PATVIRTINTA
Kauno technologijos universiteto inžinerijos licėjus direktoriaus
2023 m. sausio 3 d. įsakymu Nr. V-3

KAUNO TECHNOLOGIJOS UNIVERSITETO INŽINERIJOS LICĖJAUS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS BENDROSIOS NUOSTATOS

1. Informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Kauno technologijos universiteto inžinerijos licėjaus (toliau – Įstaiga) informacinių sistemų (toliau – Informacinė sistema) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Informacinės sistemos elektroninės informacijos saugos politikos tikslas – užtikrinti Informacinės sistemos elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

3. Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame 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“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), ir Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose 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“ (toliau – Techniniai elektroninės informacijos saugos reikalavimai).

4. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

4.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

4.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

4.3. vykdyti elektroninės informacijos saugos (kibernetinių) incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos (kibernetinius) incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

5. Informacinės sistemos elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Informacinės sistemos elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė;

5.2. Informacinės sistemos elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.3. Informacinės sistemos tvarkymo kontrolė;

5.4. Informacinės sistemos paslaugų ir naudojimosi Informacinės sistemos elektronine informacija kontrolės užtikrinimas;

5.5. Informacinės sistemos tvarkomų asmens duomenų apsauga;
5.6. Informacinės sistemos veiklos tęstinumo užtikrinimas;
5.7. Informacinės sistemos naudotojų mokymas.

6. Už elektroninės informacijos saugą (kibernetinį saugumą) pagal kompetenciją atsako Informacinės sistemos valdytojas ir tvarkytojas – Įstaiga.

7. Įstaiga atsako už elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir politikos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą. Taip pat atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimo užtikrinimą saugos politiką įgyvendinančiuose dokumentuose (toliau – Saugos dokumentai) nustatyta tvarka.

8. Saugos nuostatai taikomi Informacinės sistemos valdytojui ir tvarkytojui Kauno technologijos universiteto inžinerijos licėjui, įstaigos adresas S. Lozoraičio g. 13, Kaunas, Informacinės sistemos saugos įgaliotiniui, Informacinės sistemos administratoriams, Informacinės sistemos naudotojams, Informacinei sistemai funkcionuoti reikalingų paslaugų teikėjams.

9. Įstaigos funkcijos:
9.1. organizuoti ir vadovauti informacinių sistemų veiklai;
9.2. rengti ir tvirtinti teisės aktus, susijusius su duomenų sauga, ir prižiūrėti, kaip jų laikomasi;
9.3. kontroliuoti, kad Informacinė sistema būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, Saugos nuostatais ir kitais teisės aktais;
9.4. tvirtinti Saugos nuostatus, saugos dokumentus ir kitus teisės aktus, susijusius su Informacinės sistemos elektroninės informacijos sauga (kibernetiniu saugumu) ir užtikrinti jų įgyvendinimą;
9.5. nagrinėti Informacinės sistemos tvarkytojų pasiūlymus dėl Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo ir priimti dėl jų sprendimus;
9.6. skirti Informacinės sistemos saugos įgaliotinį ir Informacinės sistemos administratorius;
9.7. užtikrinti nepertraukiamą Informacinės sistemos veiklą;
9.8. užtikrinti saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;
9.9. pagal kompetenciją prižiūrėti Informacinės sistemos duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, įsilaužimų aptikimo sistemas, elektroninės informacijos perdavimo tinklus ir kitus Informacinės sistemos komponentus, užtikrinti jų veikimą;
9.10. pagal kompetenciją užtikrinti Informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą);
9.11. ne rečiau kaip kartą per metus organizuoti saugos dokumentų peržiūrėjimą ir aktualizavimą.

10. Informacinės sistemos saugos įgaliotinio funkcijos:
10.1. koordinuoti ir prižiūrėti elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimą saugos dokumentuose nustatyta tvarka;
10.2. teikti Įstaigos vadovui siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo;
10.3. atlikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;
10.4. teikti Įstaigos vadovui siūlymus dėl Saugos nuostatų ir Informacinės sistemos saugos dokumentų priėmimo arba keitimo;
10.5. supažindinti Informacinės sistemos administratorius ir Informacinės sistemos naudotojus su Saugos nuostatų ir saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą;

10.6. organizuoti Informacinės sistemos naudotojų mokymus elektroninės informacijos saugos klausimais, informuoti juos apie elektroninės informacijos saugos problemas;

10.7. duoti Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Saugos nuostatų ir saugos dokumentų įgyvendinimu;

10.8. teikti Įstaigos vadovui pasiūlymus dėl koordinuojančio Informacinės sistemos administratoriaus paskyrimo ir reikalavimų jam nustatymo;

10.9. koordinuoti elektroninės informacijos saugos (kibernetinių) incidentų tyrimą Įstaigoje ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos (kibernetinius) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetiniais) incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos (kibernetinio saugumo) darbo grupės;

10.10. teikti Informacinės sistemos administratoriams ir Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimo;

10.11. atlikti kitas Įstaigos vadovo pavestas Saugos nuostatuose ir saugos dokumentuose jam priskirtas funkcijas.

11. Informacinės sistemos administratoriaus funkcijos:

11.1. užtikrinti Informacinės sistemos techninės ir programinės įrangos įdiegimą ir funkcionavimą;

11.2. diegti ir prižiūrėti programinę įrangą, reikalingą Informacinės sistemos naudotojų funkcijoms vykdyti;

11.3. suteikti teisę Informacinės sistemos naudotojams naudotis elektronine informacija, kurios reikia jų funkcijoms atlikti;

11.4. užtikrinti Informacinės sistemos komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimo aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą, pagal kompetenciją nustatyti Informacinės sistemos pažeidžiamas vietas;

11.5. pagal kompetenciją dalyvauti vykdant saugumo reikalavimų įgyvendinimo stebėseną;

11.6. pagal kompetenciją teikti Įstaigos vadovui siūlymus dėl Informacinės sistemos palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

11.7. informuoti Informacinės sistemos saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikti siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

11.8. daryti Informacinės sistemos duomenų bazės atsargines kopijas ir atsakyti už archyve esančių kopijų saugojimą;

11.9. atlikti kitas Įstaigos vadovo ir Informacinės sistemos saugos įgaliotinio pavestas Saugos nuostatuose ir saugos dokumentuose nustatytas funkcijas.

12. Teisės aktai, kuriais vadovaujamasi tvarkant informacinių sistemų elektroninę informaciją ir užtikrinant jos saugą:

12.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

12.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

12.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

12.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

12.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

12.6. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo 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 Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Elektroninės informacijos svarbos nustatymo gairių aprašas);

12.7. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

12.8. Techniniai elektroninės informacijos saugos reikalavimai;

12.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Informacinių technologijų saugos atitikties vertinimo metodika);

12.10. Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, nustatantys saugų elektroninės informacijos tvarkymą;

12.11. Saugos nuostatai, saugos dokumentai ir kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 7–10 punktais, Informacinės sistemos tvarkoma informacija priskiriama prie mažiausios svarbos informacijos kategorijos.

14. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 12 punktu, Informacinė sistema priskiriama prie ketvirtosios kategorijos.

15. Informacinės sistemos saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, kasmet organizuoja Informacinės sistemos rizikos įvertinimą. Pasikeitus Informacinės sistemos duomenų bazės struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų pašalinimas ir kt.) ar po esminių organizacinių ar sisteminių pokyčių, nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis Informacinės sistemos rizikos įvertinimas. Informacinės sistemos rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu.

16. Organizuojant rizikos vertinimą turi būti paskirtas už rizikos vertinimo proceso priežiūrą ir tobulinimą atsakingas asmuo arba asmenys ir nustatyti jiems taikomi kvalifikaciniai reikalavimai. Atsakingu asmeniu gali būti skiriamas Įstaigos darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugas teikiančiu subjektu.

17. Informacinės sistemos rizikos vertinimo metu įvertinami rizikos veiksniai, galintys turėti įtakos Informacinės sistemos elektroninės informacijos saugai, jų galima žala, pasireiškimo tikimybė, galimi rizikos valdymo būdai. Svarbiausieji rizikos veiksniai:

17.1. 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, netinkamas veikimas ir kita);

17.2. 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);

17.3. 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.

18. Informacinės sistemos rizikos veiksniams vertinti naudojama dvidešimt penkių balų rizikos vertinimo sistema, pagal kurią, nustačius rizikos veiksnių tikimybę ir poveikį, apskaičiuojamas rizikos laipsnis:

18.1. rizikos laipsnis nuo 1 iki 6 – maža rizika;

18.2. rizikos laipsnis nuo 8 iki 12 – vidutinė rizika;

18.3. rizikos laipsnis nuo 15 iki 25 – didelė rizika.

19. Kuo didesnė rizikos veiksnio tikimybė ir jo poveikis, tuo rizikos laipsnis aukštesnis. Rizikos veiksniams, kuriems nustatytas aukštas rizikos laipsnis, būtina skirti didžiausią dėmesį parenkant ir įgyvendinant tinkamas rizikos mažinimo priemones.

20. Siekiant įvertinti Informacinės sistemos saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per metus, jei teisės aktuose nenustatyta kitaip, organizuojamas informacinių technologijų saugos atitikties vertinimas.

21. Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Įstaigos vadovui. Pastebėtų trūkumų šalinimo planą, atsakingus jo vykdytojus paskiria ir įgyvendinimo terminus nustato taip pat Įstaigos vadovas.

22. Informacinės sistemos atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

23. Elektroninės informacijos saugos (kibernetinio saugumo) priemonės (techninės, programinės, organizacinės ir kitos informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) priemonės) parenkamos vadovaujantis šiais principais:

23.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

23.2. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei;

23.3. kur galima, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės informacijos saugos (kibernetinio saugumo) priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

24. Elektroninės informacijos saugai užtikrinti yra taikomos šios bendrosios programinės įrangos naudojimo nuostatos:

24.1. turi būti naudojama tik legali Informacinės sistemos funkcijoms vykdyti būtina programinė įranga;

24.2. programinė įranga turi būti nuolatos atnaujinama laikantis gamintojo reikalavimų;

24.3. turi būti įdiegta prieigos prie Informacinės sistemos elektroninės informacijos per registravimą, teisių suteikimą ir slaptažodžius sistema;

24.4. turi būti rekomenduojama keisti slaptažodžius ne rečiau kaip kas 180 dienų.

25. Informacinės sistemos duomenų saugai užtikrinti tarnybinėse stotyse taikomos šios programinės įrangos naudojimo nuostatos:

25.1. operacinių sistemų ir taikomųjų programų sąranka parenkama taip, kad būtų užtikrintas didžiausias saugumo lygis, sustabdomi nereikalingi darbui procesai;

25.2. ribojama ar blokuojama prieiga prie operacinės sistemos prievadų;

25.3. programinę įrangą atnaujina ir kontroliuoja administratorius. Paslaugų tiekėjai programinę įrangą gali atnaujinti tik dalyvaujant administratoriui.

26. Duomenų saugai užtikrinti informacinės sistemos naudotojų, darbuotojų darbo vietose taikomos šios programinės įrangos naudojimo nuostatos:

26.1. įdiegiama programinė įranga, skirta apsisaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.). Antivirusinės sistemos virusų parašų duomenų bazė atnaujinama automatiškai. Ilgiausias leistinas neatnaujinimo laikas – 14 darbo dienų. Kompiuterio operacinė sistemos kritinės pataisos diegiamos automatiškai. Programinę įrangą atnaujina ir kontroliuoja administratorius;

26.2. informacinės sistemos naudotojų paskyros turi būti apribotų teisių, kurios neleidžia įdiegti papildomos programinės įrangos bei keisti sistemos, kompiuterio ar programinės įrangos sisteminių nustatymų. Programinę įrangą diegia administratorius.

27. Pagrindiniai atsarginių kopijų darymo ir atkūrimo reikalavimai:

27.1. Duomenų saugai užtikrinti daromos pagrindinių duomenų atsarginės duomenų kopijos;

27.2. atsarginės kopijos daromos reguliariai, kiekvieną darbo dieną ir saugomos bent savaitę.

27.3. atsarginės kopijos turi būti daromos automatiškai. Jas atkurti turi teisę tik administratorius;

IV SKYRIUS
REIKALAVIMAI PERSONALUI

28. Informacinės sistemos saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti elektroninės informacijos saugos (kibernetinio saugumo) srities kvalifikaciją, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą (kibernetinį saugumą). Informacinės sistemos tvarkytojas turi sudaryti sąlygas saugos įgaliotiniui kelti kvalifikaciją.

29. Informacinės sistemos saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, 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 prijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

30. Informacinės sistemos administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti Informacinės sistemos komponentus (stebėti Informacinės sistemos komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti Informacinės sistemos komponentų nepertraukiamą funkcionavimą ir pan.). Informacinės sistemos administratoriai turi būti susipažinę su saugos dokumentais.

31. Informacinės sistemos naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, informacinių sistemų elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo laikyti jų paslaptį ir būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

32. Informacinės sistemos naudotojų ir Informacinės sistemos administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo periodiškumo reikalavimai:

32.1. Informacinės sistemos naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos (kibernetinio saugumo) problemas (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems informacinių sistemų naudotojams, informacinių sistemų administratoriams ir pan.);

32.2. mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), saugos įgaliotinio, Informacinės sistemos naudotojų ar informacinių sistemų administratorių poreikius;

32.3. mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kt. teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.);

32.4. mokymai Informacinės sistemos naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už mokymų organizavimą atsakingas Informacinės sistemos saugos įgaliotinis. Mokymai Informacinės sistemos saugos įgaliotiniui ir Informacinės sistemos administratoriams turi būti organizuojami pagal poreikį.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

33. Informacinės sistemos naudotojai, Informacinės sistemos administratoriai ir saugos įgaliotinis, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

34. Pakartotinai su Saugos nuostatais ir saugos dokumentais Informacinės sistemos naudotojai supažindinami jiems pasikeitus.

35. Saugos nuostatai bei kiti dokumentai, reglamentuojantys saugų elektroninės informacijos tvarkymą, skelbiami Įstaigos interneto svetainėje.

36. Tvarkyti Informacinės sistemos elektroninę informaciją gali tik Informacinės sistemos naudotojai, kurie yra susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų. Informacinės sistemos naudotojai atsako už Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

37. Saugos nuostatai ir saugos dokumentai iš esmės turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

____