Projektas

Asociacija „Slėnis Nemunas“

TVIRTINU,
Asociacijos „Slėnis Nemunas“
Direktorius _____

_____
Data 2011-12-07
A.V.

ASOCIACIJOS „SLĖNIS NEMUNAS“ INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Asociacijos „Slėnis Nemunas“ informacinės sistemos (toliu – SNIS) duomenų saugos nuostatų (toliau – nuostatai) paskirtis – nustatyti reikalavimus saugiai tvarkyti duomenis asociacijos „Slėnis Nemunas“ informacinėje sistemoje (toliau – sistema).

2. SNIS valdytoja – asociacija „Slėnis Nemunas“.

3. SNIS administratorius – Asociacijos "Slėnis Nemunas" įstatų ar kitų dokumentų nustatyta tvarka paskirtas administratorius.

4. Nuostatai taikomi sistemos valdytojai, administratoriui ir visiems naudotojams.

II. SISTEMOS INFORMACINĖ STRUKTŪRA

5. SNIS kaupiami ir tvarkomi duomenys:

5.1. duomenys apie užsiregistravusius SNIS:

5.1.1. mokslo darbuotojus;

5.1.2. tyrėjus;

5.1.3. idėjų iniciatorius;

5.1.4. aptariamas idėjas;

5.1.5. vykdomus projektus;

5.1.6. projektų vykdytojus;

5.1.7. kitus SNIS dalyvius.

5.2. nuorodos į:

5.2.1. asociacijos “Slėnis Nemunas“ narių tinklalapius;

5.2.2. duomenų bazes Lietuvoje;

5.2.3. duomenų bazes užsienyje;

5.2.4. socialinius tinklalapius;

5.2.5. kitų žemės ūkio mokslo, mokymo ir konsultavimo bei administravimo institucijų ir įstaigų bei verslo subjektų tinklalapius.

6. Duomenų srautai tarp SNIS ir kitų informacinių sistemų:

6.1. asociacijos „Slėnis Nemunas“ narių naudojami informacinių sistemų, susijusių su asociacijos „Slėnis Nemunas“ misija, duomenys;

6.2. kitų žemės ūkio mokslo, mokymo ir konsultavimo bei administravimo institucijų ir įstaigų bei verslo subjektų informacinių sistemų, susijusių su asociacijos „Slėnis Nemunas“ misija, duomenys.

III. SISTEMOS FUNKCINĖ STRUKTŪRA

7. SNIS funkcinę struktūrą sudaro:

7.1. informacinis portalas, veikiantis su pagrindinėmis naršyklėmis (IE, Firefox, Opera ir Chrome), kuriam nustatomi šie reikalavimai:

7.1.1. turi būti įdiegtas asociacijos „Slėnis Nemunas“ narių bei kitų klientų prieigos (informacijai pateikti arba paimti) prie SNIS informacinių resursų administravimo modulis, vadovaujantis SNIS saugos politika ir šiais nuostatais;

7.1.2. esant poreikiui, sistema turi būti lengvai plečiama - papildoma naujais moduliais.

7.2. Pagrindinės dalys/moduliai:

7.2.1. profesinis tinklas:

7.2.1.1. narių registracija;

7.2.1.2. nario priskyrimas tikslinėms grupėms;

7.2.1.3. privačių žinučių sistema;

7.2.1.4. galimybė nariui įtraukti pasirinktus asmenis į savo kontaktų sąrašą;

7.2.1.5. prieigos, prie skirtingų grupių, projektų, kitų SNIS modulių, teisių valdymas.

7.2.2. žinių duomenų bazė:

7.2.2.1. statistinių duomenų bazė, nuorodos į atitinkamas duomenų bazes;

7.2.2.2. mokslininkų gautų rezultatų prezentacijos;

7.2.2.3. gerosios praktikos technologiniai pavyzdžiai;

7.2.2.4. video archyvas.

7.2.3. įdėjų inicijavimas:

7.2.3.1. autorizuotas dalyvių registravimas ir administravimas;

7.2.3.2. dalyvių registruojamų Sistemoje idėjų originalumo patikra. Sistema turi patikrinti ar nėra jau registruota Sistemoje tokiu pačiu pavadinimu idėja;

7.2.3.3. idėjos aptarimas ir balsavimas;

7.2.3.4. idėjos atmetimas;

7.2.3.5. idėjos vystymas iki projekto;

7.2.3.6. aptartos idėjos patalpinimas žinių bazėje.

7.2.4. projektų valdymas:

7.2.4.1. kiekviename atskirame projekte galimybė aktyvuoti šias funkcijas: naujienos, užduotys, forumas, įdėjų valdymas, bylų saugykla (dokumentai, paveikslėliai ir t.t.), straipsniai, video archyvas, tiesioginės video transliacijoss ir kt.;

7.2.4.2. prieigų projekto grupės nariams saugus valdymas;

7.2.4.3. prieigų prie projekto modulių valdymo teisių suteikimas projekto grupės nariams. Jie turi turėti galimybę informaciją apie savo vykdomą projektą paviešinti kitoms grupėms ir neregistruotiems vartotojams, tačiau turi patvirtinti, kad šiuo atveju riziką dėl autorių teisių praradimo jie prisiima sau;

7.2.5. video archyvas:

7.2.5.1. plačiausiai naudojamų video formatų įdiegimas;

7.2.5.2. video bylų konvertavimas;

7.2.5.3. pavadinimo, aprašymo ir tikslinių žodžių suteikimas kiekvienai bylai;

7.2.5.4. grojaraščių iš kelių bylų sudarymas;

7.2.5.5. video medžiagos peržiūra Web naršyklėje;

7.2.5.6. atskirų video bylų pateikimas kituose sistemos moduliuose.

7.2.6. tiesioginių video transaliacijų:

7.2.6.1. tiesioginės transliacijos iš vaizdo kamerų;

7.2.6.2. vaizdo perkodavimas ir pateikimas Web naršyklėje ar TV;

7.2.6.3. transliacijų video medžiagos archyvavimas.

IV. DUOMENŲ SAUGOS ORGANIZAVIMAS IR NENUMATYTŲ SITUACIJŲ VALDYMAS

8. Sistemos duomenų saugos organizavimas ir nenumatytų situacijų valdymas vykdomas vadovaujantis:

8.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu (Žin., 1996, Nr. 63-1479; 2000, Nr. 64-1924; 2003, Nr. 15-597);

8.2. LST ISO/IEC 17799:2006 reikalavimais;

8.3. LST ISO/IEC 27001:2006 reikalavimais;

8.4. ISO/IEC 20000-1:2011 reikalavimais;

8.5. kitais norminiais dokumentais, reglamentuojančiais Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugumą, pvz.: „Informacijos technologija. Saugumo metodai“, techniniais saugos reikalavimais, patvirtintais LR vidaus reikalų ministro 2008 m. spalio 27 d. įsakymu Nr. 1V-384 (Žin., 2008, Nr 127-4866).

9. Sistemos valdytoja tvirtina šiuos nuostatus ir kitus saugumo politiką reglamentuojančius dokumentus.

10 Už sistemos duomenų saugos organizavimą vadovaujantis patvirtinta politika atsako sistemos administratorius.

11. Sistemos administratorius skiria administratoriaus atstovą informacijos saugos vadybai (toliau – AAISV), kuris atsako už saugumo politikos įgyvendinimą ir kontrolę.

12. AAISV teikia siūlymus sistemos administratoriui dėl sistemos saugos vadybos gerinimo.

13. Sistemos administratoriaus darbuotojai ir AAISV turi turėti patvirtintas kvalifikacijas, įgytas specializuotuose kvalifikacijos kėlimo kursuose ir patvirtintas pažymėjimais/sertifikatais LST ISO/IEC 17799:2006, LST ISO/IEC 27001:2006, ISO/IEC 20000-1:2011 srityse bei naudojamų operacinių sistemų ir taikomųjų programų klausimais.

14. Sistemos naudotojai, pastebėję saugumo politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti sistemos administratoriui arba – AAISV.

15. Sistemos naudotojų veiksmus esant nenumatytai situacijai reglamentuoja nenumatytų situacijų valdymo planas (toliau – planas), kurį rengia AAISV, kasmet peržiūri ir teikia tvirtinti sistemos administratoriaus vadovui.

16. Plano nuostatos pagrįstos šiais principais:

16.1. sistemos veiklos atstatymas, įvykus incidentui, kurio metu sutrinka sistemos veikimas;

16.2. sistemos naudotojų mokymas ir supažindinimas. Sistemos naudotojai turi būti supažindinti su teisės aktais, nustatančiais asmeninę kiekvieno sistemos naudotojo atsakomybę.

V. RIZIKOS ĮVERTINIMAS IR DETALI DARBO TVARKA

17. Pagrindinės sistemos rizikos mažinimo priemonės išdėstomos rizikos ataskaitoje, kuri rengiama įvertinus nustatytus rizikos veiksnius. Rizikos vertinimo planą rengia AAISV ir teikia tvirtinti administratoriaus vadovui. Rizikos vertinimo planas kasmet peržiūrimas ir atnaujinamas,

18. Konkrečias sistemos duomenų tvarkymo ir saugumo vadybos taisykles rengia administratorius ir teikia tvirtinti valdytojai. Taisykles sudaro:

18.1. techninės, programinės ir fizinės duomenų saugos priemonės (rezervinis elektros energijos tiekimas, antivirusinė programinė įranga, duomenų šifravimas, kompiuterių tinklų apsaugos sistema, patalpų fizinė sauga ir kita);

18.2. prieinamumo prie duomenų principai ir kontrolė (sistemos naudotojų registravimas, teisės dirbti su sistemos duomenimis suteikimas, sistemos naudotojų išregistravimas, sistemos naudotojų tapatybės nustatymas, specialios sistemos naudotojų tapatybės nustatymo priemonės, elektroninis parašas ir kita);

18.3. sistemos ir duomenų vientisumo pažeidimų fiksavimo ir pažeistų duomenų atkūrimo tvarka (sistemos naudotojų veiksmų registravimas, atsarginės duomenų kopijos ir jų saugojimas bei saugojimo kontrolė, duomenų atkūrimo tvarka ir kita);

18.4. saugaus duomenų teikimo duomenų naudotojams pagal sutartis tvarka ir kontrolė;

18.5. saugaus duomenų perkėlimo ar perdavimo tvarka ir jos laikymosi kontrolė;

18.6. įgaliojimai sistemos administratoriui ir jo teisės.

VI. SISTEMOS NAUDOTOJŲ ATSAKOMYBĖ

19. Visi sistemos naudotojai privalo rūpintis sistemos bei joje tvarkomų duomenų saugumu.

20. Tvarkyti sistemos duomenis gali tik sistemos naudotojai, susipažinę su šiais nuostatais ir kitais saugumo politiką reglamentuojančiais teisės aktais.

21. Sistemos naudotojų supažindinimas, su nuostatais ir kitais saugumo politiką reglamentuojančiais teisės aktais, organizuojamas ir įgyvendinamas naudotojo registravimosi proceso metu.

22. Naudotojas nesutinkantis laikytis šių nuostatų ir kitų saugumo politiką reglamentuojančių teisės aktų reikalavimų bei atsakomybės už šių reikalavimų nesilaikymą, negali būti registruojamas SNIS naudotoju.

23. Sistemos naudotojams turi būti nuolat rengiami duomenų saugos mokymai, įvairiais būdais primenama apie saugumo problemas (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės pagrindiniame lange ir pan.).

24. Sistemos naudotojai, pažeidę šių nuostatų ar kitų saugumo politiką reglamentuojančių teisės aktų reikalavimus, atsako įstatymų nustatyta tvarka.

VII. NUOSTATŲ ATNAUJINIMO TVARKA

25. AAISV, siekdamas užtikrinti sistemos ir joje tvarkomų duomenų saugumą, teikia siūlymus sistemos administratoriaus vadovui dėl nuostatų keitimo ar kitų saugumo politiką reglamentuojančių teisės aktų priėmimo, keitimo ar panaikinimo.

26. Nuostatų ir kitų saugumo politiką reglamentuojančių teisės aktų įgyvendinimo lygis nustatomas ne rečiau kaip kartą per metus atliekant auditą.

VIII. BAIGIAMOSIOS NUOSTATOS

27. Siekiant užtikrinti šiuose nuostatuose ir kituose saugumo politiką reglamentuojančiuose dokumentuose išdėstytų saugumo reikalavimų įgyvendinimo kontrolę, AAISV kasmet organizuoja auditą.

28. Audito klausimyną rengia AAISV.

29. Auditą atlieka administratoriaus vadovo sudaryta audito grupė, sudaryta iš darbuotojų turinčių pažymėjimais/sertifikatais patvirtintas reikalingas kvalifikacijas.

30. Audito metu įvertinama nuostatų ir kitų saugumo politiką reglamentuojančių teisės aktų atitiktis realiai duomenų saugos situacijai.

31. Inventorizuojama sistemos konfigūracija, administratoriaus techninė ir programinė įranga, naudojama SNIS veikimui užtikrinti.

32. Peržiūrima sistemos rizikos vertinimo planai ir ataskaitos.

33. Įvertinamas administratoriaus pasiruošimas sistemos veiklos atstatymui nenumatytose situacijose.

34 Atlikus auditą rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato sistemos administratoriaus vadovas.

Parengė: UAB „Ambernetas“, 2011-12-07