PATVIRTINTA
Lietuvos Respublikos
akademinės etikos ir procedūrų kontrolieriaus
2019 m. spalio 3 d. įsakymu Nr. V-27

INFORMACIJOS SAUGOS INCIDENTŲ VALDYMO TVARKOS LIETUVOS RESPUBLIKOS AKADEMINĖS ETIKOS IR PROCEDŪRŲ KONTROLIERIAUS TARNYBOJE APRAŠAS

I. BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos akademinės etikos ir procedūrų kontrolieriaus tarnybos informacijos saugos incidentų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja informacijos saugos incidentų valdymo tvarką Akademinės etikos ir procedūrų kontrolieriaus tarnyboje (toliau – Tarnyba), siekiant užtikrinti Tarnybos disponuojamos informacijos saugumą.

2. Aprašas yra privalomas Tarnybos valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau – Tarnybos darbuotojas), studentams, atliekantiems praktiką Tarnyboje, ir tyrėjams, kurie mokslinių tyrimų tikslais naudoja Tarnybos skundų ir tyrimų medžiagą (toliau – tyrėjai).

3. Tiekėjams ir susijusioms šalims taikomas Aprašo 3 skyrius (Pranešimų teikimo apie informacijos saugumo įvykius tvarka). Šio skyriaus nuostatos privalo būti pateikiamos tiekėjams ir susijusioms šalims kaip priedas prie sutarties.

4. Apraše vartojamos sąvokos:

Informacijos saugumas – apima informacijos konfidencialumo, vientisumo ir pasiekiamumo išsaugojimą.

Informacijos saugos įgaliotinis – Lietuvos Respublikos akademinės etikos ir procedūrų kontrolieriaus (toliau – kontrolierius) įsakymu paskirtas vyriausiasis specialistas (informatikas), kuris yra atsakingas už informacijos saugumo valdymo Tarnyboje įgyvendinimą ir palaikymą.

Informacijos saugumo įvykis – nustatytas sistemos, Tarnybos ar tinklo įvykis, rodantis galimą informacijos saugumo politikos spragą ar informacijos saugumo priemonių sutrikimą arba anksčiau nenumatytos situacijos, kuri gali būti susijusi su informacijos saugumu, atsiradimą.

Informacijos saugos incidentas – vienas ar daugiau nepageidaujamų ir netikėtų informacijos saugumo įvykių, turinčių didelę tikimybę pakenkti Tarnybos veiklai ir keliančių grėsmę informacijos saugumui.

IS – informacinė sistema.

Naudotojas – Tarnybos darbuotojas, tiekėjas ir susijusios šalys, studentas, atliekantis praktiką Tarnyboje, ir tyrėjas.

II. FUNKCIJOS IR ATSAKOMYBĖS

5. Už informacijos saugumo įvykių / informacijos saugos incidentų valdymą Tarnyboje atsakingi šie Tarnybos darbuotojai:

5.1. Informacijos saugos įgaliotinis:

5.1.1. įvertina užregistruotus informacijos saugumo įvykius;

5.1.2. tiria informacijos saugos incidentus;

5.1.3. analizuoja informacijos saugos incidentų tyrimo metu nustatytą ir / ar iš Tarnybos darbuotojų gautą informaciją apie informacijos saugumo įvykius;

5.1.4. teikia rekomendacijas ir metodinę pagalbą informacijos saugumo gerinimui Tarnyboje;

5.1.5. užtikrina, kad informacijos saugos incidentų valdymo tvarka būtų gerai žinoma Tarnybos darbuotojams.

6. Informacijos saugos įgaliotinio laikino nebuvimo darbe metu jį pavaduoja kontrolieriaus įsakymu paskirtas Tarnybos asmens duomenų apsaugos pareigūnas.

7. Naudotojai yra atsakingi už jiems nustatytos pareigos – pranešti apie bet kokį informacijos saugumo įvykį – tikslų vykdymą. Teisinė atsakomybė naudotojams taikoma individualiai – laikantis

bendrų teisinės atsakomybės skyrimo principų: priklausomai nuo vykdomų funkcijų, padarytos žalos dydžio bei masto.

8. Naudotojai privalo teikti informacijos saugos įgaliotiniui visą su informacijos saugumo įvykiais ir incidentais susijusią informaciją kaip galima greičiau nuo jų atsiradimo momento.

III. PRANEŠIMŲ TEIKIMO APIE INFORMACIJOS SAUGUMO ĮVYKIUS TVARKA

9. Naudotojai, pastebėję informacijos saugumo įvykius ar informacijos saugumo silpnąsias vietas, privalo nedelsiant pranešti apie tai elektroniniu paštu informacijos saugos įgaliotiniui bei apie juos informuoti kontrolierių. Įvykiai, apie kuriuos reikia pranešti, gali būti tokie:

9.1. informacijos saugumo politikos ar reikalavimų pažeidimai;

9.2. techninės ir (ar) programinės įrangos sutrikimai ir (ar) netikėti apkrovos pasikeitimai dėl neaiškių priežasčių;

9.3. fizinės saugos priemonių pažeidimai;

9.4. vagystės;

9.5. pastebėti įtartini lankytojų veiksmai;

9.6. asmens duomenų saugumo pažeidimai;

9.7. kitų asmenų pranešimai apie galimą grėsmę ir informacijos saugumo pažeidimus, įskaitant ir anoniminius pranešimus;

9.8. kiti įvykiai, galintys turėti įtakos informacijos saugumui.

10. Pranešimus apie pastebėtus informacijos saugumo įvykius galima pateikti ir:

10.1. telefonu;

10.2. tiesiogiai žodžiu informacijos saugos įgaliotiniui jo darbo vietoje.

IV. INFORMACIJOS SAUGUMO ĮVYKIŲ IR INCIDENTŲ REGISTRAVIMAS

11. Informacijos saugos įgaliotinis, gavęs pranešimą arba pats pastebėjęs informacijos saugumo pažeidimą, užregistruoja jį informacijos saugumo įvykių ir incidentų registre, kuriame turi būti nurodyta data ir laikas, įvykio aprašymas, sprendimas ar įvykis priskiriamas informacijos saugumo incidentui, kategorija ir numatomas incidento išsprendimo laikas, tipas, atsakingas už incidento sprendimą asmuo, žalos aprašymas, įvykio priežastis, incidento sprendimo aprašymas, informacija apie įrodymus (jei reikia), incidento išsprendimo data.

12. Informacijos saugos įgaliotinis nusprendžia, ar užregistruotas informacijos saugumo įvykis priskiriamas informacijos saugumo incidentui.

13. Informacijos saugumo įvykiai turi būti stebimi, o informacijos saugos incidentai – tiriami.

V. INFORMACIJOS SAUGOS INCIDENTŲ TYRIMO TVARKA

14. Gavęs pranešimą apie naują užregistruotą informacijos saugumo įvykį, informacijos saugos įgaliotinis atlieka pirminį informacijos saugumo įvykio įvertinimą. Pirminio įvertinimo metu nustatoma, ar informacijos saugumo įvykis yra informacijos saugos incidentas ir gali kelti grėsmę informacijos saugumui:

14.1. jei informacijos saugumo įvykis negali kelti grėsmės informacijos saugumui, fiksuojama, kad buvo gautas pranešimas apie informacijos saugumo įvykį, bet informacijos saugumo įvykio tyrimas neatliekamas. Apie informacijos saugos incidentą pranešęs naudotojas informuojamas apie informacijos saugumo įvykio tyrimo neatlikimą su komentaru;

14.2. jei informacijos saugumo įvykis gali kelti grėsmę informacijos saugumui, atliekamas antrinis įvertinimas.

15. Antrinio įvertinimo metu:

15.1. informacijos saugos įgaliotinis nustato informacijos saugos incidento tipą. Galimi keturi informacijos saugos incidentų tipai:

15.1.1. Elektroninės informacijos saugos incidentas – tai įvykis, veiksmas ar neveikimas, kuris sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie IS ar

elektroninių ryšių tinklo, sutrikdyti ar pakeisti (įskaitant valdymo perėmimą) IS ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, gali sudaryti sąlygas pasisavinti, paskelbti, platinti ar kitaip panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims;

15.1.2. Neelektroninės informacijos saugos incidentas – tai įvykis, veiksmas ar neveikimas, susijęs su kitų formų informacija (spausdintiniai, rašytiniai dokumentai ir jų kopijos ir t. t.). Taip pat tai įvykiai, susiję su fizine apsauga, kurie galėjo kilti Tarnyboje disponuojamos informacijos ar jos dalies praradimo bei sugadinimo rizika;

15.1.3. Kibernetinis incidentas – įvykis ar veikla, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie IS, sutrikdyti ar pakeisti IS veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją ar elektroninius duomenis panaikinti ar apriboti galimybę naudotis elektronine informacija ar elektroniniais duomenimis, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją ar elektroninius duomenis tokios teisės neturintiems asmenims.

15.1.4. Informacijos saugos incidentas, susijęs su asmens duomenų saugumo pažeidimu.

15.2. Informacijos saugos įgaliotinis informacijos saugos incidentą pagal kompetenciją sprendžia pats arba, atsižvelgdamas į informacijos saugos incidento tipą, pasitelkia reikiamus ekspertus, atlikti informacijos saugos incidentų tyrimą.

16. Atliekant informacijos saugos incidento tyrimą:

16.1. informacijos saugos incidentui priskiriama pavojingumo kategorija, pagal žemiau pateiktus kriterijus:

16.1.1. I kategorijos – kai informacijos saugos incidentas sukelia neigiamas pasekmes visai Tarnybai, kai dėl tokio informacijos saugos incidento gali sutrikti visų IS veikla;

16.1.2. II kategorijos – kai informacijos saugos incidentas kenkia vienai ar kelioms Tarnybos funkcijoms;

16.1.3. III kategorijos – kai informacijos saugos incidentas iš esmės nedaro įtakos Tarnybos veiklai arba su ja susijęs neženkliai;

17.2. Informacijos saugos įgaliotinis, atsižvelgdamas į informacijos saugos incidento kategoriją:

17.2.1. nusprendžia, kokia seka ir apimtimi vykdyti reagavimo į incidentą veiklas:

17.2.1.1. neatidėliotinus veiksmus;

17.2.1.2. faktinių aplinkybių (įrodymų) nustatymą;

17.2.1.3. komunikaciją;

17.2.2. užtikrina vykdomų operacijų atkūrimą ir išlaikymą:

17.2.2.1. reikiamu lygiu;

17.2.2.2. per atitinkamą laiko tarpą;

17.2.2.3. laikantis taikomų procedūrų, leidžiančių per reikiamą laiką atkurti ir atstatyti veiklos operacijas bei informacijos parengtumą;

17.2.2.4. nustatytu priimtinu informacijos ir paslaugų praradimo lygiu.

17.2.3. taiko atitinkamas priemones, apimančias:

17.2.3.1. incidento priežasties nustatymą ir analizę;

17.2.3.2. incidentų suvaldymą;

17.2.3.3. pataisos veiksmų planavimą ir įgyvendinimą, siekiant išvengti informacijos saugos incidento pasikartojimo;

17.2.3.4. ryšio palaikymą su asmenimis, kurių darbas susijęs su informacijos saugos incidentų sukeltų nesklandumų panaikinimu;

17.2.4. sprendžia, ar informacijos saugos incidentas yra valdomas.

18. Atlikus informacijos saugos incidento tyrimą, informacijos saugos įgaliotinis privalo informacijos saugumo įvykių ir incidentų registre įrašyti komentarą apie informacijos saugos incidento priežastis, priemones / veiksmus, kurių buvo imtasi, siekiant užkirsti kelią informacijos saugos incidentui pasikartoti ateityje.

19. Informacijos saugos įgaliotinis periodiškai, kartą per mėnesį peržiūri užregistruotus informacijos saugos incidentus.

20. Informacijos saugos incidentų analizės pagrindu informacijos saugos įgaliotinis gali inicijuoti neeilinį informacijos saugos rizikos vertinimą.

21. Incidentų analizės duomenys analizuojami ir iš jų mokomasi, siekiant sumažinti ateityje įvyksiančių informacijos saugos incidentų įtaką ir (ar) tikimybę.

VI. INFORMACIJOS APIE INFORMACIJOS SAUGOS INCIDENTUS SAUGOJIMAS IR ATASKAITŲ TEIKIMAS

22. Visi pranešimai apie informacijos saugumo įvykius ir informacijos saugos incidentus bei informacijos saugos incidentų tyrimo metu surinkta medžiaga saugoma Tarnybos dokumentų valdymo sistemoje.

23. Vieną kartą per metus, iki einamųjų metų rugsėjo 5 d., informacijos saugos įgaliotinis teikia kontrolieriui per praėjusį laiką nustatytų informacijos saugos incidentų apibendrintas ataskaitas su komentarais, apie tai, ar kartojasi informacijos saugos incidentai, ar kartojasi jų atsiradimo priežastys bei siūlymais, kaip mažinti galimų informacijos saugos incidentų atsiradimo riziką, apsvarstant galimybę tam skirti papildomus išteklius.

VII. BAIGIAMOSIOS NUOSTATOS

24. Aprašas tikrinamas ir peržiūrimas pagal poreikį (po rizikos analizės ar informacinių technologijų saugumo atitikties vertinimo atlikimo arba įvykus esminiams organizaciniams, sisteminiams ar kitiems informacinės sistemos pokyčiams), bet ne rečiau kaip vieną kartą per kalendorinius metus.