PATVIRTINTA
Biržų Vlado Jakubėno muzikos mokyklos
direktoriaus 2024 m. sausio 23 d.
įsakymu Nr. VK-8

BIRŽŲ VLADO JAKUBĖNO MUZIKOS MOKYKLOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Biržų Vlado Jakubėno muzikos mokyklos (toliau – Mokykla) 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 Informacijos ir kibernetinio saugumo politiką.

2. Informacijos ir kibernetinio saugumo 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.

3.3. **Kibernetinis saugumas** – reiškia gebėjimą kibernetinėje erdvėje apsaugoti elektroninį ryšių tinklą, informacines valdymo sistemas bei jas apginti kibernetinių atakų atveju. Tai visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, juos aptikti, analizuoti ir reaguoti į juos bei įprastinei elektroninių ryšių tinklų, informacinių ir pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.

3.4. **Informacijos saugos įvykis** (toliau – saugos 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.

3.5. **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.

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

3.7. **Informacinės sistemos administratorius** (toliau – administratorius) – Mokyklos darbuotojas, 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 nustatytomis sąlygomis ir tvarka perduotos informacinės sistemos ir (ar) jos infrastruktūros priežiūros funkcijos.

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

3.9. **Informacinės sistemos saugos įgaliotinis** (toliau – saugos įgaliotinis) Mokyklos darbuotojas, ,koordinuojantis ir prižiūrintis saugos politikos įgyvendinimą informacinėje sistemoje.

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

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

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

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

3.14. 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 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“. Kitos saugumo 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. Informacijos ir kibernetinio saugumo principai:

6.1. Darbuotojai turi tinkamai suvokti informacijos ir kibernetinio saugumo svarbą, galimą neigiamą poveikį Mokyklos veiklai, keliamų tikslų įgyvendinimui;

6.2. Svarbiausių veiklos procesų, informacijos ir kibernetinio saugumo grėsmių rizika vertinama periodiškai, bet ne rečiau kaip kartą per metus, taip pat atsiradus poreikiui;

6.3. Užtikrinti atitiktį teisės aktuose nustatytiems informacijos ir kibernetinio saugumo reikalavimams, Mokyklos sutartiniams įsipareigojimams trečiosioms šalims, taikant rizikos vertinimu pagrįstas informacijos ir kibernetinio saugumo priemones;

6.4. Valdant informacijos saugumo ir kibernetinius incidentus, užtikrinamas reikiamas reagavimas, suvaldymas ir mokymasis iš incidentų, siekiant išvengti jų pasikartojimo ar pažeidžiamumų išnaudojimo.

7. Saugos nuostatai privalomi:

7.1. IS tvarkytojui;

7.2. IS naudotojams;

7.3. IS saugos įgaliotiniui;

7.4. IS administratoriui.

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. Mokyklos 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 naudotojo vadovui (Mokyklos direktoriui) siūlymus dėl IS sisteminės priežiūros ir tvarkymo administratoriaus paskyrimo ir reikalavimų jiems nustatymo;

10.2. teikia IS naudotojo vadovui (Mokyklos direktoriui) siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo;

10.3. atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“ ir Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo 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 naudotojui;

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 naudotojas;

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. 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 naudotojo 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 aprašas;

12.7. 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);

12.8. Lietuvos standartai LST ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai;

12.9. 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, Mokykloje 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, Mokyklos IS priskiriamas ketvirtajai informacinių sistemų kategorijai.

15. IS elektroninei informacijai, techninei, programinei įrangai, patalpoms IS naudotojo 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.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

19. IS kompiuterinėse darbo vietose turi būti kenksmingos programinės įrangos aptikimo priemonės.

20. Kenksmingos programinės įrangos aptikimo programos turi būti reguliariai atnaujinamos.

21. Programinės įrangos, įdiegtos kompiuteriuose, 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 reguliariai 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;

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 naudotojo stacionarų kompiuterį prijungti prie IS kompiuterių tinklo gali tik IS sisteminės priežiūros ir tvarkymo administratorius;

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

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

24.1. užtikrinant saugų elektroninės informacijos teikimą ir (ar) gavimą iš kitų 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. Reguliariai daromos elektroninės informacijos atsarginės kopijos.

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; mokėti administruoti ir prižiūrėti informacines sistemas;

28.2. 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 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 darbo vietoje tvarkomos 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.

V SKYRIUS
IS NAUDOTOJŲ SUPAŽINDINIMO SU IS SAUGOS DOKUMENTAIS PRINCIPAI

32. Už naudotojų supažindinimą pasirašytinai su šiais saugumo nuostatais, saugumo politiką įgyvendinančiais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą yra atsakingas IS saugos įgaliotinis.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

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

_____