje nurodytas laikas** | – |
| **Informacija apie sertifikavimo paslaugų teikėją** | EID-SK 2016, AS Sertifitseerimiskeskus EE |
| **Sertifikato galiojimo laikas** | 2019-01-23 12:56:45 – 2024-01-22 23:59:59 |
| **Parašo paskirtis** | Pasirašymas |
| **Parašą sukūrusio asmens vardas, pavardė ir pareigos** | Artūras Žukauskas, Rektorius, Centrinė administracija |
| **Sertifikatas išduotas** | ARTŪRAS,ŽUKAUSKAS LT |
| **Parašo sukūrimo data ir laikas** | 2019-12-09 16:05:13 (GMT+02:00) |
| **Parašo formatas** | XAdES-T |
| **Laiko žymoje nurodytas laikas** | 2019-12-09 16:05:31 (GMT+02:00) |
| **Informacija apie sertifikavimo paslaugų teikėją** | EID-SK 2016, AS Sertifitseerimiskeskus EE |
| **Sertifikato galiojimo laikas** | 2019-08-12 11:16:51 – 2024-08-10 23:59:59 |
| **Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti** | "Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA, VI Registru centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Vilniaus universitetas, į.k. 211950810 LT", sertifikatas galioja nuo 2018-12-27 14:18:54 iki 2021-12-26 14:18:54 |
| **Pagrindinio dokumento priedų skaičius** | 2 |
| **Pagrindinio dokumento pridedamų dokumentų skaičius** | – |
| **Pridedamo dokumento sudarytojas (-ai)** | – |
| **Pridedamo dokumento pavadinimas (antraštė)** | – |
| **Pridedamo dokumento registracijos data ir numeris** | – |
| **Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas** | Dokumentų valdymo sistema Avilys, versija 3.5.13 |
| **Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)** | Atitinka specifikacijos keliamus reikalavimus.<br>Visi dokumente esantys elektroniniai parašai galioja (2019-12-09 16:11:15) |
| **Paieškos nuoroda** | – |
| **Papildomi metaduomenys** | Nuorašą suformavo 2019-12-09 16:11:15 Dokumentų valdymo sistema Avilys |