SAVIVALDYBĖS ĮMONĖS „VILNIAUS ATLIEKŲ SISTEMOS ADMINISTRATORIUS“

INFORMACIJOS SAUGUMO POLITIKA

PATVIRTINTA
SĮ „Vilniaus atliekų sistemos administratorius direktorės 2022 m. sausio 13 d. įsakymu Nr. V-2022-10

TURINYS

BENDROSIOS NUOSTATOS	3
INFORMACIJOS SAUGOS ORGANIZAVIMAS	3
INFORMACIJOS SAUGOS ORGANIZACINIAI PRINCIPAI	4
ISVS TAIKYMO SRITIS IR ĮGYVENDINIMO ETAPAI	5
PRIEIGŲ VALDYMAS	5
INFORMACINIŲ IŠTEKLIŲ VALDYMAS	7
REIKALAVIMAI DARBUOTOJAMS	8
FIZINIS SAUGUMAS	9
RYŠIŲ SAUGUMAS	10
INFORMACINIŲ IŠTEKLIŲ ĮSIGIJIMAS IR PRIEŽIŪRA	11
KOMPIUTERINĖS DARBO VIETOS IR MOBILŪS ĮRENGINIAI	12
INTERNETO IR ELEKTRONINIO PAŠTO NAUDOJIMAS	13
INCIDENTŲ VALDYMAS	13
ATSARGINIS KOPIJAVIMAS	14
VEIKLOS TĘSTINUMO VALDYMAS	14
RIZIKŲ VERTINIMAS	15
PAŽEIDŽIAMUMŲ VALDYMAS	15
INFORMACIJOS SAUGUMO AUDITAS	16
ATITIKTIS TEISINIAMS IR KITIEMS INFORMACIJOS SAUGUMO REIKALAVIMAMS	16
BAIGIAMOSIOS NUOSTATOS	16

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacijos saugumo politika (toliau – Politika) nustato SĮ Vilniaus atliekų sistemos administratorius (toliau – Įmonė) informacijos saugumo organizavimo principus ir informacijos saugumo reikalavimus tinkamai Informacinių išteklių saugai nuo išorės bei vidaus grėsmių.

2. Politikoje naudojami sutrumpinimai ir apibrėžimai:

2.1. Informacija – bet kokia Įmonės ar jai pateikta informacija (žinios apie faktus, įvykius, daiktus, procesus, idėjas, sąvokas ir kitus objektus, kurios kuriame nors kontekste turi kokią nors prasmę), nepriklausomai nuo to, kokioje laikmenoje ji užfiksuota arba kokiu būdu pateikiama ar perduodama.

2.2. Informacijos sauga – Informacijos konfidencialumo, prieinamumo ir vientisumo užtikrinimas.

2.3. ISVS – Informacijos saugos valdymo sistema – rizikų valdymu pagrįsta Įmonės vadybos sistemos dalis, kuria siekiama sukurti, įgyvendinti, valdyti, stebėti, vertinti, prižiūrėti ir gerinti Informacijos saugą.

2.4. Išorinės šalys – paslaugų teikėjai, partneriai, klientai, kiti asmenys ir organizacijos, turintys ar galintys turėti prieigą prie Įmonės informacinių išteklių.

2.5. Naudotojas – Įmonės ar Išorinės šalies darbuotojas, kuriam suteikta teisė naudotis Įmonės informaciniais ištekliais.

2.6. Informacinių išteklių administratorius (Administratorius) – Įmonės darbuotojas, kuris prižiūri, konfigūruoja Įmonės informacinius išteklius.

2.7. ITT – informacinės technologijos ir telekomunikacijos.

II SKYRIUS
INFORMACIJOS SAUGOS ORGANIZAVIMAS

3. Pagrindinis Įmonės Informacijos saugos tikslas – Įmonės valdomos Informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas, bei kylančių rizikų sumažinimas iki priimtino lygio. Įmonės informacijos saugos valdymas grindžiamas rizikų vertinimu, t. y. naudojamos informacijos saugos priemonės atitinka informacijos svarbą ir jai kylančias rizikas.

4. Įmonės vadovybė Informacijos saugos valdymą laiko neatsiejama Įmonės veiklos dalimi ir įsipareigoja skirti visą reikalingą dėmesį ir išteklius užtikrinant Informacijos saugos tikslo įgyvendinimą.

5. Įmonės vadovybė atsakinga už Informacijos saugos tikslo, suderinto su Įmonės veiklos strategija ir tikslais, nustatymą ir komunikavimą.

6. Įmonės vadovybė užtikrina Informacijos saugos valdymo sistemos nuolatinį tobulinimą, periodišką peržiūrėjimą ir gerinimą. Užtikrinant informacijos saugą Įmonėje, vadovaujamasi pripažintais Lietuvos ir tarptautiniais standartais (pvz., ISO/IEC 27000) ir metodikomis.

7. Įmonė privalo identifikuoti ir dokumentuoti visus Įmonei taikomus informacijos saugos reikalavimus, įskaitant:

7.1. Lietuvos Respublikos ir Įmonės teisės aktų reikalavimus;

7.2. Veiklą prižiūrinčių įmonių reikalavimus;

7.3. Sutartinių įsipareigojimų reikalavimus.

8. Už Politikos ir ISVS įgyvendinimą atsakingas Įmonės direktorius. Informacijos saugos vertinimo, planavimo, įgyvendinimo ir kontrolės funkcijos gali būti deleguotos Informacijos saugos vadovui.

9. Informacijos sauga yra kiekvieno darbuotojo atsakomybė. Darbuotojai privalo informuoti Įmonės vadovybę ir/ar jos paskirtą atsakingą asmenį – Informacijos saugos vadovą (IT vadovą) – apie pastebėtu Informacijos saugos incidentus.

III SKYRIUS
INFORMACIJOS SAUGOS ORGANIZACINIAI PRINCIPAI

10. **Teisinis informacijos saugos organizavimo pagrįstumas**. Įmonės ISVS organizuojama vadovaujantis Įmonei nustatytais informacijos saugos reikalavimais.

11. **Tinkamos kompetencijos, įgaliojimų ir resursų suteikimas**. Politiką ir jos pagrindu sukurtą Įmonės ISVS įgyvendinantis asmuo (asmenys) turi turėti reikiamas kompetencijas ir jam (jiems) suteikiami reikalingi įgaliojimai bei resursai.

12. **Įmonės Informacinių išteklių žinojimas ir klasifikavimas**. Visi Įmonės Informaciniai ištekliai turi būti žinomi, jų valdymui ir prieigos suteikimui prie jų turi būti priskirti atsakingi valdytojai.

13. **Informacijos saugumo rizikų vertinimas**. Įmonės ISVS projektuojama ir įgyvendinama atsižvelgiant į Informacijos saugumo rizikų vertinimo Įmonės Informaciniams ištekliams rezultatus. Vertinant rizikas atsižvelgiama į Įmonės veiklos ir valdomos informacijos svarbą, galimas grėsmes ir pažeidžiamumus. Informacijos saugumo rizikų valdymas turi būti periodinis ir integruotas į esamą Įmonės rizikos valdymo procesą.

14. **Informacijos saugos valdymo priemonių proporcingumas**. Parinktos Informacijos saugos valdymo priemonės turi sumažinti nustatytą riziką, padidinti Informacijos saugumo lygį, užtikrinti veiklos tęstinumą, užtikrinti nuolatinę informacinių išteklių apsaugą bei būti orientuotos į prevenciją ir galimos žalos sumažinimą. Šių priemonių įgyvendinimo ir palaikymo kaštai negali būti didesni nei galimos pasekmės, jeigu tos priemonės nebūtų taikomos. Parinktų valdymo priemonių efektyvumas turi būti reguliariai stebimas.

15. **Gerųjų praktikų panaudojimas**. ISVS įgyvendinama taikant tarptautinius standartus ISO/IEC 27001:2013 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ bei ISO/IEC 27002:2009, ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos kodeksas/nuostatai“ tokia apimtimi, kiek jų taikymas neprieštarauja LR įstatymams ir susijusiems poįstatyminiams teisės aktams.

16. **Sąmoningumo Informacijos saugos klausimais didinimas**. Įmonės darbuotojai turi turėti pakankamas informacijos saugos žinias ir šios žinios turi būti periodiškai atnaujinamos. Kiekvienas darbuotojas privalo elgtis su informacija taip, kad nesukeltų informacijos saugumo grėsmių.

17. **Atsakomybė už informacijos saugumo pažeidimus**. Už Politikos ir ją įgyvendinančių teisės aktų pažeidimus atsakoma LR įstatymuose ir Įmonės vidiniuose teisės aktuose nustatyta tvarka.

IV SKYRIUS
ISVS TAIKYMO SRITIS IR ĮGYVENDINIMO ETAPAI

18. Įmonėje įdiegta ISVS apima informacinių technologijų, telekomunikacijų infrastruktūros paslaugų ir programinės įrangos priežiūrą ir aptarnavimą.

19. ISVS įgyvendinama vadovaujantis LST ISO/IEC 27001:2013 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ standartu ir kitais galiojančiais teisės aktais.

20. ISVS įgyvendinama šiais etapais:

21. **Planavimas**. Šio etapo metu numatoma ISVS politika, tikslai, procesai, susiję su rizikų valdymu ir informacijos saugos valdymu ir tobulinimu, siekiant rezultatų, atitinkančių veiklos tikslus;

22. **Taikymas**. Šio etapo metu vykdoma ISVS politika, taikomos valdymo priemonės ir procesai;

23. **Tikrinimas**. Šio etapo metu stebimas ir vertinamas taikomų ISVS procesų veikimas, atsižvelgiant į ISVS politiką, tikslus bei praktinę patirtį, o gauti rezultatai pateikiami Įmonės vadovybės vertinimui;

24. **Plėtra**. Šio etapo metu imamasi korekcinių bei prevencinių veiksmų, atsižvelgiant į ISVS vidinio audito rezultatus ir Įmonės vadovybės atliktą analizę ar kitą aktualią informaciją, siekiant užtikrinti nuolatinį ISVS tobulinimą.

V SKYRIUS
PRIEIGŲ VALDYMAS

25. Prieiga prie informacinių išteklių suteikiama vadovautis „būtina žinoti" principu, t.y. subjektams (darbuotojams, rangovams, kitoms šalims, informacinėms sistemoms, ir kt.) suteikiama tik minimali, būtina veiklai, prieiga.

26. Prieigos inicijavimo, sankcionavimo ir administravimo atsakomybės turi būti atskirtos, t. y. prieigos teises patvirtinti ir prieigos teises suteikti turi skirtingi asmenys.

27. Naudotojams turi būti suteikiama minimali prieiga tik prie būtinų darbo funkcijoms atlikti tinklų ir tinklo paslaugų.

28. Įmonėje turi būti nustatytos formalios naudotojų registravimo, išregistravimo ir teisių peržiūros procedūros visiems informaciniams ištekliams. Jei naudotojo pareigos Įmonėje keičiasi, ankstesnės teisės turi būti panaikinamos ir suteikiamos naujas pareigas atitinkančios teisės. Už naudotojų teisių patvirtinimą, periodinę peržiūra ir teisių panaikinimą atsakingas informacinių išteklių valdytojas.

29. Kiekvienas Naudotojas turi būti unikaliai atpažįstamas taip užtikrinant individualią atsakomybę už atliekamus veiksmus.

30. Anoniminė prieiga leidžiama tik prie viešos informacijos.

31. Administratoriaus funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms naudotojo funkcijoms atlikti.

32. Naudotojo tapatybė turi būti patvirtinama naudojant prisijungimo vardą ir slaptažodį arba kitą tapatybės patvirtinimo priemonę.

33. Kai prieiga prie informacinių išteklių yra nebereikalinga, nes Naudotojas išeina iš darbo, keičiasi jo pareigos ar dėl kitokių priežasčių, Naudotojo prieiga prie informacinių išteklių turi būti nedelsiant panaikinama.

34. Baigus darbą su kompiuteriu ar Naudotojui pasitraukiant iš kompiuterinės darbo vietos, turi būti imamasi priemonių, kad su informacija, negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinių išteklių, įjungiama ekrano užsklanda su slaptažodžiu.

35. Naudotojui neatliekant jokių veiksmų 15 min., kompiuteris turi užsirakinti, kad toliau naudotis juo būtų galima tik pakartotinai patvirtinus tapatybę.

36. Prisijungimo slaptažodžių reikalavimai:

36.1. Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių.

36.2. Slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai) ar prisijungimo vardas.

36.3. Draudžiama slaptažodžius atskleisti kitiems asmenims.

36.4. Informaciniai ištekliai, patvirtinantys Naudotojo tapatumą, turi neleisti automatiškai išsaugoti slaptažodžius.

36.5. Turi būti nustatytas didžiausias leistinas Naudotojo mėginimų įvesti teisingą slaptažodį skaičius (ne daugiau kaip 5 kartai).

36.6. Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta, Naudotojo paskyra turi užsirakinti ir neleisti Naudotojui patvirtinti tapatybės ne trumpiau kaip 30 minučių. Jei yra techninė galimybė, Administratorius apie tai turi būti automatizuotai informuojamas.

36.7. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jeigu naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

36.8. Slaptažodis turi būti keičiamas ne rečiau kaip kas 90 kalendorinių dienų.

36.9. Slaptažodį turi sudaryti ne mažiau kaip 8 simboliai.

36.10. Keičiant slaptažodį, Naudotojui neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių.

36.11. Pirmąkart jungiantis prie informacinių išteklių, turi būti reikalaujama, kad Naudotojas pakeistų slaptažodį.

36.12. Turi būti patvirtinti asmenų, kuriems suteiktos administratoriaus teisės prisijungti prie Informacinių išteklių, sąrašai, periodiškai peržiūrimi Informacijos saugos vadovo.

37. Turi būti vykdoma Administratorių paskyrų kontrolė:

37.1. Periodiškai tikrinama, ar nėra nereikalingų/nebegaliojančių Administratoriaus paskyrų.

37.2. Turi būti registruojami visi prašymai suteikti/panaikinti/pakoreguoti prieigos teises prie informacinių išteklių.

38. Draudžiama Informacinių išteklių techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į naujus.

39. Įmonėje turi būti taikoma „švaraus stalo" tvarka - draudžiama palikti be priežiūros dokumentus (pvz.: darbo kabinete ant stalo pasibaigus darbo laikui) su svarbia informacija (pvz.: informacija skirta vidiniam naudojimui, komercinės ar technologinės paslaptys, asmens

duomenys ir kt.). Svarbūs dokumentai turi būti tinkamai apsaugoti nuo nesankcionuotos prieigos (įskaitant patalpų priežiūros personalo prieigą).

40. Turi būti užtikrinama apsauga nuo nesankcionuotos loginės ir fizinės prieigos prie kompiuterinio tinklo įrenginių valdymo (diagnostikos, konfigūravimo) prievadų. Visi nebūtini veiklai tinklo įrenginių valdymo prievadai turi būti išjungti.

41. Nuotoliniam prisijungimui gali būti naudojami tik saugūs prisijungimo metodai bei tinkamos apsaugos priemonės, tokios kaip VPN.

42. Nuotolinis prisijungimas per VPN turi būti suteikiamas ribotam laikotarpiui.

43. Išorinių šalių nuotoliniai prisijungimai galimi tik apibrėžtam išorinės šalies darbuotojų skaičiui, pasirašiusiems atitinkamus konfidencialumo įsipareigojimus.

44. Įmonės duomenų tinklas turi būti segmentuojamas į skirtingų saugumo lygių zonas. Ugniasienėmis turi būti atskirtos: sistemų prieinamų iš išorės grupės; vidinių sistemų grupės; naudotojų grupės. Duomenų srautai tarp skirtingų saugumo zonų turi būti kontroliuojami ir leidžiami tik minimalūs, būtini veiklai.

45. Darbo vietų, tarnybinių stočių bei kitos įrangos operacinės sistemos turi būti apsaugotos nuo nesankcionuotos prieigos. Operacinės sistemos starto metu turi būti apsaugotos nuo alternatyvių OS paleidimo metodų (pvz.: startas iš USB, CD/DVD laikmenų). Prieiga prie BIOS nustatymų turi būti apsaugota saugiu slaptažodžiu.

46. Naudojamose operacinėse sistemose turi būti įgyvendinti slaptažodžių sudėtingumo ir keitimo reikalavimai. Slaptažodžių saugojimui naudojami tik patikimi ir saugūs šifravimo bei maišos algoritmai.

47. Operacinių sistemų naudotojams turi būti panaikinti visi, nebūtini veiklai, OS komponentai (servisai, taikomosios programos, sisteminės priemonės).

VI SKYRIUS
INFORMACINIŲ IŠTEKLIŲ VALDYMAS

48. Įmonėje leidžiama naudoti tik gamintojų palaikomą aparatinę įrangą. Turi būti naudojama aparatinės įrangos gamintojo išleista naujausia programinė-aparatinės įrangos versija, turinti visas saugumo pataisas.

49. Įmonės aparatinėje įrangoje turi būti naudojama kompetentingų specialistų paruošta ir įdiegta operacinė sistema.

50. Įmonės aparatinėje įrangoje turi būti naudojama sankcionuota, leistinuose sąrašuose esanti, programinė įranga. Turi būti įdiegtos programinės įrangos gamintojo išleistos kritinius ir svarbius programinės įrangos saugumo pažeidžiamumus taisančios pataisos.

51. Visi Įmonės informaciniai ištekliai turi būti apskaitomi ir priskirti konkretiems asmenims – informacinių išteklių savininkams.

52. Informaciniuose ištekliuose turi būti įdiegta antivirusinė programinė įranga, kuri turi reguliariai atsinaujinti. Jei nėra galimybės informaciniuose ištekliuose įdiegti antivirusinės programos, informaciniai ištekliai turi būti atjungti nuo interneto, informacija ir duomenys perkeliami į šiuos informacinius išteklius prieš tai turi būti patikrinami ar juose nėra kenksmingo kodo.

53. Įmonės informacija turi būti klasifikuojama pagal informacijos svarbą ir poreikį jos saugai.

54. Visi Įmonės darbuotojai turi būti pasirašytinai susipažinę ar elektroninių priemonių pagalba patvirtinę susipažinimą su konfidencialios informacijos apibrėžimu, reikalavimais konfidencialios informacijos saugojimui ir savo atsakomybe.

55. Internetu pasiekiamų informaciniai ištekliai turi tenkinti šiuos reikalavimus:

55.1. Perduodami duomenys turi būti šifruojami.

55.2. Šifravimui naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų.

55.3. Perduodamų duomenų šifravimu turi būti naudojamas TLS (angl. Transport Layer Security) standartas.

55.4. Turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. SQL injection), įterptinių instrukcijų atakų (angl. Cross-site scripting), atkirtimo nuo paslaugos (angl. DOS), paskirstyto atsisakymo aptarnauti (angl. DDOS) ir kitų, priemonės; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. The Open Web Application Security Project (OWASP)) interneto svetainėje www.owasp.org.

55.5. Turi būti naudojama informacinių išteklių naudotojo įvedamų duomenų tikslumo kontrolė (angl. Validation).

55.6. Tarnybinė stotis, kurioje yra informacinių išteklių, neturi rodyti naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį.

55.7. Informacinių išteklių saugumo priemonės turi gebėti automatiškai uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir panašiai).

55.8. Tarnybinė stotis, kurioje yra informaciniai ištekliai, turi leisti tik informacinių išteklių funkcionalumui užtikrinti reikalingus HTTP metodus.

55.9. Turi būti uždrausta naršyti informacinių išteklių aplankuose (angl. Directory browsing).

56. Įmonės informacinėse sistemose turi būti registruojama ir ne mažiau kaip 12 mėnesių saugoma su informacine sistema atliktų veiksmų informacija:

56.1. prisijungusio naudotojo ar administratoriaus identifikatoriai;

56.2. esminių įvykių laikai;

56.3. kompiuterio, iš kurio jungiamasi, informacija;

56.4. sėkmingos ir nesėkmingos prieigos įrašai;

56.5. administracinių teisių naudojimas;

56.6. sistemos konfigūracijos keitimas, sisteminių priemonių naudojimas;

56.7. resursai, prie kurių buvo suteikta prieiga;

56.8. sisteminiai pranešimai.

57. Veiksmų žurnaliniai įrašai turi būti apsaugoti nuo neautorizuoto modifikavimo ir ištrynimo.

58. Visų Įmonės informacinių sistemų laikrodžiai turi būti sinchronizuoti pagal sutartą tikslų laiko šaltinį. Naudotojams keisti sistemos laiką turi būti draudžiama.

VII SKYRIUS
REIKALAVIMAI DARBUOTOJAMS

59. Įmonėje turi būti nustatyti ir į atitinkamus vidaus dokumentus (darbo sutartis, darbo tvarkos taisykles, pareiginius nuostatus, konfidencialumo susitarimus ir kt.) įtraukti darbuotojams (rangovams, paslaugų teikėjams, bei kitiems išorinių šalių atstovams) keliami saugos reikalavimai, prievolės ir atsakomybės. Reikalavimuose turi būti numatytos prievolės:

59.1. laikytis Įmonės informacijos saugos politikos ir ją įgyvendinančių Įmonės tvarkų reikalavimų;

59.2. saugoti Įmonės informacinius išteklius nuo nesankcionuotos prieigos, atskleidimo, modifikavimo ar sunaikinimo;

59.3. informuoti atsakingus asmenis apie saugumo incidentus ar įvykius.

60. Prieš įdarbinant naują darbuotoją Įmonėje turi būti įsitikinta kandidato pateiktos informacijos autentiškumu (pvz.: pateikiami kvalifikaciją patvirtinančių dokumentų originalai, įsitikinama rekomendacinių laiškų autentiškumu), bei patikrinama kita, kandidato pateikta, reikšminga informacija.

61. Prieiga prie Įmonės informacinių išteklių naujam darbuotojui suteikiama tik darbuotojui pasirašytinai susipažinus su Politika, ją įgyvendinančiomis Įmonės tvarkomis ir kitais informacijos saugos reikalavimais bei darbuotojo atsakomybe.

62. Darbuotojų informacijos saugos mokymai rengiami ne rečiau kaip kartą per metus.

63. Nutraukus darbo santykius su darbuotoju ar keičiantis darbuotojo pareigoms prieiga prie informacinių sistemų/išteklių turi būti nedelsiant panaikinama. Įmonėje turi būti įgyvendinta tvarka, kuria užtikrinama, kad darbuotojai grąžina visus suteiktus fizinius informacinius išteklius iki nutraukiant darbo sutartį.

VIII SKYRIUS
FIZINIS SAUGUMAS

64. Visos patalpos, kuriose yra svarbi informacinių išteklių įranga (pvz., tarnybinių stočių patalpos, duomenų centrai, ryšių mazgai) ar duomenys (pvz., dokumentų archyvai), (toliau - padidinto saugumo zonos) turi būti identifikuotos ir nurodytos fizinės saugos plane.

65. Įmonės objektų perimetras turi būti aiškiai apibrėžtas ir įgyvendintos tinkamos perimetro saugumo priemonės, kurios užtikrintų efektyvią apsaugą nuo patekimo į objektą iš išorės. Įmonės patalpų perimetrui apsaugoti turi būti naudojama išorinio perimetro elektroninė apsauga, vaizdo stebėjimo sistema, leidimų režimas, elektroninė įeigos kontrolės sistema. Patekimas į tarnybines patalpas/pastatus leidžiamas tik sankcionuotam personalui. Pašaliniai asmenys, esantys tarnybinėse patalpose (lankytojai, rangovai ir kt.), turi būti lydimi Įmonės darbuotojo.

66. Padidinto saugumo zonose turi būti numatytos prieigos kontrolės priemonės, kurios ribotų patekimą tik sankcionuotam personalui:

66.1. visi patekimai į padidinto saugumo zonas turi būti dokumentuojami, nurodant įėjimo/išėjimo laikus, asmenis. Lankytojai patalpose gali būti tik prižiūrimi atsakingo asmens. Prieš patenkant visi asmenys turi būti supažindinti su saugumo reikalavimais taikomais šiai zonai.

66.2. padidinto saugumo zonų prieigos teisės turi būti nuolat peržiūrimos ir, esant reikalui, atnaujinamos.

67. Kabinetai ir kitos patalpos turi būti žymimos taip, kad iš pavadinimo nebūtų galima suprasti apie patalpose esančias informacijos apdorojimo priemones.

68. Padidinto saugumo zonų apsauga nuo aplinkos veiksnių:

68.1. draudžiama saugoti degias ar lengvai užsiliepsnojančias medžiagas,
68.2. draudžiama gerti, valgyti ar rūkyti,
68.3. turi būti atliekamas nuolatinis aplinkos parametrų stebėjimas,
68.4. atsarginė įranga ir atsarginės kopijos turi būti saugomos saugiu atstumu nuo pagrindinės įrangos ir duomenų.

69. Viešos prieigos zonos, pvz., krovinių pristatymo ar išsiuntimo zonos, klientų aptarnavimo zonos, į kurias gali patekti ne Įmonės darbuotojai, turi būti tinkamai apsaugotos ir, pagal galimybes, izoliuotos nuo informacijos apdorojimo priemonių.

70. ITT įranga turi būti apsaugota nuo palaikymo sistemų (elektros energijos ir vandens tiekimas, nuotekos, šildymas, vėdinimas ir oro kondicionavimas) sutrikimų.

71. Visos palaikymo sistemos turi būti adekvačios palaikomoms ITT sistemoms, t. y. palaikymo sistemų pajėgumas ir konfigūracija turi atitikti ITT sistemų funkcionavimui keliamus reikalavimus. Palaikymo sistemos turi būti periodiškai tikrinamos.

72. Nepertraukiamo maitinimo šaltiniai turi užtikrinti korektišką sistemų išsijungimą ar veikimą nutrūkus elektros energijos tiekimui.

73. Elektros ir telekomunikacijų kabeliai turi būti apsaugoti nuo sugadinimo ar nesankcionuoto prisijungimo. Turi būti naudojamas aiškus ir dokumentuotas kabelių žymėjimas. Kabeliai turi būti klojami minimizuojant nesankcionuotos fizinės prieigos galimybę.

74. Įranga turi būti prižiūrima vadovaujantis įrangos gamintojo nurodytomis instrukcijomis ir nurodytu periodiškumu. Priežiūrą gali atlikti tik sankcionuotas personalas. Turi būti vedami gedimų registravimo žurnalai.

75. Duomenys kompiuterinėse laikmenose turi būti sunaikinti neatkuriamai prieš utilizuojant, remontuojant ar pakartotinai naudojant kompiuterinę įrangą vadovaujantis duomenų naikinimo ir šalinimo tvarka.

IX SKYRIUS
RYŠIŲ SAUGUMAS

76. Įmonėje turi būti įgyvendintos tinkamos kompiuterių tinklo kontrolės priemonės:
76.1. Įmonės darbuotojų kompiuterinis tinklas turi būti atskirtas nuo serverių tinklo;
76.2. Prieiga prie Įmonės valdomo kompiuterinio tinklo ir tinklo įrangos privalo būti identifikuota ir patvirtinta (vykdoma griežta įrenginių kontrolė);
76.3. Neatpažintų įrenginių darbas tinkle turi būti blokuojamas pagal nutylėjimą iki tokie įrenginiai pažymimi sistemoje kaip patvirtinti.
76.4. Informacija apie neatpažintus įrenginius turi būti automatiškai išsiunčiama atsakingam darbuotojui.
76.5. Turi būti vykdomas tinklo įrangos konfigūracijų rezervinis kopijavimas po kiekvieno pakeitimo tinklo konfigūracijoje, bet ne vėliau kaip per 1 savaitę nuo pakeitimų atlikimo.
76.6. Tinklo įrenginių administravimas gali būti vykdomas naudojant tik saugius protokolus, pavyzdžiui HTTPS, SSH.
76.7. Ugniasienės privalo žurnalizuoti tinklo srautus (šaltinio adresas, paskirties adresas, protokolas/prievadas, laikas ir trukmė).
76.8. Ugniasienės privalo blokuoti visą tinklo srautą (angl. „deny by default“) ir praleisti tik taisyklių pagalba įtrauktas išimtis.

76.9. Turi būti išjungti nenaudojami TCP (angl. Transmission Control Protocol) / UDP (angl. User Datagram Protocol) prievadai.
76.10. Turi būti registruojami duomenys apie visus įrenginius turinčius IP adresus: kompiuteriai, telefonai, serveriai, tinklo įrenginiai, IP telefonai, kita periferija.
76.11. Bevielis ryšys turi būti saugiai šifruojamas.
76.12. Turi būti sudaryta ir patvirtinta vieninga saugi bevielio ryšio komunikacijų įrangos (Wi-Fi) konfigūracija.
76.13. Įmonės vidaus bevielio tinklo apsaugai turi būti taikomas WPA2 (angl. „Wi-Fi Protected Access 2“) arba saugesnis protokolas bei naudojamas šifravimas mažiausiai 128 bitų ilgio raktu.
76.14. Prieiga prie Įmonės bevielio tinklo turi būti leidžiama tik autorizuotiems naudotojams.
76.15. Turi būti atliekamas nuolatinis tinklo parametrų ir saugumo įvykių stebėjimas.
76.16. Visi svarbūs duomenys perduodami tinklais turi būti saugiai šifruojami.
77. Taikomos saugos priemonės susijusios su interneto ryšio naudojimu:
77.1. Prieiga iš interneto turi būti saugoma ugniasienės pagalba;
77.2. Įmonė gali, be išankstinio perspėjimo, blokuoti interneto resursus, jei šie resursai yra/buvo nesaugūs ar jie neatitinka keliamų saugumo reikalavimų bei sukelia grėsmes Įmonės tinklams (pvz. DDoS atakos, spam žinutės ir kt.).
77.3. Įmonė gali blokuoti interneto resursus, kurie tiesiogiai ar netiesiogiai sukuria didelę papildomą tinklo/sistemų apkrovą ar gali kitaip įtakoti Įmonės veiklą.
77.4. Įmonė gali riboti prieigą prie kitų el. pašto sistemų/portalų, kurie nesiejami su darbuotojo atliekamomis darbo funkcijomis.
78. Papildomi reikalavimai bevielės prieigos taškams:
78.1. Kas savaitę privalo būti vykdoma reguliari belaidės prieigos taškų patikra.
78.2. ne rečiau kaip kartą per dieną saugasienių administratorių turi būti atliekama saugasienių užfiksuotų įvykių analizė. Saugasienių užfiksuotų įvykių ataskaita reguliariai turi būti pateikiama ir Informacijos saugumo vadovui.
78.3. turi būti uždraustas SNMP (angl. „Simple Network Managment Protocol“) protokolo naudojimas belaidėje sąsajoje, išskyrus protokolo saugios versijos naudojimą stebėsenos tikslais;
78.4. turi būti uždrausti visi nebūtini bevielių įrenginių valdymo protokolai.

X SKYRIUS
INFORMACINIŲ IŠTEKLIŲ ĮSIGIJIMAS IR PRIEŽIŪRA

79. Prieš įsigyjant, kuriant naujus ar plečiant esamus informacinius išteklius (operacines sistemas, ITT infrastruktūros elementus, taikomąją programinę įrangą, ITT paslaugas), turi būti nustatyti ir dokumentuoti informacijos saugos reikalavimai. Saugumo rizikų įvertinimas turi būti atliekamas sistemų inicijavimo stadijoje.

80. Įsigyjami ar kuriami informaciniai ištekliai privalo užtikrinti apdorojamų duomenų tikslumą.

81. Informacinių sistemų kūrimo, testavimo ir darbinės (eksploatacinės) aplinkos turi būti atskirtos. Programinės įrangos ir duomenų perkėlimo iš vienos aplinkos į kitą procesas turi būti nustatytas ir dokumentuotas.

82. Taikomosios programinės įrangos testavimą ir diegimą atlieka specialistai laikydamiesi dokumentuotų procedūrų. Informacinių išteklių funkcionalumo testavimui turi būti naudojama testavimo aplinka, kuri turi būti saugoma laikantis tų pačių reikalavimų kaip ir darbinė aplinka.

83. Prieiga prie informacinių išteklių išeitinių tekstų turi būti apribota tik sankcionuotiems asmenims, kuriems ji būtina pagal darbo pobūdį.

84. Informacinių išteklių pakeitimai turi būti atliekami laikantis dokumentuotos keitimų valdymo procedūros. Turi būti užtikrinta, kad prieš atliekant pakeitimus sistemoje įvertinamas galimas poveikis sistemoms. Keitimo inicijavimo ir įgyvendinimo atsakomybės turi būti atskirtos, keitimai turi būti dokumentuojami.

85. Nauji informaciniai ištekliai turi būti integruoti su esamomis saugos sistemomis (pvz. žurnalinių įrašų centralizuoto surinkimo sistema, pažeidžiamumų valdymo sistema, atnaujinimų valdymas ir pan.).

XI SKYRIUS
KOMPIUTERINĖS DARBO VIETOS IR MOBILŪS ĮRENGINIAI

86. Įmonės kompiuterinėje įrangoje turi būti įdiegta legali, gamintojo palaikoma ir Įmonės leidžiama operacinė sistema bei programinė įranga.

87. Kompiuterinių darbo vietų naudotojai negali turėti kompiuterio administravimo teisių.

88. Standartinės, gamintojo sukurtos, vartotojų paskyros privalo būti ištrintos arba išjungtos, įskaitant Guest/Anonymous paskyras.

89. Nenaudojami procesai arba nenaudojami operacinės sistemos programiniai paketai privalo būti išjungti arba ištrinti.

90. Kompiuterinėse darbo vietose turi būti diegiamos gamintojo išleistos operacinės sistemos ar programinės įrangos pataisos.

91. Ne rečiau kaip kartą per mėnesį kompiuterinės darbo vietos turi būti atnaujinamos.

92. Windows operacinėje sistemoje standartinis kompiuterio diskų dalinimasis (angl. „Administrative Share“ arba „C$“) turi būti išjungtas.

93. Administravimo tikslais jungtis nuotoliniu būdu prie Įmonės darbuotojų kompiuterių leidžiama tik, jei:

93.1. yra gautas kompiuterio naudotojo sutikimas;

93.2. yra registruotas atitinkamas kreipinys;

93.3. yra centralizuotai kaupiami žurnaliniai įrašai apie tokius prisijungimus.

94. Visų Įmonės nešiojamų kompiuterių kietajame diske esantys duomenys privalo būti šifruojami.

95. Įmonėje turi būti išjungtas failų automatinio paleidimo (angl. „auto-run“) funkcionalumas į kompiuterius įjungus USB/CD/DVD/Flash/FireWire įrenginius.

96. USB/išorinių HDD/CD/DVD/Flash atmintinių naudojimas yra draudžiamas. Išimtis nustato Įmonės vadovas arba jo įgaliotas asmuo.

97. Kompiuterinės darbo vietos privalo būti sukonfigūruotos taip, kad darbuotojas negalėtų išjungti ar pakeisti sisteminės ar saugos priemonių programinės įrangos, tokios kaip antivirusinė programinė įranga, nustatymų.

98. Kompiuterinėse darbo vietose turi būti įdiegta antivirusinė programa, kuri:

98.1. pasileistų ir būti aktyvi sistemos paleidimo ir darbo metu;

98.2. turėtų aktyvuotą realaus laiko grėsmių stebėjimą bei blokuotų galimus kenkėjiškus veiksmus;
98.3. tikrintų ar yra atnaujinimų ne rečiau kaip kas 8val. ir sudiegtų esamus atnaujinimus nedelsiant;
98.4. automatiškai skanuotų visą sistemą ne rečiau kaip kas 7 dienas;
98.5. būtų administruojama centralizuotai;
98.6. palaikytų priverstinius atnaujinimus iš centralizuoto valdymo serverio;
98.7. automatiškai skanuotų bylas prieš jas atidarant ar paleidžiant;

99. Draudžiama dirbti su konfidencialia įmonės informacija viešosiose vietose.

100. Dirbant su konfidencialia informacija ne viešose vietose per telekomunikacinių įmonių tinklus ji privalo būti perduodama saugiu šifruotu kanalu (pvz., VPN) arba užšifruojant perduodamą informaciją.

101. Nešiojami įrenginiai, kuriuose yra slapta ir/arba konfidenciali Įmonės informacija, negali būti paliekami be priežiūros, jei patalpos kuriose paliekama įranga nėra fiziškai apsaugotos nuo pašalinių asmenų prieigos.

102. Draudžiama dalintis įmonės nešiojamais kompiuteriais ir mobiliais įrenginiai su kitais asmenimis (kolegomis, svečiais, draugais ar šeimos nariais) ir, pvz., mobilaus telefono baterijos pakrovimo tikslu, jungti prie svetimo kompiuterio.

103. Kelionėse (pvz., lėktuve, traukinyje, autobuse ir pan.) saugoti nešiojamus kompiuterius ir mobilius įrenginius, neatiduoti transportavimui į bagažą.

104. Visuose mobiliuose įrenginiuose privalo būti įdiegta slaptažodžiu ar PIN kodu apsaugota prieiga. Slaptažodžiai privalo būti periodiškai keičiami.

105. Nešiojamo kompiuterio ar mobilaus įrenginio netekimo atveju (pametus, pavogus ir pan.) darbuotojas nedelsiant privalo informuoti savo tiesioginį vadovą.

XII SKYRIUS
INTERNETO IR ELEKTRONINIO PAŠTO NAUDOJIMAS

106. Draudžiama naudotis internetu ir elektroniniu paštu sukčiavimo, reklamos ir asmeninės finansinės naudos tikslais, dalyvauti interneto lažybose ir azartiniuose lošimuose, lankytis pornografiniuose tinklalapiuose.

107. Draudžiama Įmonės sukurtos paskyros duomenis naudoti trečiųjų šalių interneto svetainėse.

108. Elektroninis paštas yra ryšio priemonė, skirta tiesioginėms funkcijoms atlikti ir naudotojai turi naudoti šią priemonę atsakingai, veiksmingai ir teisėtais tikslais.

109. Draudžiama elektroniniu paštu siusti Įmonės konfidencialią informaciją, jei dėl tokios informacijos siuntimo nebuvo gautas tiesioginio vadovo leidimas.

110. Draudžiama elektroniniu paštu siųsti Naudotojo tapatybės patikrinimui naudojamą informaciją (pavyzdžiui, slaptažodį).

111. Neatidarinėti laiškų, jeigu siuntėjas nėra aiškus, prie jų pridėtas failas ar neaiškus laiško turinys.

112. Draudžiama spausti ant elektroniniame laiške esančių nuorodų, jei laiško siuntėjas yra nežinomas.

XIII SKYRIUS
INCIDENTŲ VALDYMAS

113.Apie visus incidentus, aptiktas saugumo spragas, silpnas saugumo vietas nedelsiant turi būti pranešama pagalbos tarnybai. Visi Įmonės darbuotojai, rangovai ir kiti susiję asmenys turi būti informuoti apie savo pareigą pranešti apie saugumo incidentus, aiškiai nurodant kokiomis priemonėmis ir kas yra informuojamas apie incidentus.

114.Saugumo incidentai ir įvykiai turi būti sistemingai ir nuosekliai valdomi, užtikrinant reikiamą reagavimą ir incidentų poveikio mažinimą.

115.Saugumo incidentai valdomi pagal nustatytą incidentų valdymo tvarką.

XIV SKYRIUS
ATSARGINIS KOPIJAVIMAS

116.Siekiant užtikrinti informacinių išteklių atstatymą įvykus sutrikimui, turi būti atliekamas visų svarbių informacinių išteklių atsarginis kopijavimas.

117.Informacinių išteklių konfigūracijos nustatymų atsarginės kopijos turi būti daromos ne rečiau kaip kartą per dieną.

118.Informacijos ir duomenų kopijos turi būti daromos ne rečiau kaip kartą per savaitę.

119.Atsarginės kopijos saugomos atskiroje patalpoje. Jei daromos kopijos į skaitmenines laikmenas, jos turi būti laikomos nedegiame, rakinamame seife, esančiame atskiroje patalpoje.

120.Atsarginė kopija saugoma 3 (tris) mėnesius. Pasibaigus saugojimo laikui, seniausia kopija ištrinama, vietoj jos įrašoma naujausia kopija.

121.Registruojami visi atvejai, kai vykdomas duomenų atkūrimas iš atsarginių kopijų.

122.Informacinių išteklių atsarginis kopijavimas ir atstatymas vykdomas vadovaujantis Įmonės atsarginio kopijavimo ir atkūrimo iš atsarginių kopijų tvarka.

XV SKYRIUS
VEIKLOS TĘSTINUMO VALDYMAS

123.Įmonės veiklos tęstinumas valdomas vadovaujantis Įmonės vadovo patvirtintu veiklos tęstinumo valdymo planu. Veiklos tęstinumo planas rengiamas remiantis poveikio veiklai analize. Plane pateikiama ši informacija:

123.1. Bendroji dalis – veiklos tęstinumo tikslai, plano apimtis, įgyvendinimo resursai ir atsakomybės;

123.2. Poveikio veiklai analizė – kritinės Įmonės funkcijos ir jų praradimo poveikis, kritinių funkcijų valdytojai, kritines funkcijas užtikrinantys resursai (įskaitant informacinius resursus), reikalavimai funkcijų atkūrimo laikui, apimtims ir resursams, kritinėms funkcijoms ir resursams kylančios rizikos ir grėsmių scenarijai;

123.3. Veiklos tęstinumo strategijos – reagavimo, krizinių ir nenumatytų situacijų valdymo/komunikavimo struktūros, kritinių funkcijų tęstinumo ir atkūrimo procedūros ir resursai;

123.4. Tęstinumo plano palaikymas – plano išbandymo, komunikavimo ir atnaujinimo nuostatos, personalo mokymai.

124.Įmonės informacinių sistemų veiklos tęstinumas valdomas vadovaujantis IT vadovo patvirtintu informacinių sistemų veiklos tęstinumo valdymo planu. Plane pateikiama ši informacija:

124.1. Bendroji dalis – informacinių sistemų aprašymas, plano tikslai ir apimtis, personalo vaidmenys ir atsakomybės;

124.2. Plano aktyvavimas ir informavimas - aktyvavimo kriterijai ir atsakomybės, informavimo / komunikacijos priemonės ir procedūros, poveikio masto įvertinimo procedūros;

124.3. Atkūrimas - atkūrimo strategijos, informacinių sistemų komponentų atkūrimo eiliškumas, detalios atkūrimo procedūros, susijusių šalių informavimo procedūros, atkūrimo patvirtinimo procedūros, plano atšaukimo procedūros;

124.4. Plano išbandymo reikalavimai;

124.5. Priedai - visa sėkmingam atkūrimui būtina informacija (kontaktinė personalo informacija ir paslaugų teikėjų informacija, programinės ir aparatinės įrangos sąrašai ir kt.).

XVI SKYRIUS
RIZIKŲ VERTINIMAS

125.Rizikos, kylančios Įmonės valdomiems informaciniams ištekliams vertinamos periodiškai, bet ne rečiau kaip kartą per metus, arba reikšmingai pasikeitus Įmonės veiklos pobūdžiui, informacinių išteklių valdymo priemonėms.

126.Rizikų vertinimas atliekamas vertinant rizikos veiksnius, galinčius turėti įtakos informacinių išteklių saugumui, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus.

127.Svarbiausi rizikos veiksniai:

127.1. subjektyvūs netyčiniai (informacinių išteklių tvarkymo klaidos ir apsirikimai, informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai ITT sutrikimai, informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

127.2. subjektyvūs tyčiniai (nesankcionuotas informacinių sistemų naudojimas informacijai gauti, informacijos pakeitimas ar sunaikinimas, duomenų perdavimo tinklais sutrikdymas, saugos pažeidimai, vagystės ir kita);

128.Rizikų vertinimo rezultatai išdėstomi rizikų vertinimo ataskaitoje, kuri teikiama Įmonės vadovui.

129.Atsižvelgdamas į rizikų vertinimo ataskaitą, Įmonės vadovas prireikus tvirtina rizikų valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikų valdymo priemonėms įgyvendinti.

130.Informacinių išteklių saugumo būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis saugos priemonėmis, kurios pasirenkamos atsižvelgiant į Įmonės turimus išteklius, vadovaujantis šiais principais:

130.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

130.2. informacinių išteklių saugumo priemonių diegimo kaina turi būti proporcinga saugomų informacinių išteklių vertei;

130.3. atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegtos prevencinės, aptikimo ir korekcinės saugos priemonės.

XVII SKYRIUS
PAŽEIDŽIAMUMŲ VALDYMAS

131.Siekiant sumažinti saugos incidentų tikimybę, Įmonėje vykdomas informacinių sistemų techninių pažeidžiamumų identifikavimas ir šalinimas.

132.Kritinėms informacinėms sistemoms ir jų komponentams, kurie pasiekiami iš vidinio tinklo, vykdomas reguliarus, ne rečiau kaip kartą per metus, automatizuotas vidinis pažeidžiamumų skenavimas.

133.Kritinėms informacinėms sistemoms ir jų komponentams, kurie pasiekiami iš interneto, vykdomas reguliarus, ne rečiau kaip kartą per pusmetį, išorinis pažeidžiamumų skenavimas.

134.Visi aktyviniai tinklo įrenginiai turintys IP adresus tikrinami nuo pažeidžiamumų.

135.Kritiniai pažeidžiamumai privalo būti pašalinti ne ilgiau kaip per 14 dienų nuo pažeidžiamumo identifikavimo dienos.

136.Svarbūs pažeidžiamumai privalo būti pašalinti ne ilgiau kaip per 30 dienų nuo pažeidžiamumo identifikavimo dienos.

137.Kiti pažeidžiamumai privalo būti pašalinti ne ilgiau kaip per 60 dienų nuo pažeidžiamumo identifikavimo dienos.

XVIII SKYRIUS
INFORMACIJOS SAUGUMO AUDITAS

138.Vidinis informacijos saugumo auditas turi būti atliekamas ne rečiau kaip kartą per metus.

139.Nepriklausomas Įmonės informacijos saugumo auditas turi būti atliekamas periodiškai, ne rečiau kaip kartą per 2 metus, arba reikšmingai pasikeitus Įmonės veiklos pobūdžiui, informacinių išteklių valdymo priemonėms.

XIX SKYRIUS
ATITIKTIS TEISINIAMS IR KITIEMS INFORMACIJOS SAUGUMO REIKALAVIMAMS

140.Įmonė turi imtis tinkamų priemonių užtikrinant naudojamos programinės įrangos teisėtumą (legalumą) ir apsaugant intelektinės autorių nuosavybės teises. Įmonėje turi būti parengti naudojamos programinės įrangos ir šios įrangos licencijų registrai.

141.Įmonės veiklos dokumentai (įskaitant elektroninius dokumentus) turi būti tinkamai valdomi ir apsaugoti nuo sugadinimo, praradimo, neteisėto naudojimo, pakeitimo ir naikinimo, laikantis Lietuvos Respublikos teisės aktų ir Įmonės veiklos reikalavimų.

142.Įmonėje turi būti parengta dokumentų valdymo tvarka, kurioje nurodomi pagrindiniai dokumentų (įskaitant elektroninius dokumentus) rengimo, tvarkymo, apskaitos, saugojimo ir naikinimo reikalavimai.

143.Įmonė privalo užtikrinti tinkamas darbuotojų ir klientų asmens duomenų apsaugos priemones nuo atsitiktinio ar neteisėto duomenų sunaikinimo, pakeitimo, atskleidimo ar neteisėto tvarkymo, laikantis Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, Lietuvos Respublikos elektroninių ryšių įstatymo ir kitų LR teisės aktų reikalavimų.

144.Įmonės visų lygių vadovai užtikrindami saugumo politikos ir kitų saugumo reikalavimų įgyvendinimą savo atsakomybės ribose privalo periodiškai vertinti šių reikalavimų vykdymą ir šalinti neatitikimus.

XX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

145.Už Politikos atnaujinimą ir peržiūrą, ne rečiau kaip vieną kartą per metus, yra atsakingas Įmonės vadovas. Neeilinė peržiūra atliekama, įvykus pokyčiams, galintiems turėti įtakos informacijos saugumui ir jo valdymui.

146.Politika yra sudėtinė Įmonės teisės aktų, reglamentuojančių Informacijos saugos reikalavimus Įmonėje, dalis.

147.Įmonė rengia Politikos įgyvendinimo tvarkų aprašus, taisykles, procesus ar kitus su Informacijos sauga susijusius Įmonės teisės aktus, vadovaujantis šios Politikos nuostatomis ir laikantis teisės aktų.

148.Politika taikoma visiems Įmonės darbuotojams.

149.Visi Įmonės darbuotojai turi būti pasirašytinai susipažinę ar elektroninių priemonių pagalba patvirtinę susipažinimą su Politika.