PATVIRTINTA
Vilniaus universiteto rektoriaus
2018 m. gegužės 3 d. įsakymu Nr. R-271

ANGLŲ-LIETUVIŲ-ANGLŲ IR PRANCŪZŲ-LIETUVIŲ-PRANCŪZŲ KALBŲ MAŠININIO VERTIMO, PAREMTO STATISTINIAIS METODAIS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Anglų-lietuvių-anglų ir prancūzų-lietuvių-prancūzų kalbų mašininio vertimo, paremto statistiniais metodais, informacinės sistemos saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Anglų-lietuvių-anglų ir prancūzų-lietuvių-prancūzų kalbų mašininio vertimo, paremto statistiniais metodais, informacinės sistemos (toliau – informacinės sistema) elektroninės informacijos saugos valdymą, organizacinius ir techninius reikalavimus, reikalavimus personalui ir informacinės sistemos naudotojų supažindinimo su saugos dokumentais principus.

2. Saugos nuostatų tikslas – sudaryti sąlygas saugiai automatiniu būdu tvarkyti informacinės sistemos informaciją, užtikrinti elektroninės informacijos prieinamumą ir vientisumą.

3. Saugos nuostatuose vartojamos sąvokos:

3.1. **Ekspertas** – asmuo turintis teisę aprašinėti informacinėje sistemoje pateikiamus skaitmeninius objektus;

3.2. **Registruoti informacinės sistemos naudotojai** (toliau – informacinės sistemos naudotojai) - informacinės sistemos naudotojai, pateikę duomenis autentifikacijos tikslu;

3.3. Kitos Saugos nuostatuose vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimų apraše (toliau – Aprašas) bei Saugos dokumentų turinio gairių apraše (toliau – Saugos dokumentų turinio gairių aprašas), patvirtintuose 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“ bei kituose teisės aktuose vartojamas sąvokas.

4. Informacijos saugumo užtikrinimo prioritetinės kryptys:

4.1. elektroninės informacijos prieinamumo užtikrinimas;

4.2. elektroninės informacijos vientisumo užtikrinimas;

4.3. informacinės sistemos veiklos tęstinumas.

5. Informacinės sistemos valdytojo ir tvarkytojo pavadinimai ir adresai:

5.1. informacinės sistemos valdytojas ir tvarkytojas yra Vilniaus universitetas, Universiteto g. 3, LT-01513, Vilnius.

5.2. Informacinės sistemos valdytojo funkcijas atlieka Vilniaus universiteto Fizikos fakulteto Fotonikos ir nanotechnologijų institutas, Saulėtekio al. 3, Vilnius.

5.3. Informacinės sistemos tvarkytojo funkcijas atlieka Vilniaus universiteto Informacinių technologijų paslaugų centras, Saulėtekio al. 9, Vilnius.

6. Informacinės sistemos valdytojo funkcijos ir atsakomybė:

6.1. prižiūri, kaip laikomasi informacinės sistemos duomenų saugos reikalavimų;

6.2. priima įsakymus dėl informacinės sistemos saugumo užtikrinimo, tikrina, kaip jie vykdomi;

6.3. atsako už informacinės sistemos saugos politikos formavimą ir įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą, tvirtina saugos politikos įgyvendinamuosius dokumentus (Saugaus elektroninės informacijos tvarkymo taisykles, informacinės sistemos veiklos tęstinumo valdymo planą, informacinės sistemos naudotojų administravimo taisykles);

6.4. skiria duomenų valdymo įgaliotinį.

7. Informacinės sistemos tvarkytojo funkcijos ir atsakomybė:

7.1. užtikrina nepertraukiamą informacinės sistemos veikimą, elektroninės informacijos, esančios informacinėje sistemoje, saugą ir saugų elektroninės informacijos perdavimą kompiuterių tinklais (automatiniu būdu);

7.2. teikia pasiūlymus informacinės sistemos valdytojui, kaip tobulinti informacinės sistemos saugą;

7.3. užtikrina tinkamą informacinės sistemos valdytojo priimtų teisės aktų ir rekomendacijų įgyvendinimą;

7.4. skiria informacinės sistemos saugos įgaliotinį;

7.5. skiria informacinės sistemos administratorių arba kelis administratorius, vykdančius atskiras informacinės sistemos administravimo funkcijas;

7.6. užtikrina informacinės sistemos sąveiką su kitomis informacinėmis;

8. Informacinės sistemos tvarkytojo vadovas yra atsakingas už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politikos įgyvendinamuosiuose dokumentuose nustatyta tvarka.

9. Duomenų valdymo įgaliotinis, vadovaudamasis informacinių technologijų plėtros planu, kitais institucijos planavimo dokumentais:

9.1. įgyvendina informacinės sistemos plėtrą;

9.2. tiesiogiai prižiūri, kaip kuriama ir tvarkoma informacinė sistema, diegiama programinė įranga, panaudojamos investicijos;

9.3. rengia informacinės sistemos biudžetų projektus;

9.4. tiesiogiai prižiūri, kad informacija, duomenys, dokumentai ir (arba) jų kopijos būtų teikiami, skelbiami ir (arba) perduodami pagal teisės aktuose nustatytus reikalavimus;

9.5. teikia pasiūlymus dėl darbuotojų, kuriems pavesta tvarkyti informacinės sistemos duomenis, informaciją, dokumentus ir (arba) jų kopijas, teisių ir pareigų;

9.6. organizuoja informacinės sistemos turto inventorizacijas;

9.7. užtikrina informacinės sistemos naudotojų pasirengimą dirbti su informacine sistema;

9.8. atsako už tinkamą Saugos nuostatuose nustatytų funkcijų vykdymą;

9.9. atlieka kitas teisės aktuose nustatytas funkcijas.

10. Informacinės sistemos saugos įgaliotinio funkcijos ir atsakomybė:

10.1. teikia informacinės sistemos tvarkytojo vadovui pasiūlymus dėl:

10.1.1. informacinės sistemos administratoriaus (administratorių) paskyrimo;

10.1.2. informacinių technologijų saugos atitikties vertinimo Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 43 punkte nurodytoje metodikoje nustatyta tvarka;

10.1.3. saugos dokumentų priėmimo, keitimo;

10.2. koordinuoja elektroninės informacijos saugos incidentų tyrimą, išskyrus atvejus, kai šią funkciją atlieka informacijos saugos darbo grupės;

10.3. teikia informacinės sistemos administratoriui (administratoriams) privalomus vykdyti nurodymus ir pavedimus dėl saugos politikos įgyvendinimo;

10.4. organizuoja informacinės sistemos rizikos įvertinimą;

10.5. periodiškai organizuoja informacinės sistemos administratorių mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas;

10.6. atlieka kitas informacinės sistemos valdytojo ir/ar tvarkytojo vadovo pavestas ir kituose teisės aktuose jam priskirtas funkcijas.

11. Informacinės sistemos administratoriaus (administratorių) funkcijos:

11.1. administruoja informacinės sistemos naudotojų duomenis;

11.2. analizuoja informacinės sistemos naudotojų veiksmų registracijos žurnalų įrašus;

11.3. kuria ir atkuria atsargines informacinės sistemos duomenų bazės kopijas;

11.4. rengia ir tikrina informacinės sistemos diegimo sąranką;

11.5. nustato pažeidžiamas informacinės sistemos vietas ir užtikrina savalaikį sistemos saugos spragų šalinimą;

11.6. atlieka informacinės sistemos naudotojams suteiktų teisių ir priskirtų funkcijų atitikties vertinimą;

11.7. informuoja informacinės sistemos saugos įgaliotinį apie saugos pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones;

11.8. vykdo privalomus duomenų valdymo ir saugos įgaliotinio nurodymus;

11.9. atlieka kitas teisės aktuose nustatytas funkcijas.

12. Saugų informacinės sistemos duomenų tvarkymą reglamentuoja:

12.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

12.2. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

12.3. Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ (toliau – Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašas);

12.4. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

12.5. Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtinti Valstybinės duomenų apsaugos inspekcijos direktoriaus 2014 m. gruodžio 18 d. įsakymo Nr. 1T-71 (1.12) „Dėl Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms patvirtinimo“ (toliau - Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms);

12.6. Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

12.7. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką ir duomenų tvarkymo teisėtumą, valstybės informacinių sistemų tvarkytojų veiklą bei duomenų saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Informacinėje sistemoje tvarkoma elektroninė informacija priskirtina kitos elektroninės informacijos kategorijai, vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 10 punkto nuostatomis.

14. Informacinė sistema priskiriama ketvirtai kategorijai, vadovaujantis Valstybės informacinių išteklių įstatymo 3 straipsnio 4 dalimi, Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 12.4 papunkčio nuostatomis, atsižvelgiant į joje apdorojamos elektroninės informacijos svarbos kategoriją.

15. Informacinėje sistemoje asmens duomenys tvarkomi tik vidaus administravimo reikmėms naudotojų paskyroms administruoti, todėl, vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, priskiriamas pirmas tvarkomų asmens duomenų saugumo lygis.

16. Informacinės sistemos saugos įgaliotinis, vadovaudamasis Vidaus reikalų ministerijos metodine priemone „Rizikos analizės vadovas“, Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais, kasmet organizuoja informacinės sistemos rizikos veiksnių vertinimą. Prireikus, informacinės sistemos saugos įgaliotinis gali organizuoti neeilinį informacinės sistemos rizikos veiksnių vertinimą.

17. Informacinės sistemos rizikos vertinimas surašomas rizikos įvertinimo ataskaitoje, kuri pateikiama informacinės sistemos valdytojo ir tvarkytojo vadovams.

18. Informacinės sistemos rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai yra šie:

18.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

18.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

18.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

19. Informacinės sistemos rizikos vertinimo metu atliekami darbai:

19.1. įtakos informacinės sistemos veiklai vertinimas;

19.2. grėsmės ir pažeidimų analizė;

19.3. liekamosios rizikos vertinimas.

20. Informacinės sistemos valdytojas, atsižvelgdamas į informacinės sistemos rizikos įvertinimo ataskaitą, prireikus tvirtina informacinės sistemos rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis informacinės sistemos rizikos valdymo priemonėms įgyvendinti.

21. Pagrindiniai elektroninės informacijos saugos priemonių parinkimo principai yra šie:

21.1. liekamoji rizika turi būti sumažinama iki priimtino lygio;

21.2. informacijos saugos priemonės diegimo kaina turi būti adekvati saugomos informacijos vertei;

21.3. kur galima, turi būti įdiegtos prevencinės, detekcinės ir korekcinės informacijos saugos priemonės.

22. Atlikus rizikos įvertinimą, esant poreikiui, saugos įgaliotinis rengia ir teikia valdytojui tvirtinti rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

23. Siekiant užtikrinti informacinės sistemoms saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose teisės aktuose išdėstytų nuostatų įgyvendinimo kontrolę, saugos įgaliotinis, ne rečiau kaip kartą per du metus, vadovaujantis Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ patvirtinta metodika, atlikus rizikos vertinimą organizuoja informacinės sistemos saugos atitikties vertinimą, kurio metu:

23.1. surenkama vertinimui būtina informacija apie informacinių technologijų saugos padėtį Vilniaus universiteto informacinėse sistemose ir dokumentai, būtini užtikrinant informacinės sistemos saugą;

23.2. įvertinama saugos nuostatų ir saugos politiką įgyvendinančių teisės aktų atitiktis Bendriesiems duomenų saugumo reikalavimams. Vertinimo metu vertintojas gali atlikti informacinės sistemos naudotojų ir administratorių apklausą;

23.3. vertintojas parengia informacinių sistemų saugos atitikties vertinimo ataskaitą ir teikia ją atitinkamam vadovui, kuris organizuoja trūkumų šalinimo priemonių plano rengimą.

24. Atlikus informacinės sistemos saugos atitikties vertinimą, rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus skiria ir įgyvendinimo terminus nustato valdytojo vadovas.

25. Trūkumų šalinimo priemonių plano vykdymo kontrolę užtikrina saugos įgaliotinis.

III SYKRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

26. Programinės įrangos, skirtos informacinei sistemai nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

26.1. tarnybinėse stotyse ir kompiuterinėse darbo vietose su „Microsoft Windows“ operacine sistema privalo būti įdiegta apsauga nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos ir kt.);

26.2. apsaugai naudojama programinė įranga privalo atsinaujinti ne rečiau kaip kartą per savaitę.

27. Programinės įrangos, įdiegtos kompiuteriuose ir serveriuose, naudojimo nuostatos:

27.1. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu;

27.2. naudojama tik legali programinė įranga;

27.3. programinė įranga yra nuolatos atnaujinama laikantis gamintojo reikalavimų;

27.4. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka tik informacinės sistemos administratoriai.

28. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. proxy) ir kt.) pagrindinės naudojimo nuostatos:

28.1. įmonės kompiuteriniai tinklai nuo viešųjų telekomunikacijų tinklų (interneto) atskirti ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos įranga;

28.2. visas informacinės sistemos duomenų srautas į ir iš interneto yra filtruojamas naudojant apsaugą nuo virusų ir kitos kenkėjiškos programinės įrangos;

28.3. papildomos priemonės kompiuteriams ir mobiliems įrenginiams, kurie gali būti panaudoti nustatytoms administravimo funkcijoms atlikti ne institucijos patalpose, nustatomos Saugaus elektroninės informacijos tvarkymo taisyklėse.

29. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

29.1. nuotolinis prisijungimas prie informacinės sistemos galimas naudojantis „IPSec“ (angl. Internet Protocol Security) protokolų rinkiniu ir jungiantis kaip „IPSec“ programiniam klientui. Šia galimybe gali būti pasinaudota tik informacinės sistemos administravimo tikslais.

29.2. teikti elektroninę informaciją automatiniu būdu galima tik pagal duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas.

30. Informacinės veiklos tęstinumo užtikrinimui elektroninė informacija yra periodiškai kopijuojama į rezervinių kopijų laikmenas kas 24 valandos ir laikmenos saugomos taip, kad avarijos atveju informacinę sistemą galima būtų atkurti taip, kad informacinės sistemos neveikimo laikotarpis būtų neilgesnis nei 24 valandos.

31. Informacinės sistemos prieinamumas per metus turi būti užtikrintas ne mažiau kaip 70 proc. laiko darbo metu darbo dienomis.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

32. Informacinės sistemos saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą.

Informacinės sistemos saugos įgaliotinis privalo sugebėti prižiūrėti, kaip įgyvendinama saugos politika. Saugos įgaliotinis privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

33. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumo srityje, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau nei vieni metai.

34. Informacinės sistemos administratoriai privalo išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugumą. Informacinės sistemos administratorius privalo mokėti administruoti ir prižiūrėti duomenų bazes, turėti darbo kompiuteriu įgūdžių, mokėti tvarkyti informacinės sistemos duomenis, būti susipažinęs su Saugos nuostatais ir saugos politikos įgyvendinamaisiais teisės aktais.

35. Informacinės sistemos naudotojai ir administratoriai, pažeidę Saugos nuostatų ar kitų saugos politikos įgyvendinamųjų teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

36. Už informacinės sistemos naudotojų supažindinimą su Saugos nuostatais ir kitais saugos politikos įgyvendinamaisiais teisės aktais bei atsakomybe už šių reikalavimų nesilaikymą yra atsakingas informacinės sistemos saugos įgaliotinis.

37. Informacinės sistemos naudotojų supažindinimą su saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą organizuoja saugos įgaliotinis.

38. Su Saugos nuostatais susipažįstama pasirašytinai arba elektroniniu būdu, užtikrinančiu susipažindinimo įrodomumą.

39. Saugos nuostatai ir kiti saugos politikos įgyvendinamieji teisės aktai skelbiami informacinės sistemos naudotojams pasiekiamoje interneto svetainėje.

40. Pakartotinai su saugos politiką reguliuojančiais teisės aktais informacinės sistemos naudotojai supažindinami tik iš esmės pasikeitus informacijos saugą reguliuojantiems teisės aktams. Informacija apie saugos politikos įgyvendinamųjų teisės aktų pakeitimus siunčiama elektroniniu būdu.

_____