Elektroninio dokumento nuorašas

ŠIRVINTŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS DIREKTORIUS

ĮSAKYMAS DĖL ŠIRVINTŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2023 m. d. Nr.
Širvintos

Vadovaudamasi Lietuvos Respublikos vietos savivaldos įstatymo 34 straipsnio 1 dalimi, Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto 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“, 7 punkto 7.1 papunkčiu, 11, 19 ir 26 punktais:

1. T v i r t i n u Širvintų rajono savivaldybės administracijos informacinės sistemos duomenų saugos nuostatus (pridedama).

2. S k i r i u:

2.1. Širvintų rajono savivaldybės administracijos informacinės sistemos administratoriais Bendrojo skyriaus vyriausiąjį specialistą Gediminą Masiulį ir Bendrojo skyriaus specialistą (informacinių technologijų techniką) Marių Lukošių.

2.2. Širvintų rajono savivaldybės administracijos informacinės sistemos saugos įgaliotine Bendrojo skyriaus vedėją Dianą Mičelienę.

3. Į p a r e i g o j u :

3.1. Bendrojo skyriaus vyriausiąjį specialistą Gediminą Masiulį ir Bendrojo skyriaus specialistą (informacinių technologijų techniką) Marių Lukošių ne vėliau kaip per 6 mėnesius nuo šio įsakymo įsigaliojimo dienos parengti, suderinti su Nacionalinio kibernetinio saugumo centru prie Krašto apsaugos ministerijos ir pateikti Širvintų rajono savivaldybės administracijos direktoriui tvirtinti saugos politiką įgyvendinančius dokumentus – Saugaus elektroninės informacijos tvarkymo taisykles, Informacinės sistemos veiklos tęstinumo valdymo planą ir Informacinės sistemos naudotojų administravimo taisykles.

3.2. Bendrojo skyriaus specialistą (informacinių technologijų techniką) Marių Lukošių supažindinti su šiuo įsakymu Savivaldybės administracijos darbuotojus per dokumentų valdymo

sistemą „Kontora“.

4. P r i p a ž į s t u netekusiu galios Širvintų rajono savivaldybės administracijos direktoriaus 2017 m. gruodžio 21 d. įsakymą Nr. 9-979 „Dėl Širvintų rajono savivaldybės administracijos informacinės sistemos duomenų saugos“.

Šis įsakymas gali būti skundžiamas Lietuvos Respublikos administracinių bylų teisenos įstatymo nustatyta tvarka.

Administracijos direktorė Ingrida Baltušytė

PARENGĖ:

Bendrojo skyriaus specialistas
(informacinių technologijų technikas)

Marius Lukošius

SUDERINTA:

Bendrojo skyriaus vedėja

Diana Mičelienė

Teisės, personalo ir civilinės metrikacijos
skyriaus vedėjo pavaduotoja

Vaida Šeipūnė

Švietimo ir kultūros skyriaus vedėja

Rasa Kralikevičienė

PATVIRTINTA
Širvintų rajono savivaldybės administracijos
direktoriaus 2023 m. d.
įsakymu Nr.

ŠIRVINTŲ RAJONO SAVIVALDYBĖS ADMINISTRACIJOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Širvintų rajono savivaldybės administracijos informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato tvarkomos elektroninės informacijos saugos tikslus, elektroninės informacijos saugos užtikrinimo prioritetines kryptis, saugų elektroninės informacijos valdymą, organizacinius, techninius ir personalui keliamus reikalavimus, naudotojų supažindinimo su saugos dokumentais principus, apibrėžia elektroninės informacijos saugos politiką.

2. Saugos politika įgyvendinama vadovaujantis saugaus elektroninės informacijos tvarkymo taisyklėmis, informacinių sistemų veiklos tęstinumo valdymo planu, naudotojų administravimo taisyklėmis ir kitais teisės aktais, reglamentuojančiais informacinės sistemos duomenų tvarkymo teisėtumą ir saugų duomenų valdymą.

3. Saugos nuostatuose vartojamos sąvokos:

3.1. **Elektroninė informacija** (toliau – informacija) – visa informacija, kuri tvarkoma informacinių technologijų priemonėmis. Tai programos, failai ir kita informacija, kuri saugoma, perduodama ir sukuriama kompiuteriu.

3.2. **Elektroninės informacijos saugos politika** (toliau – saugos politika) – pagrindiniai elektroninės informacijos saugos užtikrinimo ir valdymo principai, reikalavimai, į kuriuos atsižvelgiant turi būti derinami informacinės sistemos veiklos ir naudojimo procesai, procedūros ir rengiami juos reglamentuojantys dokumentai. Saugos politika išdėstoma informacinės sistemos valdytojo tvirtinamuose Saugos nuostatuose.

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

3.4. **Informacijos saugos incidentas** (toliau – saugos incidentas) – įvykis ar veiksmas, kurie gali sudaryti neteisėto prisijungimo prie informacinės sistemos galimybę, sutrikdyti ar pakeisti informacinės sistemos veiklą, sunaikinti, sugadinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, sudaryti sąlygas neleistinai elektroninę informaciją pasisavinti, paskleisti ar kitaip panaudoti.

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

3.6. **Informacinės sistemos administratorius** (toliau – administratorius) – Širvintų rajono savivaldybės administracijos (toliau – Savivaldybės administracija) valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, prižiūrintis informacinę sistemą ir (ar) jos infrastruktūrą, užtikrinantis jos veikimą ir elektroninės informacijos saugą, ar kitas asmuo (asmenų grupė), kuriam (kuriai) Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos informacinės sistemos ir (ar) jos infrastruktūros priežiūros funkcijos.

3.7. **Informacinės sistemos naudotojas** – Savivaldybės administracijos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, ar kitas asmuo, informacinių sistemų veiklą reglamentuojančių teisės aktų nustatyta tvarka pagal kompetenciją naudojantis ir (ar) tvarkantis elektroninę informaciją.

3.8. **Informacinės sistemos saugos įgaliotinis** (toliau – saugos įgaliotinis) – Savivaldybės administracijos valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, koordinuojantis ir prižiūrintis saugos politikos įgyvendinimą informacinėje sistemoje.

3.9. **Konfidencialumas** – elektroninės informacijos savybė – su informacinėje sistemoje tvarkoma elektronine informacija gali susipažinti tik tą daryti įgalioti asmenys.

3.10. **Prieinamumas** – elektroninės informacijos savybė – elektroninė informacija gali būti tvarkoma reikiamu metu.

3.11. **Vientisumas** – elektroninės informacijos savybė – elektroninė informacija nebuvo atsitiktinai ar neteisėtai pakeista ar sunaikinta.

3.12. **Savivaldybės administracijos informacinė sistema** (toliau – IS) apibrėžiama kaip informacijos apdorojimo sistemos ir Savivaldybės administracijos išteklių (pačios informacijos, žmonių, techninių priemonių, finansų ir pan.) visuma, skirta informacijai apdoroti, formuoti (kurti), skleisti (siųsti ir gauti).

3.13. Saugos nuostatuose vartojamos sąvokos apibrėžtos 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“, Lietuvos Respublikos standartuose LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, 2010 m. paprojekčio „Lietuvos ir Norvegijos savivaldos asociacijų ir savivaldybių bendradarbiavimo stiprinimas savivaldybių ir elektroninės valdžios paslaugų plėtojimo srityje“ parengtame leidinyje. Kitos saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip saugų duomenų tvarkymą reglamentuojančiuose Lietuvos Respublikos teisės aktuose, Lietuvos bei tarptautiniuose standartuose.

4. IS elektroninės informacijos sauga užtikrinama vadovaujantis šiomis prioritetinėmis kryptimis:

4.1. įgyvendinant atliekamų veiksmų su IS elektronine informacija įrašų kaupimą;

4.2. kopijuojant IS duomenų bazę, saugant archyve esančias kopijas;

4.3. saugant IS elektroninę informaciją nuo žalingos programinės įrangos poveikio;

4.4. įrengiant saugias informacinei sistemai tvarkyti skirtas patalpas ir kompiuterizuotas darbo vietas jose;

4.5. tobulinant IS naudotojų kvalifikaciją;

4.6. įgyvendinant IS elektroninės informacijos integralumą su registrais ir informacinėmis sistemomis;

4.7. įgyvendinant IS veiklos tęstinumą;

4.8. užtikrinant informacijos konfidencialumą;

4.9. užtikrinant teisėtą ir saugų asmens duomenų naudojimą.

5. IS elektroninės informacijos saugos užtikrinimo tikslas – sudaryti sąlygas automatizuotu būdu saugiai rinkti, apdoroti, kaupti, saugoti elektroninę informaciją ir ją teikti archyvo registrams, informacinėms sistemoms, suinteresuotiems juridiniams ir fiziniams asmenims.

6. Saugos nuostatai, saugaus elektroninės informacijos tvarkymo taisyklės, veiklos tęstinumo valdymo planas, naudotojų administravimo taisyklės (toliau visi kartu – IS saugos dokumentai) privalomi:

6.1. IS valdytojui – Savivaldybės administracijai, Vilniaus g. 61, LT-19120 Širvintos;

6.2. IS tvarkytojui – Savivaldybės administracijos struktūriniams padaliniams;

6.3. IS naudotojams – Savivaldybės administracijos valstybės tarnautojams, darbuotojams, dirbantiems pagal darbo sutartį;

6.4. saugos įgaliotiniui;

6.5. administratoriui.

7. IS valdytojas:

7.1. pagal kompetenciją atsako už saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą;

7.2. tvirtina IS saugos dokumentus ir kitus teisės aktus, kuriuose reglamentuojamas IS tvarkymo teisėtumas ir IS elektroninės informacijos sauga;

7.3. skiria saugos įgaliotinį, paveda jam organizuoti IS saugos politiką ir kontroliuoti jos įgyvendinimą;

7.4. analizuoja saugos įgaliotinio pateiktus siūlymus, priima sprendimus dėl IS techninių ir programinių priemonių, būtinų IS elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

7.5. kontroliuoja, kad informacinė sistema būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, Saugos nuostatais, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu 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), 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas) ir kitais elektroninės informacijos saugos valdymą reglamentuojančiais teisės aktais ir standartais;

7.6. įgyvendina tinkamas organizacines ir technines priemones, kurios skirtos elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

7.7. užtikrina nepertraukiamą informacinės sistemos veikimą ir duomenų, esančių informacinės sistemos duomenų bazėse, saugumą ir saugų duomenų perdavimą kompiuterių tinklais;

7.8. vykdo techninių, programinių priemonių, kurios skirtos informacinei sistemai eksploatuoti, prižiūrėti ir plėtoti, įsigijimą, jų įdiegimą ir modernizavimą, informacinės sistemos techninės, programinės įrangos priežiūrą ir tobulinimą;

7.9. vykdo informacinę sistemą sudarančių informacinių išteklių inventorizaciją;

7.10. pagal kompetenciją atsako už informacinės sistemos elektroninės informacijos tvarkymo teisėtumą ir saugumą bei informacinės sistemos saugos reikalavimų atitiktį galiojantiems Lietuvos Respublikos teisės aktams.

8. IS tvarkytojas:

8.1. tvarko informaciją pagal jų veiklą reglamentuojančių įstatymų ir kitų teisės aktų reikalavimus;

8.2. teikia informaciją duomenų gavėjams;

8.3. vykdo IS saugos dokumentuose nustatytus reikalavimus ir užtikrina tinkamą duomenų saugą;

8.4. teikia pranešimus apie saugos įvykius.

9. Savivaldybės administracijos direktorius skiria informacinės sistemos saugos įgaliotinį, informacinės sistemos administratorių arba kelis administratorius, vykdančius atskiras informacinės sistemos administravimo funkcijas (toliau – administratorius), darbuotoją, administruojantį IS naudotojų prieigą prie IS elektroninės informacijos.

10. Saugos įgaliotinis:

10.1. teikia IS valdytojo vadovui siūlymus dėl IS sisteminės priežiūros ir tvarkymo administratoriaus paskyrimo ir reikalavimų jiems nustatymo;

10.2. teikia IS valdytojo vadovui siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo;

10.3. atsižvelgdamas į Nacionalinio kibernetinio saugumo centro interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“ ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto 2018 m.

rugpjūčio 13 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ V skyriuje nustatyta tvarka ne rečiau kaip kartą per metus organizuoja IS rizikos vertinimą. Pasikeitus IS duomenų bazės struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų šalinimas ir kt.) ar nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis IS rizikos vertinimas;

10.4. IS rizikos vertinimą išdėsto įvertinimo ataskaitoje. IS įvertinimo ataskaita rengiama, atsižvelgus į rizikos veiksnius, galinčius turėti ar turinčius įtakos IS elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę, galimus rizikos valdymo būdus. Svarbiausieji rizikos veiksniai yra šie:

10.4.1. 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 ir kita);

10.4.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis elektronine informacija, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

10.4.3. atsitiktinės subjektyvios aplinkybės (darbuotojų praradimas, vandens poveikis, elektros instaliacijos gedimas ir kita);

10.4.4. 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;

10.5. pateikia rizikos įvertinimo ataskaitą IS valdytojui;

10.6. atlikus informacinės sistemos informacinių technologijų saugos atitikties vertinimą, rengia pastebėtų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir nustatytų trūkumų šalinimo įgyvendinimo terminus nustato informacinės sistemos valdytojas;

10.7. koordinuoja elektroninės informacijos saugos incidentų, įvykusių informacinėse sistemose, tyrimą (išskyrus atvejus, kai šią funkciją atlieka informacijos saugos darbo grupės);

10.8. teikia sisteminės priežiūros ir tvarkymo administratoriams ir IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su IS saugos politikos įgyvendinimu;

10.9. konsultuoja naudotojus informacijos saugos klausimais;

10.10. periodiškai organizuoja IS naudotojų ir IS administratoriaus mokymą elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie elektroninės informacijos saugos problemas (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės naujiems darbuotojams ir kt.);

10.11. supažindina sisteminės priežiūros ir tvarkymo administratorius ir IS naudotojus su IS saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą, organizuoja IS naudotojų mokymą elektroninės informacijos saugos klausimais, informuoja juos apie elektroninės informacijos saugos problemas.

11. IS administratoriaus funkcijos:

11.1. užtikrina IS techninės ir programinės įrangos įdiegimą ir funkcionavimą;

11.2. diegia ir prižiūri programinę įrangą, reikalingą IS naudotojų funkcijoms vykdyti;

11.3. suteikia teisę IS naudotojams naudotis elektronine informacija, kurios reikia jų funkcijoms atlikti;

11.4. užtikrina IS komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimų aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą;

11.5. pagal kompetenciją teikia IS valdytojo vadovui siūlymus dėl IS palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

11.6. informuoja saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

11.7. atsako už IS duomenų bazės saugų atsarginių kopijų darymą ir archyve esančių kopijų

saugojimą;

11.8. reguliariai, ne rečiau kaip kartą per metus ir (arba) po informacinės sistemos pokyčio, patikrina (peržiūri) informacinės sistemos sąranką (konfigūraciją) ir informacinės sistemos būsenos rodiklius;

11.9. informuoja saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikia siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo.

12. Teisės aktai, kuriais vadovaujamasi tvarkant IS elektroninę informaciją ir užtikrinant jos saugumą:

12.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

12.2. Lietuvos Respublikos dokumentų ir archyvų įstatymas;

12.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

12.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

12.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas, Saugos dokumentų turinio gairių aprašas ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtinti 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“;

12.6. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

12.7. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

12.8. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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);

12.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

12.10. Lietuvos standartai LST ISO/IEC 27001 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai;

12.11. IS saugos dokumentai ir kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą valstybės institucijose.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto 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“, 10 punktu, Savivaldybės administracijoje tvarkoma informacija priskiriama mažiausios svarbos informacijos kategorijai.

14. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto 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“, 12.4 papunkčiu, IS priskiriamas ketvirtajai informacinių sistemų kategorijai.

15. IS elektroninei informacijai, techninei, programinei įrangai, patalpoms IS valdytojo įstaigoje vertinti naudojama penkiabalė rizikos veiksnių tikėtumo ir žalos vertinimo metodika:

15.1. nereikšminga rizikos veiksnių tikimybė, žala – 1 balas;

15.2. maža rizikos veiksnių tikimybė, žala – 2 balai;

15.3. vidutinė rizikos veiksnių tikimybė, žala – 3 balai;

15.4. didelė rizikos veiksnių tikimybė, žala – 4 balai;

15.5. labai didelė rizikos veiksnių tikimybė, žala – 5 balai.

16. IS saugos priemonės parenkamos, įvertinus galimus rizikos veiksnius IS elektroninės informacijos vientisumui ir prieinamumui.

17. IS elektroninės informacijos saugos priemonių parinkimo pagrindiniai principai yra tokie:

17.1. saugos priemonės turi būti valdomos centralizuotai;

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

17.3. likutinė rizika turi būti sumažinta iki priimtino lygio;

17.4. kur galima, būtina įdiegti prevencines informacijos saugos priemones;

17.5. IS veiklos tęstinumo ir elektroninės informacijos sauga turi būti užtikrinama, patiriant kuo mažiau išlaidų.

18. Siekiant įvertinti IS saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per dvejus metus organizuojamas IS informacinių technologijų saugos atitikties vertinimas:

18.1. inventorizuojama IS techninė ir programinė įranga;

18.2. patikrinama (įvertinama) IS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis IS saugos dokumentams.

19. Rizikos įvertinimo ataskaitas, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas, informacinių technologijų saugos atitikties vertinimo ataskaitas, pastebėtų trūkumų šalinimo plano kopijas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo Savivaldybės administracijos saugos įgaliotinis turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemoje Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

20. Reikalavimai apsaugoti IS nuo kenksmingos programinės įrangos:

20.1. IS tarnybinėse stotyse ir kompiuterinėse darbo vietose turi būti kenksmingos programinės įrangos aptikimo priemonės, kurios reguliariai tikrina atnaujinamus ne rečiau kaip kartą per parą;

20.2. turi būti naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų.

21. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo nuostatos:

21.1. turi būti naudojama tik legali programinė įranga;

21.2. programinė įranga turi būti nuolat atnaujinama, laikantis gamintojo reikalavimų;

21.3. programinę įrangą diegti, šalinti ir konfigūruoti gali tik IS sisteminės priežiūros ir tvarkymo administratorius;

21.4. turi būti įgyvendinta prievolė ne rečiau kaip kas tris mėnesius keisti slaptažodžius;

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

22.1. IS elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų, naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami;

22.2. IS programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų.

23. Leistinos kompiuterių naudojimo ribos:

23.1. stacionarūs ir nešiojamieji IS naudotojų kompiuteriai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi IS duomenys ir IS informacija;

23.2. stacionariuose ir nešiojamuose kompiuteriuose turi būti naudojamas įjungimo slaptažodis;

23.3. IS valdytojo stacionarų kompiuterį prijungti prie IS kompiuterių tinklo gali tik IS sisteminės priežiūros ir tvarkymo administratorius;

23.4. išvežti iš patalpų nešiojamieji kompiuteriai negali būti palikti be priežiūros viešose vietose, kelionės metu nešiojamieji kompiuteriai turi būti saugomi;

23.5. visų nešiojamų kompiuterių failų sistema turi būti šifruojama algoritmais, atitinkančiais teisės aktų reikalavimus.

24. Metodai, kuriais užtikrinamas saugus IS elektroninės informacijos teikimas ir (ar) gavimas:

24.1. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų valstybės institucijų, naudojami saugūs ryšio kanalai, kuriais perduodami šifruoti duomenys;

24.2. elektroninė informacija iš susijusių registrų gaunama tik pagal duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

24.3. prieigos prie IS elektroninės informacijos teises gali suteikti tik IS sisteminės priežiūros ir tvarkymo administratorius. IS naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

24.4. pasibaigus IS naudotojo darbo sutarčiai, teisė naudotis IS elektronine informacija turi būti panaikinta. IS naudotojui prieiga prie IS turi būti ribojama ar sustabdoma, kai vyksta IS naudotojo veiklos tyrimas, naudotojas turi ilgalaikes atostogas arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos.

25. Pagrindiniai atsarginių IS elektroninės informacijos kopijų (toliau – atsarginės kopijos) darymo ir atkūrimo reikalavimai:

25.1. turi būti sudaromi IS elektroninės informacijos, kurių atsarginės kopijos daromos, sąrašai;

25.2. atsarginės kopijos turi būti laikomos atskirai nuo tarnybinių stočių. Už atsarginių kopijų darymą ir atkūrimą atsakingas IS administratorius;

25.3. atkūrimo iš atsarginių kopijų funkcija privalo būti išbandoma ne rečiau kaip kartą per metus. Testavimo eiga ir rezultatai įforminami kopijų darymo žurnale. Duomenų atkūrimo bandymą

organizuoja saugos įgaliotinis;

25.4. elektroninė informacija atsarginėse kopijose turi būti šifruota (šifravimo raktai turi būti saugomi atskirai nuo atsarginių kopijų);

25.5. atsarginės kopijos yra daromos ir saugomos taip, kad jos nebūtų prieinamos tretiesiems asmenims, kurie neturi teisės su jomis dirbti.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

26. Saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat galiojančią 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, arba elektroninių ryšių infrastruktūros įrengimo, naudojimo, apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jo paskyrimo praėję mažiau kaip vieneri metai.

27. Saugos įgaliotinis turi:

27.1. išmanyti elektroninės informacijos saugos užtikrinimo principus;

27.2. gebėti vertinti rizikos veiksnių tikimybes ir žalos galimybes, organizuoti ir kontroliuoti trūkumų šalinimą;

27.3. tobulinti kvalifikaciją elektroninės informacijos saugos srityje;

27.4. savo darbe vadovautis IS saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

28. Administratorius turi:

28.1. išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugą;

28.2. mokėti administruoti ir prižiūrėti informacines sistemas;

28.3. būti susipažinęs su IS Saugos nuostatais, IS saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

29. IS naudotojai turi:

29.1. 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;

29.2. būti susipažinę su Saugos nuostatais bei teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą;

29.3. rūpintis tvarkomos darbo vietoje informacijos saugumu.

30. IS naudotojai, saugos įgaliotinis ir administratorius turi būti pasirašę konfidencialumo pasižadėjimą saugoti asmens duomenų paslaptį.

31. IS naudotojai, pastebėję saugos politikos pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti saugos įgaliotiniui.

32. IS naudotojų ir IS administratoriaus mokymai organizuojami taip, kaip numatyta Saugos nuostatų 10.10 papunktyje, ne rečiau kaip kartą per metus.

V SKYRIUS
IS NAUDOTOJŲ SUPAŽINDINIMO SU IS SAUGOS DOKUMENTAIS PRINCIPAI

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

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

34. IS naudotojai, administratorius, saugos įgaliotinis, pažeidę IS duomenų saugos politiką įgyvendinančių dokumentų reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Širvintų rajono savivaldybės administracija
Dokumento pavadinimas (antraštė)	Dėl Širvintų rajono savivaldybės administracijos informacinės sistemos duomenų saugos nuostatų patvirtinimo
Dokumento registracijos data ir numeris	2023-06-14 Nr. 9-406
Dokumento gavimo data ir dokumento gavimo registracijos numeris	-
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Ingrida Baltušytė Administracijos direktorė
Parašo sukūrimo data ir laikas	2023-06-14 11:36
Parašo formatas	Ilgalaikio galiojimo (XAdES-XL)
Laiko žymoje nurodytas laikas	2023-06-15 00:01
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA-A
Sertifikato galiojimo laikas	2023-04-21 09:40 - 2026-04-20 09:40
Parašo paskirtis	Registravimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Diana Mičelienė Vedėja(-as)
Parašo sukūrimo data ir laikas	2023-06-14 11:44
Parašo formatas	Ilgalaikio galiojimo (XAdES-XL)
Laiko žymoje nurodytas laikas	2023-06-14 11:45
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016
Sertifikato galiojimo laikas	2019-03-23 15:15 - 2024-03-21 23:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	-
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	0
Pridedamo dokumento sudarytojas (-ai)	-
Pridedamo dokumento pavadinimas (antraštė)	Duomenų saugos nuostatai (2023-05-10 Nr. 12-2522 suderinti su NKSC).docx
Pridedamo dokumento registracijos data ir numeris	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Elpako v.20230613.4
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Tikrinant dokumentą nenustatyta jokių klaidų (2023-06-16)
Elektroninio dokumento nuorašo atspausdinimo data ir ją atspausdinęs darbuotojas	2023-06-16 nuorašą suformavo Gabrielė Morozovaitė
Paieškos nuoroda	-
Papildomi metaduomenys	-