

PATVIRTINTA

Kauno miesto savivaldybės

administracijos direktoriaus

2012 m. spalio 11 d.

įsakymu Nr. A-3778

[..\\A123778.DOC](#)

KAUNO MIESTO SAVIVALDYBĖS INFORMACINĖS SISTEMOS DUOMENŲ SAUGUMO NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Kauno miesto savivaldybės (toliau – Savivaldybė) informacinės sistemos duomenų saugumo nuostatai (toliau – saugumo nuostatai) reglamentuoja Savivaldybės informacinės sistemos (toliau – informacinė sistema) duomenų saugumą ir nustato informacinės sistemos saugumo politiką.

2. Saugumo nuostatų tikslas – užtikrinti informacinėje sistemoje tvarkomų duomenų konfidencialumą, prieinamumą, vientisumą ir tinkamą kompiuterizuotų darbo vietų bei kompiuterių tinklo įrangos funkcionavimą.

3. Saugumo nuostatuose vartojamos sąvokos:

Elektroninė informacija (toliau – informacija) – visa informacija, kuri tvarkoma informacinių technologijų priemonėmis.

Informacijos saugumo įvykis (toliau – saugumo įvykis) – nustatytas sistemos, tarnybos ar tinklo įvykis, rodantis, kad yra galima saugumo užtikrinimo spraga ar apsaugos priemonių triktis arba anksčiau nenumatyta situacija, kuri gali būti svarbi saugumui.

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

Informacinės sistemos naudotojai (toliau – naudotojai) – Savivaldybės tarybos nariai, Savivaldybės tarybos sekretoriato, Savivaldybės kontrolės ir audito tarnybos, Savivaldybės administracijos valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartį.

Informacijos tvarkymas – visos su informacija atliekamos operacijos: rinkimas, kaupimas, saugojimas, keitimas, kopijavimas, sujungimas, atskleidimas, teikimas, naudojimas, naikinimas naudojant informacines technologijas.

Kitos saugumo nuostatuose vartojamos sąvokos suprantamos taip, kaip saugų duomenų tvarkymą reglamentuojančiuose Lietuvos Respublikos teisės aktuose, Lietuvos bei tarptautiniuose standartuose.

4. Informacijos saugumo užtikrinimo prioritetinės kryptys:
 - 4.1. informacijos konfidencialumo užtikrinimas;
 - 4.2. informacijos vientisumo užtikrinimas;
 - 4.3. informacijos prieinamumo užtikrinimas;
 - 4.4. informacinės sistemos veiklos tęstinumas;
 - 4.5. asmens duomenų apsauga.
5. Informacinės sistemos valdytoja ir tvarkytoja yra Savivaldybės administracija, adresas Laisvės al. 96, LT-44251 Kaunas.
 6. Savivaldybės administracija, kaip informacinės sistemos valdytoja ir tvarkytoja:
 - 6.1. atsako už informacinėje sistemoje tvarkomos informacijos tvarkymo teisėtumą ir informacijos saugumą;
 - 6.2. rengia dokumentus, susijusius su informacinės sistemos saugumo užtikrinimu;
 - 6.3. užtikrina nepertraukiamą informacinės sistemos veikimą ir duomenų, esančių informacinės sistemos duomenų bazėse, saugumą ir saugų duomenų perdavimą kompiuterių tinklais (automatiniu būdu);
 - 6.4. tobulina informacinę sistemą ir informacinės sistemos duomenų saugumą;
 - 6.5. organizuoja informacinės sistemos rizikos vertinimą;
 - 6.6. vykdo informacinę sistemą sudarančių informacinių išteklių inventORIZaciją;
 - 6.7. atlieka kitas saugumo nuostatuose ir kituose teisės aktuose numatytas funkcijas.
 7. Informacijos tvarkytojai yra Savivaldybės administracijos padaliniai, atsakingi už jiems priskirtos informacijos tvarkymą, priežiūrą ir saugumą.
 8. Informacijos tvarkytojai atlieka šias funkcijas:
 - 8.1. tvarko informaciją pagal jų veiklą reglamentuojančių įstatymų ir kitų teisės aktų reikalavimus;
 - 8.2. teikia informaciją duomenų gavėjams;
 - 8.3. vykdo saugumo dokumentuose nustatytus reikalavimus ir užtikrina tinkamą duomenų saugumą;
 - 8.4. teikia pranešimus apie saugumo įvykius;
 - 8.5. atlieka kitas saugumo nuostatuose ir kituose teisės aktuose numatytas funkcijas.
 9. Savivaldybės administracijos direktorius skiria informacinės sistemos saugumo įgaliotinį (toliau – saugumo įgaliotinis) ir informacinės sistemos administratorių arba kelis administratorius, vykdančius atskiras informacinės sistemos administravimo funkcijas (toliau – administratorius).
 10. Saugumo įgaliotinis, įgyvendindamas informacijos saugumą, atlieka šias funkcijas:
 - 10.1. teikia siūlymus dėl saugumo dokumentų priėmimo, keitimo ar panaikinimo;

- 10.2. dalyvauja saugumo įvykių, įvykusių informacinėje sistemoje, tyrime;
- 10.3. konsultuoja naudotojus informacijos saugumo klausimais;
- 10.4. atlieka kitas saugumo nuostatuose ir kituose teisės aktuose numatytas funkcijas.
- 11. Administratorius atlieka tokias funkcijas:
 - 11.1. naudotojams suteikia teisę naudotis informacija ir kompiuteriu paskirtoms funkcijoms atlikti;
 - 11.2. administruoja serverius, kompiuterių tinklo įrangą, interneto svetainę, pašto ir paieškos sistemas, nustato pažeidžiamų vietų ir saugumo reikalavimų atitikti;
 - 11.3. registruoja saugumo įvykius, informuoja apie juos savo tiesioginį vadovą, teikia pasiūlymus dėl įvykių sukėlusių priežasčių pašalinimo;
 - 11.4. atlieka kitas saugumo nuostatuose ir kituose teisės aktuose numatytas funkcijas.
- 12. Informacinės sistemos saugumo politiką įgyvendinantys dokumentai yra Saugaus elektroninės informacijos tvarkymo Kauno miesto savivaldybės informacinėje sistemoje taisyklės, Kauno miesto savivaldybės informacinės sistemos veiklos tęstinumo valdymo planas ir Kauno miesto savivaldybės informacinės sistemos naudotojų administravimo taisyklės (toliau – saugumo politiką įgyvendinantys dokumentai).
- 13. Savivaldybės informacinės sistemos saugumas užtikrinamas vadovaujantis Lietuvos standartais LST ISO/IEC 27001:2006 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai (tapatus ISO/IEC 27001:2005)“ ir LST ISO/IEC 27002:2009 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 27002:2005)“, kitais Lietuvos bei tarptautiniais standartais, reglamentuojančiais informacijos saugumą.

II. INFORMACIJOS SAUGUMO VALDYMAS

- 14. Pagrindiniai informacijos saugumo priemonių parinkimo principai yra šie:
 - 14.1. rizika turi būti sumažinta iki priimtino lygio;
 - 14.2. informacijos saugumo priemonės diegimo kaina adekvati saugomos informacijos vertei;
 - 14.3. kur galima, turi būti įdiegtos prevencinės informacijos saugumo priemonės.
- 15. asmens duomenų apsauga turi būti užtikrinta vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir Savivaldybės administracijos direktoriaus patvirtintomis Asmens duomenų tvarkymo taisyklėmis.
- 16. Informacinės sistemoje įvykusių saugumo incidentų valdymas ir informacinės sistemos veiklos atkūrimas vykdomas Kauno miesto savivaldybės informacinės sistemos veiklos tęstinumo valdymo plane nustatyta tvarka.

17. Siekiant užtikrinti šiuose saugumo nuostatuose ir kituose saugumo politiką įgyvendinančiuose dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per metus:

17.1. inventorizuojama informacinės sistemos techninė ir programinė įranga;

17.2. sudaromas informacinės sistemos informacinių išteklių sąrašas;

17.3. tikrinamas ir atnaujinamas Kauno miesto savivaldybės informacinės sistemos veiklos atkūrimo detalusis planas.

18. Techninės, administracinės ir kitos duomenų saugumo valdymo priemonės turi būti pasirenkamos taip, kad su kuo mažesnėmis išlaidomis būtų užtikrintas informacinės sistemos veiklos tęstinumas ir saugus naudotojų darbas.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

19. Naudotojų prieigos prie informacinės sistemos suteikimo tvarka nustatyta Kauno miesto savivaldybės informacinės sistemos naudotojų administravimo taisyklėse.

20. Prieiga naudotojams suteikiama tik prie tų išteklių, kurie yra būtini tiesioginėms pareigoms atlikti.

21. Naudotojų naudojama kompiuterinė technika skirta tik naudotojų tiesioginėms pareigoms atlikti.

22. Naudotojams draudžiama patiems diegti bet kokią programinę įrangą. Programinę įrangą, reikalingą naudotojo funkcijoms atlikti, diegia ir prižiūri Informacinių technologijų skyriaus darbuotojai arba informacinės sistemos posistemių administratoriai, išskyrus programinę įrangą nešiojamuosiuose kompiuteriuose, perduotuose naudotis Savivaldybės tarybos nariams jų kadencijos laikotarpiui.

23. Naudotojams gali būti suteikiama nuotolinio prisijungimo prie informacinės sistemos galimybė.

24. Nuotoliniam prisijungimui prie informacinės sistemos taikomi saugumo reikalavimai turi būti ne žemesni, nei taikomi prisijungimui prie vidinio Savivaldybės kompiuterių tinklo.

25. Serveriuose ir naudotojų kompiuteriuose turi būti naudojama programinė įranga, skirta apsaugoti informacinę sistemą nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.) (toliau – antivirusinė programinė įranga). Antivirusinė programinė įranga turi būti atnaujinama kiekvieną dieną.

26. Savivaldybės kompiuterių tinklas turi būti užkarda atskirtas nuo viešųjų telekomunikacijų tinklų.

27. Duomenų kopijų darymo tvarka nustatyta Saugaus elektroninės informacijos tvarkymo Kauno miesto savivaldybės informacinėje sistemoje taisyklėse.

28. Duomenys automatinio būdu gali būti teikiami ir (ar) gaunami tik laikantis duomenų teikimo ir (ar) gavimo sutartyse nustatytos tvarkos arba teisės aktuose numatytais atvejais.

IV. REIKALAVIMAI PERSONALUI

29. Naudotojai privalo rūpintis tvarkomos informacijos saugumu.

30. Naudotojai turi būti susipažinę su šiais saugumo nuostatais ir saugumo politiką įgyvendinančiais dokumentais.

31. Saugumo įgaliotinis privalo išmanyti informacijos saugumo užtikrinimo principus, savo darbe vadovautis teisės aktais, standartais ir kitais su informacijos saugumu susijusiais dokumentais, reglamentuojančiais saugų informacijos tvarkymą.

32. Administratorius privalo išmanyti informacijos saugumo principus, darbą su kompiuterių tinklais, mokėti užtikrinti jų saugumą, taip pat administruoti ir prižiūrėti duomenų bazes, turi būti susipažinęs su saugumo nuostatais ir saugumo politiką įgyvendinančiais dokumentais.

33. Naudotojai turi turėti kvalifikaciją (informacinių technologijų naudotojų kvalifikacijos kursai, pradinis saugaus darbo su informacija mokymas, ECDL (Europos kompiuterio naudotojo pažymėjimas), naudotojo sertifikatas ar pan.) ir patirties dirbant su atitinkamomis operacinėmis sistemomis ir taikomosiomis programomis.

34. Viešosios vadybos ir personalo skyrius organizuoja naudotojų mokymus duomenų saugumo klausimais.

V. NAUDOTOJŲ SUPAŽINDINIMAS SU SAUGUMO DOKUMENTAIS

36. Už naudotojų supažindinimą pasirašytinai su šiais saugumo nuostatais, saugumo politiką įgyvendinančiais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą yra atsakingi Savivaldybės administracijos padalinių vadovai.

37. Saugumo nuostatai ir saugumo politiką įgyvendinantys dokumentai yra skelbiami naudotojams skirtame Savivaldybės svetainės tinklalapyje.

VI. BAIGIAMOSIOS NUOSTATOS

38. Saugumo nuostatai yra privalomi saugumo įgaliotiniui, administratoriui ir naudotojams.

39. Naudotojai, pažeidę šių saugumo nuostatų ar saugumo politiką įgyvendinančių dokumentų reikalavimus, atsako teisės aktų nustatyta tvarka.
