

PATVIRTINTA:

Vilniaus universiteto Rektoriaus

2015 m. spalio 6 d. įsakymu Nr. R-411

## **NACIONALINIO ATVIROS PRIEIGOS MOKSLINIŲ TYRIMŲ DUOMENŲ ARCHYVO INFORMACINĖS SISTEMOS ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ TYRIMO TVARKOS APRAŠAS**

### **I. BENDROSIOS NUOSTATOS**

1. Nacionalinio atviros prieigos mokslinių tyrimų duomenų archyvo informacinės sistemos elektroninės informacijos saugos incidentų tyrimo tvarkos aprašas (toliau – aprašas) reglamentuoja Nacionalinio atviros prieigos mokslinių tyrimų duomenų archyvo informacinės sistemos (toliau – MIDAS) elektroninės informacijos saugos incidentų (toliau – saugos incidentai) tyrimo tvarką.

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

2. MIDAS naudotojas apie saugos incidentus nedelsdamas praneša MIDAS pagrindiniam tvarkytojui IT pagalbos telefonu 6200 darbo valandomis ir elektroniniu paštu [pagalba@vu.lt](mailto:pagalba@vu.lt) nedarbo valandomis.

3. Gautas pranešimas apie saugos incidentą registruojamas adresu [pagalba.vu.lt](http://pagalba.vu.lt) skiltyje MIDAS incidentai ir priskiriamas tyrimui MIDAS saugos įgaliotiniui ir MIDAS sisteminiam administratoriui.

4. Saugos įgaliotinis su sisteminiu administratoriumi nagrinėja ir klasifikuoja incidentą bei priima sprendimą dėl incidento kritiškumo.

5. MIDAS sisteminis administratorius, suderinęs su MIDAS saugos įgaliotiniu, atlieka neatidėliotinus MIDAS administravimo veiksmus, skirtus saugos incidento plėtrai sustabdyti ir tyrimui būtinai informacijai surinkti.

6. Jeigu nustatyta, kad incidentas kritinis, informuoja MIDAS veiklos tęstinumo valdymo grupės vadovą.

7. Jei incidentas kritinis, MIDAS veiklos tęstinumo valdymo grupės vadovas, priima sprendimą dėl tolimesnių veiksmų pagal MIDAS veiklos tęstinumo planą.

### **III. SAUGOS INCIDENTŲ TYRIMAS**

8. Jei incidentas nekritinis, saugos incidento tyrimą atlieka MIDAS administratorius ir apie jo rezultatus raštu kitą dieną informuoja MIDAS saugos įgaliotinį registruodamas juos MIDAS incidento skiltyje adresu [pagalba.vu.lt](http://pagalba.vu.lt). Gavęs tyrimo rezultatus MIDAS saugos įgaliotinis pateikia sistemoje apibendrinančią išvadą bei poreikiui esant, skiria užduotis kitiems darbuotojams. Atlikus tas užduotis MIDAS saugos įgaliotinis uždaro tyrimą.

9. Kritinio incidento tyrimas atliekamas aprašo 10-15 punktuose nustatyta tvarka.

10. Jei incidentas kritinis, ne vėliau kaip kitą darbo dieną nuo saugos incidento įregistravimo, MIDAS saugos įgaliotinis kviečia MIDAS elektroninių incidentų tyrimo grupės (toliau – Tyrimo grupė) posėdį.

11. Tyrimo grupės vardinė sudėtis tvirtinama ITTC direktoriaus įsakymu ir atnaujinama esant poreikiui.

12. Tyrimo grupei vadovauja MIDAS saugos įgaliotinis.

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

14. Tyrimo grupės nariai turi teisę:

14.1. apžiūrėti saugos incidento vietą;

14.2. apklausti su saugos incidentu galimai susijusius MIDAS naudotojus;

14.3. susipažinti su saugos incidento tyrimui reikalingais dokumentais;

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

15. Tyrimo grupės nariai informaciją apie užduoties įvykdymo rezultatus raštu teikia MIDAS saugos įgaliotiniui ir MIDAS veiklos tęstinumo valdymo grupės vadovui.

16. Tyrimo grupė:

16.1. vadovaudamasi surinkta tyrimo medžiaga, surašo saugos incidento tyrimo išvadą, kurioje išdėsto saugos incidento aplinkybes, priežastis ir jas pagrindžiančius įrodymus, taip pat nurodo asmenis, dėl kurių neteisėtos veiklos įvyko saugos incidentas, ir šiuos duomenis teikia MIDAS duomenų įgaliotiniui ir kitiems MIDAS tvarkytojams, susijusiems su saugos incidentu;

16.2. vadovaudamasi MIDAS duomenų saugos nuostatais ir kitais saugos dokumentais savo kompetencijos ribose dalyvauja MIDAS veiklos tęstinumo atstatymo veiklose;

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

17. Gavęs tyrimo rezultatus MIDAS saugos įgaliotinis pateikia sistemoje apibendrinančią išvadą bei poreikiui esant, skiria užduotis kitiems darbuotojams. Atlikus tas užduotis MIDAS saugos įgaliotinis uždaro tyrimą.

#### IV. BAIGIAMOSIOS NUOSTATOS

18. Saugos incidentų tyrimo medžiaga saugoma 5 metus nuo saugos incidento registracijos dienos.

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

---