PATVIRTINTA
Kelmės rajono savivaldybės
administracijos direktoriaus
2016 m. d. įsakymu Nr.

KELMĖS RAJONO SAVIVALDYBĖS ADMINISTRACIJOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kelmės rajono savivaldybės administracijos (toliau vadinama – Administracija) informacinės sistemos (toliau vadinama – IS) saugaus elektroninės informacijos taisyklių (toliau – Taisyklės) tikslas – nustatyti tvarką, kuria vadovaujantis būtų saugiai tvarkoma administracijos IS saugoma bei apdorojama įstaigos informacija bei saugiai automatizuotu būdu tvarkomi administracijos veiklos ir buhalterinės apskaitos duomenys administracijos informacinėse sistemose (toliau vadinama – Sistema).

2. Taisyklės reglamentuoja Sistemos automatizuotą duomenų apdorojimą ir yra privalomos visiems Administracijos valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau – sistemos naudotojas), sistemos tvarkytojo įstaigoje.

3. Taisyklėse vartojamos sąvokos atitinka teisės aktuose, kuriais vadovaujantis parengtos šios taisyklės, ir kituose saugų elektroninės informacijos bei duomenų tvarkymą reglamentuojančiuose teisės aktuose apibrėžtas sąvokas.

4. Už Taisyklių įgyvendinimą ir jų laikymosi kontrolę atsakingas Administracijos IS saugos įgaliotinis.

5. Administracijos IS saugomą bei apdorojamą informaciją sudaro:

5.1. raštvedybos duomenys;

5.2. administracijos vidaus dokumentai;

5.3. IS vartotojų duomenys;

5.4. buhalterinės apskaitos duomenys.

6. Vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo 4.3 papunkčiu, Registre tvarkoma informacija priskiriama žinybinės svarbos elektroninės informacijos kategorijai.

7. Už informacinėje sistemoje tvarkomos elektroninės informacijos (jos grupių), priskirtų žinybinės svarbos elektroninės informacijos kategorijai, tvarkymą atsakingi:

7.1. IS administratoriai;

7.2. IS naudotojai.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

8. Saugiam Administracijos IS elektroninės informacijos tvarkymui užtikrinti naudojamos kompiuterinės įrangos, programinės įrangos, fizinės, techninės ir organizacinės duomenų saugos priemonės, kurių pagalba:

8.1. per metus informacinės sistemos prieinamumas turi būti užtikrintas ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis;

8.2. informacinės sistemos neveikimo laikotarpis negali būti ilgesnis nei trečios kategorijos informacinės sistemos – 16 val.

9. Kompiuterinės įrangos saugos priemonės:

9.1. prieigos prie Administracijos IS tarnybinių stočių (serverių) kontrolė užtikrinama suteikiant prieigos teises tik autorizuotiems asmenims, kuriems pagal atliekamas funkcijas prieiga

prie Administracijos IS tarnybinių stočių turi būti suteikta, o jų veiksmai, užtikrinantys Administracijos IS duomenų apsaugą, aprašyti Administracijos IS duomenų saugos nuostatuose;

9.2. Administracijos IS administratoriaus ir vidinių Administracijos IS vartotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės; šios priemonės automatiškai turi informuoti darbo vietų administratorių apie tai, kuriems kompiuteriams yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas;

9.3. turi būti operatyviai ištestuojami ir įdiegiami Administracijos IS tvarkytojo darbuotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; darbo vietų administratoriai reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie vidinių Administracijos IS tvarkytojo darbuotojų darbo vietų kompiuterinei įrangai neįdiegtus rekomenduojamus gamintojų atnaujinimą ir susijusius saugos pažeidžiamumo svarbos lygius;

9.4. Administracijos IS administratoriui pateikus tiesioginio vadovo patvirtintą prašymą, gali būti suteikiama teisė naudoti kompiuterius tiesioginėms pareigoms atlikti ne Administracijos IS tvarkytojo patalpose;

9.5. nuotolinis prisijungimas prie Administracijos IS turi būti vykdomas protokolu, skirtu duomenų šifravimui.

10. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

10.1. Administracijos IS darbo stotyse ir vidinių naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga;

10.2. vidinių naudotojų kompiuterinėje įrangoje naudojamos autorizuotos programinės įrangos sąrašą rengia ir reguliariai atnaujina Administracijos IS administratorius;

10.3. Administracijos IS tarnybinių stočių techninė ir programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų;

10.4. Administracijos IS tarnybinių stočių techninės ir programinės įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai;

10.5. programinę įrangą turi diegti tik Administracijos IS tvarkytojo vadovo įgalioti asmenys;

10.6. neatliekant jokių veiksmų su Administracijos IS 15 minučių, Administracijos IS taikomoji programinė įranga turi užsirakinti, kad toliau naudotis Administracijos IS galima būtų tik pakartotinai patvirtinus savo tapatybę;

10.7. Administracijos IS tarnybinėse stotyse turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės; šios priemonės automatiškai turi informuoti Administracijos IS administratorius apie tai, kuriems Administracijos IS posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas; Administracijos IS komponentai be kenksmingo programinės įrangos aptikimo priemonių gali būti eksploatuojami tik jeigu rizikos vertinimo metu yra patvirtinama, kad šių komponentų rizika yra priimtina;

10.8. turi būti operatyviai ištestuojami ir įdiegiami Administracijos IS tarnybinių stočių įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; Administracijos IS administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie Administracijos IS posistemiams, funkciškai savarankiškoms sudedamosioms dalims neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius;

10.9. Administracijos IS tarnybinėse stotyse turi būti įjungtos ugniasienės, sukonfigūruotos praleisti tik su Administracijos IS funkcionalumu ir administravimu susijusį duomenų srautą;

10.10. Administracijos IS programinė įranga turi būti testuojama naudojant atskirą testavimui skirtą aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintų Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71(1.12) 14.8 punkto reikalavimais (toliau – Bendrieji reikalavimai organizacinėms ir techninėms duomenų saugumo priemonėms).

11. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

11.1. Administracijos IS naudotojas internetu jungiasi prie ugniasiene apsaugotų tarnybinių stočių, naudodamas unikalius identifikacinius prisijungimo duomenis;

11.2. Administracijos IS tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių Administracijos IS vartotojų kompiuterinę įrangą nuo kenksmingo kodo;

11.3. viešaisiais ryšių tinklais perduodamos Administracijos IS elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą, virtualų privatų tinklą ar kitas priemones;

11.4. duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima;

11.5. duomenų centro ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo ir pažeidimo.

12. Patalpų, kuriose veikia Administracijos IS tarnybinės stotys ir aplinkos saugumo užtikrinimo priemonės:

12.1. Administracijos IS tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas;

12.2. techninė įranga įnešama ir išnešama iš patalpų tik leidus autorizuotam asmeniui, kuriam pagal atliekamas funkcijas suteikta prieiga prie Administracijos IS tarnybinių stočių;

12.3. Administracijos IS tarnybinių stočių patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir (arba) apsaugos tarnybos stebėjimo pulto;

12.4. periodiškai atliekama gaisro gesinimo priemonių patikra;

12.5. svarbiausia kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne mažiau kaip 30 min.;

12.6. Administracijos IS tarnybinių stočių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga;

12.7. įgyvendintos įrangos gamintojų nustatytos techninės įrangos darbo sąlygos;

12.8. visose patalpose, kuriose yra vidinių Administracijos IS naudotojų ir Administracijos IS techninė įranga, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

12.9. tarnybinių stočių patalpos turi atskirą elektroninę perimetro kontrolės sistemą;

12.10. įrengta tam skirtų patalpų apsaugos signalizacija, kurios signalai pasibaigus darbo dienai, taip pat poilsio ir švenčių dienomis persiunčiami patalpas saugančiai tarnybai;

12.11. kiti darbuotojai į patalpas patenka tik lydimi Administracijos IS administratoriaus arba paskirto už patalpų kontrolę asmens;

12.12. įvykus apsaugos sistemos gedimui, pildomas įėjimo punkto žurnalas, nurodant pateikimo priežastį, pradžią ir pabaigą; žurnalas saugomas ne trumpiau kaip 1 metus;

12.13. įvykių žurnalas privalo būti pateiktas duomenų saugos įgaliotiniui pareikalavus;

12.14. lankytojams ir svečiams privaloma atsakingo darbuotojo palyda;

12.15. už apsilankymą atsakingas darbuotojas registruoja lankytojų ir svečių apsilankymo duomenis ir pasirašo įėjimo punkto žurnale;

12.16. į duomenų centrą savarankiškai patekti gali tiktai Administracijos IS duomenų bazės administratorius, duomenų saugos įgaliotinis ir kiti specialius leidimus turintys darbuotojai, kuriuos patvirtina pagrindinis Administracijos IS tvarkytojas;

12.17. prieš patenkant į patalpas po 22 val. ir iki 7 val. ir ne darbo dienomis, darbuotojas privalo informuoti saugos tarnybą (apsaugos darbuotoją).

13. Administracijos IS darbo apskaitos ir kitos elektroninės informacijos saugos priemonės:

13.1. Administracijos IS tarnybinių stočių įvykių žurnaluose turi būti registruojami ir ne mažiau kaip vienerius metus saugomi duomenys, nurodant įvykio datą ir laiką, apie:

13.2. Administracijos IS įjungimą ir išjungimą;

13.3. pagrindinių sisteminių komponentų (atminties, procesorių ir duomenų saugyklų bei duomenų bazių) apkrovas, viršijančias nustatytas leistinas reikšmes;

13.4. bandymus prieiti prie Administracijos IS administravimo komponentų;

13.5. kitus svarbius su Administracijos IS tvarkomos elektroninės informacijos sauga susijusius įvykius pagal suderintą su Administracijos IS administratoriumi ir duomenų saugos įgaliotiniu sąrašą.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

14. Administracijos IS duomenų keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

14.1. Administracijos IS duomenų keitimą, atnaujinimą, įvedimą ir naikinimą gali atlikti tik tam turintys teisę autorizuoti naudotojai;

14.2. Administracijos IS saugomi ir apdorojami raštvedybos duomenys ir vidaus dokumentai įvedami, atnaujinami, keičiami ir naikinami vadovaujantis Lietuvos vyriausiojo archyvaro 2011 m. liepos 4 d. įsakymu Nr. V-118 patvirtintomis dokumentų tvarkymo ir apskaitos taisyklėmis;

14.3. Administracijos IS saugomi ir apdorojami buhalterinės apskaitos duomenys įvedami, atnaujinami, keičiami ir naikinami vadovaujantis Lietuvos Respublikos buhalterinės apskaitos įstatymu;

14.4. Administracijos IS duomenys įrašomi, atnaujinami, keičiami ir naikinami vadovaujantis Administracijos IS nuostatais ir Administracijos IS duomenų saugos nuostatais;

14.5. už Administracijos IS duomenų saugą pagal kompetenciją Lietuvos Respublikos įstatymų nustatyta tvarka atsako Administracijos IS valdytojas ir Administracijos IS tvarkytojas;

14.6. visi Administracijos IS naudotojai, kurie tvarko asmens duomenis, privalo saugoti asmens duomenų paslaptį, jeigu šie asmens duomenys neskirti skelbti viešai. Ši pareiga galioja ir perėjus dirbti į kitas pareigas arba pasibaigus darbo ar sutartiniams santykiams;

14.7. Administracijos IS asmens duomenų saugumas užtikrinamas vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms.

15. Administracijos IS naudotojų veiksmų registravimo tvarka:

15.1. siekiant nustatyti neteisėtus veiksmus su Administracijos IS saugoma ir apdorojama elektronine informacija bei šios informacijos vientisumo pažeidimus naudotojų veiksmai, jų darbo su IS laikas turi būti automatiškai registruojami elektroniniuose žurnaluose.

16. Atsarginių elektroninės informacijos kopijų darymo tvarka:

16.1. IS atsarginių duomenų kopijos programinėmis priemonėmis daromos kiekvieną darbo dieną;

16.2. pakartotinės IS atsarginių duomenų kopijos daromos prieš ir po posistemių programinio atnaujinimo ar įvedus didelį kiekį naujos elektroninės informacijos;

16.3. atsarginės duomenų kopijos įrašomos ir saugomos tam skirto kompiuterio kietajame diske;

16.4. atsarginės elektroninės informacijos kopijos saugomos Kelmės rajono savivaldybės administracijos pastate, 222 kabinete;

16.5. atsarginės laikmenos su IS programinės įrangos kopijomis saugomos Kelmės rajono savivaldybės administracijos pastate, 222 kabinete.

16.6. naudotojui svarbių duomenų, nesaugomų duomenų bazėse, atsarginės duomenų kopijos daromos programinėmis priemonėmis numatytu laiku ir naudotojui savo nuožiūra pasirinkus pakartotinį kopijų darymą, saugomos tam skirto kompiuterio kietajame diske;

16.7. saugomos 5 paskutinių dienų atsarginių duomenų kopijos;

16.8. prarasti ar sunaikinti duomenys yra atkuriami iš atsarginių duomenų kopijų per 48 valandas;

16.9. IS naudotojas yra atsakingas už savo kompiuteryje saugomų duomenų išsaugojimą;

16.10. IS administratorius yra atsakingas už atsarginių duomenų kopijų darymą, duomenų atkūrimą ir atsarginių duomenų kopijų apsaugą;

16.11. duomenų saugos įgaliotinis atsakingas už atsarginių duomenų saugojimo kontrolę.

17. Elektroninės informacijos perkėlimo ir teikimo susijusioms informacinėms sistemoms ir elektroninės informacijos gavimo iš jų užtikrinimo tvarka:

17.1. naudotojams iš Administracijos IS gautus duomenis nėra draudžiama perkelti į savo IS, jei tai neprieštarauja teisės aktams;

17.2. Administracijos IS elektroninė informacija institucijoms, kitiems juridiniams ir fiziniams asmenims teikiama vadovaujantis Asmens duomenų tvarkymo Kelmės rajono savivaldybės administracijoje taisyklėmis;

17.3. Administracijos IS tvarkomi duomenys teikiami ir naudojami vadovaujantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais;

17.4. duomenų mainai tarp Administracijos IS ir susijusių registrų bei kitų informacinių sistemų vykdomi su šių registrų ir informacinių sistemų valdytojais sudarytose duomenų teikimo sutartyse numatytais būdais, terminais ir numatyta apimtimi;

17.5. duomenys sistemos nuostatuose patvirtintiems duomenų gavėjams teikiami neatlygintinai, išskyrus atvejus, kai reikalingas papildomas duomenų apdorojimas arba darbai atliekami skubos tvarka;

17.6. duomenys Europos Sąjungos valstybių narių ir (arba) Europos ekonominės erdvės valstybių, trečiųjų šalių fiziniams ir juridiniams asmenims, juridinio asmens statuso neturintiems subjektams, jų filialams ir atstovybėms teikiami Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo nustatyta tvarka;

17.7. už Administracijos IS elektroninės informacijos perdavimą į registrus ir kitas informacines sistemas bei gavimą iš jų yra atsakingas Administracijos IS tvarkytojas.

18. Duomenų neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau vadinama – neleidžiama veikla) nustatymo tvarka:

18.1. Administracijos IS administratoriai privalo naudoti visas įmanomas aparatines, programines ir administracines priemones skirtas apsisaugojimui nuo neleidžiamos veiklos;

18.2. kilus įtarimui, kad su Administracijos IS ir/arba jose saugomais ir apdorojamais duomenimis yra vykdoma neleidžiama veikla, Administracijos IS administratorius nedelsiant privalo apie tai informuoti saugos įgaliotinį;

18.3. Administracijos IS saugos įgaliotinis, gavęs pranešimą apie neleidžiamą veiklą inicijuoja IS saugos incidentų valdymo procedūrą vykdymą.

19. Programinės įrangos diegimo ar atnaujinimo, IS kompiuterių techninės įrangos keitimo ar perkėlimo (toliau – pakeitimai) tvarka:

19.1. IS pakeitimai gali būti atliekami tik IS valdytojui raštiškai pritarus;

19.2. turi būti laikomasi oficialių įforminimo, testavimo, įgyvendinimo procedūrų atliekant svarbius pokyčius esamoje sistemoje ar diegiant naujus;

19.3. prieš atliekant IS pakeitimus, kurių metu gali iškilti grėsmė duomenų konfidencialumui, vientisumui ar pasiekiamumui, IS administratorius turi ištestuoti atliekamus pakeitimus esant techninei galimybei;

19.4. atlikus vykdomų IS pakeitimų testavimą arba jei testavimo darbų dėl programinių ir/ar techninių priežasčių nebuvo galima atlikti, IS administratorius gali pradėti įgyvendinti IS pakeitimus;

19.5. įgyvendinant IS pakeitimus, kurių metu galimi IS veikimo sutrikimai, IS administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki planuojamų IS pakeitimų vykdymo pradžios informuoti IS naudotojus apie tokių darbų pradžią ir galimus IS veiklos sutrikimus;

19.6. IS administratorius naudotojams privalo pateikti visą reikalingą informaciją apie naudojimosi IS pakitimus, kurių atsiradimas susijęs su įvykdytais arba vykdomais IS pakeitimais.

19.7. Programinė įranga turi būti testuojama naudojant atskirą testavimui skirtą aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms.

19.8. programinės įrangos testavimas atliekamas imantis elektroninės informacijos saugos priemonių, numatytų šių taisyklių 14 punkte.

19.9. atlikęs vykdomų Administracijos IS pokyčių testavimą, Administracijos IS duomenų bazės administratorius gali pradėti įgyvendinti Administracijos IS pokyčius tik gavęs patvirtinimą ir suderinęs pokyčio diegimo grafiką su Administracijos IS valdytoju.

20. Informacinės sistemos pokyčių valdymas:

20.1. visi pokyčiai, įskaitant ir avarinę priežiūrą ir pataisas, susijusias su infrastruktūra ir taikomosiomis programomis darbinėje aplinkoje, valdomi ir kontroliuojami;

20.2. pokyčių (procedūrų, procesų, sistemų ir paslaugų parametrų) valdymas ir kontrolė įgyvendinama juos registruojant, vertinant, vykdomi gavus raštišką IS valdytojo pritarimą, po įgyvendinimo juos peržiūrint ir lyginant su planuotais rezultatais. Tai užtikrina pokyčių neigiamo poveikio informacinių sistemų stabilumui ar vientisumui rizikos mažinimą;

20.3. visi pokyčiai, galintys sutrikdyti ar sustabdyti informacinės sistemos darbą, turi būti suderinti su IS valdytoju, saugos įgaliotiniu ir administratoriumi ir vykdomi tik gavus jų raštišką pritarimą. Pokyčius turi teisę inicijuoti IS valdytojas, duomenų saugos įgaliotinis ir administratorius, o įgyvendinti – administratorius;

20.4. atlikdamas IS funkcijų pakeitimus, administratorius turi laikytis IS valdytojo nustatytos informacinės sistemos pokyčių valdymo tvarkos, numatytos šiose Taisyklėse;

20.5. Administracijos IS valdytojas turi užtikrinti efektyvų ir spartų informacinės sistemos funkcijų pokyčių valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas, įtakos vertinimą ir pokyčių prioritetų nustatymo procesus;

20.6. pokyčių inicijavimas dokumentuojamas, vertinimas, įgyvendinimas, pildomas keitimų žurnalas;

20.7. sprendimus dėl Administracijos IS pokyčių priima IS valdytojas, kuris nustato pokyčių prioritetus ir avarinių pakeitimų valdymą. Priėmus sprendimą įgyvendinti Administracijos IS funkcinį pokytį, jis užduočių valdymo sistemoje priskiriamas vykdytojui, taip pat stebimas pokyčio įgyvendinimas.

21. Tvarkyti Sistemos duomenis gali tik Sistemos naudotojai, susipažinę su šiomis taisyklėmis ir kitais saugumo politiką reglamentuojančiais teisės aktais bei raštiškai sutikę laikytis šių teisės aktų reikalavimų.

22. Sistemos naudotojų supažindinimą su Taisyklėmis ir kitais saugumo politiką reglamentuojančiais teisės aktais bei atsakomybę už šių reikalavimų nesilaikymą pasirašytinai organizuoja saugos įgaliotinis.

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

24. Sistemos naudotojai, pažeidę šių taisyklių ar kitą saugumo politiką reglamentuojančių teisės aktų reikalavimus, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

IV SKYRIUS
REIKALAVIMAI, KELIAMI TARNYBOS IS FUNKCIONAVIMUI REIKALINGOMAS PASLAUGOMS IR JŲ TIEKĖJAMS

25. Paslaugų teikėjų prieigos prie Administracijos IS lygiai ir sąlygos:

25.1. Administracijos IS administratorius suteikia prieigos prie Administracijos IS duomenų teisę (peržiūrėti Administracijos IS duomenis, atlikti užklausas Administracijos IS, vykdyti veiksmus su Administracijos IS duomenimis ir kt.), o Administracijos IS duomenų bazės administratorius suteikia tik būtiną paslaugų atlikimui fizinę prieigą prie duomenų, techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nustatytiems laikotarpiui ir sąlygomis ;

25.2. Administracijos IS administratorius, suteikdamas prieigos prie Administracijos IS duomenų teisę, paslaugų teikėjo įgaliotą fizinį asmenį supažindina su prieigos prie Administracijos IS duomenų sąlygomis ir vykdo sutartyje nustatytų saugos reikalavimų vykdymo priežiūrą;

25.3. pasibaigus sutartyje nurodytam laikotarpiui, Administracijos IS pagrindinis administratorius panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie Administracijos IS duomenų teisę ir apie tai jį informuoja. Duomenų saugos (konfidencialumo) įsipareigojimai galioja ir po sutarties įgyvendinimo pabaigos.

26. Reikalavimai, keliami paslaugų teikėjų patalpoms, įrangai, informacinių sistemų priežiūrai, elektroninės informacijos perdavimui tinklais ir kitoms paslaugoms:

26.1. užtikrinamas patalpų, kuriose saugomi asmens duomenys, saugumas;

26.2. užtikrinamas tik įgaliotų asmenų patekimas į atitinkamas patalpas;

26.3. paslaugų teikimo sutartyje turi būti nurodoma, kad paslaugų teikėjas:

26.3.1. kuria ar modifikuoja Administracijos IS taikomąją programinę įrangą, naudodamas įgyvendintas elektroninės informacijos saugos nuo nesankcionuoto poveikio sisteminei, programinei įrangai ir patalpoms priemones;

26.3.2. Administracijos IS testavimo duomenų bazės duomenis;

26.3.3. Administracijos IS kūrimui ir testavimui skirtą infrastruktūrą;

26.3.4. prisijungimui nuotoliniu būdu prie Administracijos IS aplinkų laikosi Administracijos IS duomenų saugos nuostatuose keliamų reikalavimų;

26.3.5. darbui naudoja tik legalią sisteminę programinę įrangą;

26.3.6. laikosi šių taisyklių, Administracijos IS duomenų saugos nuostatų ir Administracijos IS naudotojų administravimo taisyklėse nustatytų pareigų Administracijos IS administratoriams ir vidiniams naudotojams.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

27. Siekdamas, kad būtų užtikrinta taisyklėse išdėstytų nuostatų įgyvendinimo kontrolė, saugos įgaliotinis kasmet organizuoja auditą ne vėliau kaip iki tų metų gruodžio 1 d., kurio metu:

27.1. įvertinama Taisyklių ir kitų saugumo politiką reglamentuojančių teisės aktų atitiktis realiai duomenų saugos situacijai;

27.2. inventorizuojama Sistemos tvarkytojo techninė ir programinė įranga;

27.3. tikrinamos ne mažiau kaip 10 procentų sistemos vartotojų kompiuterinių darbo vietų ir visuose paslaugų kompiuteriuose įdiegtos programos ir jų konfigūracija;

27.4. peržiūrima Sistemos vartotojams suteiktų teisių atitiktis vykdomoms funkcijoms;

27.5. įvertinamas pasirengimas Sistemos veiklos atnaujinimui nenumatytais atvejais.

28. Atlikus auditą rengiamas pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Administracijos IS tvarkytojo vadovas.

29. Saugos įgaliotinis, siekdamas užtikrinti Sistemos ir joje tvarkomų duomenų saugumą, teikia siūlymus Sistemos tvarkytojo vadovui dėl Taisyklių keitimo ar kitų saugumo politiką reglamentuojančių teisės aktų priėmimo, keitimo ar panaikinimo.

30. Taisyklės ir kiti saugumo politiką reglamentuojantys teisės aktai iš esmės peržiūrimi ir prireikus keičiami ne rečiau kaip kartą per metus, atliekant šių taisyklių V skyriuje nurodytą auditą.

31. Sistemos tvarkytojas, Administracijos IS duomenų valdymo ir duomenų saugos įgaliotinis, Administracijos IS administratoriai ir naudotojai, pažeidę šių taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____

SUDERINTA
Vidaus reikalų ministerijos
2016 m. d. raštu Nr.

Kelmės rajono savivaldybės administracijos
saugaus elektroninės informacijos tvarkymo taisyklių
priedas

KELMĖS RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DUOMENŲ CENTRO LANKYTOJŲ REGISTRAVIMO ŽURNALAS

Pradėta 2016 m. _____ ___d.

Eil. Nr.	Data	DC atidarė Vardas, pavardė, parašas	Lankytojas Vardas, pavardė, parašas	Lankymo tikslas	Įėjimo laikas	Išėjimo laikas
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						
17.						
18.						
19.						
20.						
21.						
22.						