Nidos kultūros ir turizmo informacijos centras „Agila“ (Kodas 190895966)

PATVIRTINTA
Nidos kultūros ir turizmo informacijos centro „Agila“ Direktorės
2022 m. lapkričio 18 d. įsakymu
Nr. V-14

SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nidos kultūros ir turizmo informacijos centras „Agila“ (toliau – Įstaiga) saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Taisyklės) tikslas – nustatyti tvarką, užtikrinančią saugų Įstaigos informacinių sistemų techninės, programinės įrangos funkcionavimą, saugų duomenų tvarkymą ir jų teikimą kitoms institucijoms pagal teisės aktų nustatytus reikalavimus.

2. Taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716.

3. Šios Taisyklės yra privalomos visiems Įstaigos darbuotojams, dirbantiems pagal darbo sutartį, naudojantiems kompiuterinę įrangą darbo bei mokslo užduotims atlikti.

4. Šiose Taisyklėse vartojamos sąvokos:

4.1. **Įstaigos informacinės sistemos** (toliau – Informacinės sistemos) – informacinių technologijų pagrindu veikiančios sistemos, užtikrinančios kompiuterizuotą Įstaigos duomenų, dokumentų ir kitos informacijos kūrimą, tvarkymą ir saugojimą, tenkinančios kitus Įstaigos informacinius poreikius. Informacines sistemas sudaro techninė įranga (tarnybinės stotys, darbo vietų kompiuteriai, duomenų saugyklos, kompiuterių tinklo ir elektroninio ryšio priemonės, duomenų apsaugos priemonės), programinė įranga (operacinės sistemos, pagalbinės programos, taikomosios programinės įrangos), kompiuterizuotai tvarkoma Įstaigos veiklos informacija (elektroniniai dokumentai, įvairūs duomenys, duomenų bazės) ir kita informacija;

4.2. **Informacinių sistemų saugos įgaliotinis** (toliau – Saugos įgaliotinis) **–** Įstaigos vadovo paskirtas darbuotojas, dirbantis pagal darbo sutartį, įgyvendinantis elektroninės informacijos saugą Įstaigos Informacinėse sistemose;

4.3. **Informacinių sistemų administratorius** (toliau – Administratorius) – Įstaigos darbuotojas, dirbantis pagal darbo sutartį, atliekantis Informacinių sistemų priežiūrą;

4.4. **Informacinių sistemų naudotojas** (toliau – Naudotojas) – Įstaigos darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis Informacinių sistemų ištekliais numatytoms funkcijoms atlikti.

5. Kitos Taisyklėse vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimus, Saugos dokumentų turinio gaires ir Elektroninės

informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gaires patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 ir kituose Lietuvos Respublikos teisės aktuose vartojamas sąvokas.

6. Už Informacinių sistemų duomenų saugų tvarkymą atsakingi Informacinių sistemų naudotojai, Informacinių sistemų Administratorius.

7. Už Taisyklių įgyvendinimo organizavimą ir kontrolę atsakingas Saugos įgaliotinis.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

8. Saugiam elektroninės informacijos tvarkymui užtikrinti naudojamos kompiuterinės įrangos, programinės įrangos, fizinės, techninės ir organizacinės duomenų saugos priemonės.

9. Prieiga prie Informacinių sistemų suteikiama tik autorizuotiems Naudotojams. Kiekvienas Naudotojas Informacinėje sistemoje turi patvirtinti savo tapatybę vardu ir slaptažodžiu. Slaptažodžiai negali būti atskleidžiami kitiems asmenims.

10. Prieiga Naudotojams suteikiama tik prie tų išteklių, kurie yra būtini tiesioginėms pareigoms vykdyti.

11. Naudojama legali sisteminė ir taikomoji programinė įranga.

12. Programinės įrangos diegimą atlieka tik Informacinių sistemų administratoriai ar kiti įgalioti asmenys.

13. Naudojamos antivirusinės programos naudotojų kompiuteriuose, antivirusinės programos elektroninio pašto tarnybinėje stotyje, programinės ugniasienės naudotojų kompiuteriuose ir tinklo tarnybinėse stotyse apsaugai nuo virusų, šnipinėjimui skirtos programinės įrangos, nepageidaujamo elektroninio pašto ir pan.

14. Siekiant apsaugoti nuo žalingos programinės įrangos, ne rečiau kaip kartą per mėnesį turi būti atliekamas nuolatinis naudotojų ir tarnybinių stočių operacinių sistemų atnaujinimas.

15. Antivirusinių programų duomenų bazės turi būti atnaujinamos periodiškai – ne rečiau kaip kartą per dieną, jei atnaujinimą pateikia antivirusinės programos gamintojas.

16. Ne rečiau kaip kartą per metus Administratorius atlieka patikrinimą, siekdamas nustatyti, ar informacinėje sistemoje naudojama legali programinė įranga. Patikrinimą inicijuoja Saugos įgaliotinis.

17. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacijų tinklų naudojant ugniasienę.

18. Už tinklo ugniasienių administravimą, priežiūrą, operacinės sistemos atnaujinimą ir saugią ugniasienių konfigūraciją atsako Administratorius.

19. Naudotojams kompiuterių operacinėse sistemose turi būti suteikiamos teisės, kurios būtinos tiesioginėms pareigoms vykdyti.

20. Duomenys nuo jų praradimo, iškraipymo, sunaikinimo, neteisėto panaudojimo galimybių apsaugomi techninėmis, organizacinėmis, programinėmis priemonėmis.

21. Fizinė prieiga prie Informacinių sistemų tarnybinių stočių suteikiama tik informacinių technologijų darbuotojams.

22. Patalpa, kurioje veikia tarnybinės stotys atitinka priešgaisrinės saugos reikalavimus, jose yra gaisro gesinimo priemonės. Periodiškai atliekama gaisro gesinimo priemonių patikra.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

23. Informacinių sistemų duomenų keitimą, atnaujinimą ir naujų duomenų įvedimą turi teisę atlikti tik autorizuoti naudotojai, turintys teisę tai atlikti.

24. Naudotojų tapatybė ir veiksmai su Informacinių sistemų duomenimis fiksuojami programinėmis priemonėmis.

25. Už Informacinių sistemų duomenų atsarginių duomenų kopijų darymą, saugojimą ir duomenų atkūrimą iš atsarginių duomenų kopijų atsako Administratorius.

26. Atsarginės duomenų kopijos daromos kasdien, o darbo stočių duomenų kopijos daromos individualiai pagal poreikį.

27. Prarasti, iškraipyti ar sunaikinti Informacinių sistemų duomenys atkuriami iš atsarginių duomenų kopijų.

28. Duomenų atstatymas iš atsarginių kopijų turi būti periodiškai išbandomas – ne rečiau kaip kartą per metus.

29. Atstatymų išbandymą inicijuoja Saugos įgaliotinis.

30. Duomenų perkėlimo ir teikimo kitoms Informacinėms sistemoms bei duomenų gavimo iš jų tvarka nustatoma atskiromis sutartimis.

31. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarką, priklausomai nuo konkretaus atvejo, derina Administratorius.

32. Operacinių sistemų ir taikomosios programinės įrangos keitimai turi būti valdomi: planuojami ir ištestuojami, numatomos atstatomosios procedūros nesėkmingų keitimų atvejams, įvertinamas keitimų poveikis saugumui.

33. Už operacinių sistemų ir taikomosios programinės įrangos keitimų valdymą atsakingas Informacinių sistemų administratorius.

34. Administratorius, užtikrindamas Informacinių sistemų duomenų vientisumą, privalo naudoti visas įmanomas fizines, programines ir organizacines priemones, skirtas Informacinei sistemai ir joje tvarkomiems duomenims apsaugoti nuo neteisėtų veiksmų.

35. Naudotojas, įtaręs, kad su Informacinių sistemų duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai Administratoriui. Administratorius, įtaręs, kad su Informacinių sistemų duomenimis vykdomi neteisėti veiksmai, privalo apie tai pranešti Saugos įgaliotiniui. Saugos įgaliotinis, gavęs pranešimą apie vykdomus neteisėtus veiksmus su Informacinėmis sistemomis arba su Informacinių sistemų tvarkomais duomenimis, inicijuoja elektroninės informacijos saugos incidento valdymo procedūras.

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINIŲ SISTEMŲ FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

36. Administratorius suteikia prieigos prie Informacinių sistemų duomenų teisę (peržiūrėti duomenis, atlikti užklausas, vykdyti veiksmus su duomenimis ir kt.) bei fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nurodytam laikotarpiui jam nustatytoms funkcijoms atlikti.

37. Administratorius, suteikdamas prieigos prie Informacinių sistemų duomenų teisę, paslaugų teikėjo įgaliotą fizinį asmenį supažindina su prieigos prie Informacinių sistemų duomenų sąlygomis.

38. Reikalavimai Informacinėms sistemoms, reikalingoms paslaugų teikėjams ir jų projektavimo, aptarnavimo ir priežiūros teikiamoms paslaugoms funkcionuoti nustatomi šių paslaugų teikimo sutartyse.

39. Paslaugų teikimo sutartyse turi būti nurodoma, kad paslaugų teikėjas kuria ar modifikuoja programinę įrangą naudodamas:

39.1. įgyvendintas elektroninės informacijos saugos priemones nuo sankcionuoto poveikio sistemoms, programinei įrangai ir patalpoms;

39.2. sertifikuotą sisteminę programinę įrangą.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

40. Naudotojas privalo kuo greičiau informuoti Saugos įgaliotinį ar Informacinių sistemų administratorių apie pastebėtus saugumo incidentus: šių Taisyklių reikalavimų pažeidimus, informacinės sistemos veiklos sutrikimus arba neįprastą sistemos veikimą.

41. Naudotojai, pažeidę šių Taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____