

PATVIRTINTA
Mažikių politechnikos mokyklos
direktoriaus 2018 m. birželio 29 d.
įsakymu Nr. VI-86

MAŽEIKIŲ POLITECHNIKOS MOKYKLOS INFORMACIJOS APDOROJIMO PRIEMONIŲ NAUDOJIMO TVARKOS APRAŠAS

I SKYRIUS

BENDROSIOS NUOSTATOS

1. Mažeikių politechnikos mokyklos (toliau – Mokykla) informacijos apdorojimo priemonių naudojimo tvarkos aprašas (toliau – Aprašas) nustato Mažeikių politechnikos mokyklos kompiuterių ir programinės įrangos diegimą, eksploatavimą, apskaitą ir apibrėžia teisėto, saugaus ir etiško Mažeikių politechnikos mokyklos kompiuterių, kompiuterių tinklo ir interneto išteklių naudojimo principus visiems asmenims, dirbantiems Mažeikių politechnikos mokykloje.

2. Mažeikių politechnikos mokyklos darbuotojai, dirbantys pagal darbo sutartis privalo būti supažindinti su šiuo Aprašu ir jo laikytis.

II. SKYRIUS

PAGRINDINĖS SĄVOKOS

3. **Administratorius** – Darbuotojas, kuriam suteikta teisė tvarkyti Mažeikių politechnikos mokyklos kompiuterinę įrangą, diegti pagrindinę įrangą, prižiūrėti kompiuterių tinklą ir kompiuterines sistemas. Tokia teisė suteikiama mokyklos direktoriaus įsakymu.

4. **Duomenų šifravimas** – duomenų formos pakeitimas iš paprastos į specifinę, iš kurios duomenis galima pakeisti į pradinę formą tik žinant duomenų pakeitimo algoritimą.

5. **Kompiuterinė įranga** – tai sisteminis blokas ar nešiojamas kompiuteris ir jo dalys, išoriniai įrenginiai (monitoriai, skaitytuvai, spausdintuvai bei kopijavimo aparatai, klaviatūros, pelės, kolonėlės, ausinės, video bei fotokameros, multimedijos projektoriai ir pan.), kompiuterių tinklo įranga, kompiuterių bei tinklo įrangos montavimo spintos, nuolatinio elektros maitinimo šaltiniai ir pan.

6. **Kompiuterio naudotojas** – Darbuotojas, dirbantis kompiuterine ir/ar programine įranga.

7. **Kompiuterių tinklas** – tai serveriai ir darbo vietų kompiuteriai, kompiuterių tinklo įranga (kabeliai, tinklo aparatūra) sujungti į vieningą sistemą, siekiant užtikrinti kompiuterių

naudotojams operatyvų keitimąsi informacija, kolektyvinį kompiuterių ir programinės įrangos bei interneto paslaugų naudojimą.

8. **Programinė įranga** – tai kompiuterių programos, skirtos kompiuterių įrangos valdymui bei kompiuterio naudotojo uždavinių sprendimui kompiuteriu (operacinės sistemos, programavimo sistemos, biuro programų paketai, antivirusinės, archyvavimo bei kitos taikomosios programos).

9. **Privilegiuota prieiga** – teisių rinkinys, suteikiantis teisę Darbuotojui administruoti informacines sistemas techniniu ir programiniu lygmeniu ir atlikti kitas Administratoriaus teisių reikalaujančias funkcijas ar atlikti informacijos saugos įgaliojimo funkcijas. Tokia teisė suteikiama Mažeikių politechnikos mokyklos direktoriaus įsakymu.

10. **Keitimas** – bet kurios informacijos apdorojimo priemonės arba jos elemento pridėjimas, išėmimas iš arba modifikavimas.

11. **Keitimų valdymas** – procesas keitimų gyvavimo ciklui valdyti, kurios pagrindinis tikslas – leisti atlikti naudingus pokyčius minimaliai trikdant Mažeikių politechnikos mokyklos veiklą. Keitimai turi būti lengvai atsekami ir išsamiai dokumentuojami.

12. **Kompiuterių tinklo naudotojas** – tai kompiuterio tinklo naudotojams prieinamos interneto paslaugos (WWW, elektroninis paštas ir pan.), kompiuterių naudotojams skirta atmintis serverių diskuose, kolektyviai naudojama programinė įranga ir panašiai.

13. **IS** – Informacinė sistema.

14. **IT** – Informacinės technologijos.

15. **Incidentas** – realų ar potencialiai nepageidaujamą poveikį kompiuterio ar kompiuterių tinklo veiklai turintis įvykis, kurio rezultatas – apgaulė, įsilaužimas į tinklo kompiuterius, kompiuterinių virusų arba nepageidaujamų laiškų atakos nuostoliai ar piktnaudžiavimas, grėsmė informacijai, informacijos nuosavybės praradimas ar žala jai, kiti kompiuterių tinklą trikdantys veiksmai.

16. **Informacija** – visi kompiuteryje saugomi duomenų rinkiniai.

17. **Informacijos apdorojimo priemonės** – kompiuterių techninė ir programinė įranga.

18. **Materialiai atsakingas darbuotojas** – įgaliotas Mažeikių politechnikos mokyklos darbuotojas atsakingas už informacijos valdymą.

19. **Failų serveris** – duomenų laikymo įrenginys, prijungtas prie Mažeikių politechnikos mokyklos kompiuterių tinklo ir pasiekiamas visiems to tinklo naudotojams. Į failų serverį vienu metu gali kreiptis keli naudotojai.

20. **Aktyvus katalogas** (Active Directory) – tai priemonė naudojama saugoti informaciją apie tinklo išteklius ir kompiuterių naudotojus, centralizuojant kompiuterių tinklą.

21. **Patikrinimas** – procedūra, kurios metu susipažįstama su Darbuotojo elektroninio pašto turiniu, laikantis Apraše nustatytos tvarkos.

22. **Informacijos saugos įgaliotinis** – Mažeikių politechnikos mokyklos direktoriaus įsakymu paskirtas mokyklos darbuotojas, dirbantis pagal darbo sutartį.

III SKYRIUS

KOMPIUTERIO NAUDOTOJO PASKYRA

23. Kompiuterio naudotojo paskyros vardas sudaromas iš asmens vardo, taško ir pavardės, pavyzdžiui, petro petraičio paskyros registracijos vardas būtų – petras.petraitis. Jei Mažeikių politechnikos mokykloje būtų keli darbuotojai, kurių vardai ir pavardės sutaptų, vėliau pradėjusiam darbą asmeniui paskyra suteikiama, naudojant dvi vardo raides, tašką ir pavarde, pavyzdžiui:

petras.petraitis;

pe.petraitis;

24. Sudarant naudotojų paskyras, jų ilgis neturi viršyti 20 simbolių. Jeigu pavardės ilgis yra ilgesnis nei 18 raidžių, paskyros pavadinimas apribojamas 18 simbolių, paliekant 2 simbolius taškui ir vardo pirmai raidei. Gali būti naudojamos tik lotyniškos raidės.

25. Kiekvienas Kompiuterių naudotojas su savo paskyra ir savo slaptažodžiu gali prisijungti iš bet kurio Mokyklos kompiuterio, prijungto prie Aktyvaus katalogo (Active Directory), kuriame galės matyti savo dokumentus patalpintus failų serveryje ir pirminį darbalaukį (Desktop). Pirmą kartą prijungus prie kompiuterio sukuriama nauja paskyra.

26. Prisijungus prie paskyros iš kito Mažeikių politechnikos mokyklos kompiuterio, bus užtikrinta, kad prisijungęs Kompiuterio naudotojas neturėtų galimybės matyti kitų Kompiuterio naudotojų duomenų.

IV SKYRIUS

KOMPIUTERIO NAUDOJIMAS

27. Darbuotojui jo darbo Mažeikių politechnikos mokyklos laikotarpiu turi būti skirtas kompiuteris jo darbo funkcijoms vykdyti.

28. Informacija apie Kompiuterinę ir Programinę įrangą bei jų pakeitimus registruojama kompiuterio žurnale. Šį žurnalą saugo ir duomenis registruoja atsakingas Administratorius. Žurnale minimaliai turi būti šį informacija: keičiamos kompiuterinės Programinės įrangos pavadinimas, versija, paskutinė atnaujinimo data, vienetų skaičius ir informacija apie Programinės įrangos naudojamos darbo vietoje, kilmės bei legalumo dokumentus.

29. Mažeikių politechnikos mokyklos darbuotojo kompiuteris turi būti prijungtas prie Aktyvaus katalogo (Active Directory).

30. Kompiuteryje turi būti įdiegta ir periodiškai atnaujinama antivirusinė Programinė įranga.

31. Programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka Administratorius.

32. Siekiant užtikrinti kompiuterio ir IT saugumą, Kompiuterių naudotojams apribojamos teisės diegti Programinę įrangą savavališkai.

33. Kompiuterinės įrangos naudojimui draudžiama:

33.1. leisti naudotis Kompiuterine įranga pašaliniams asmenims;

33.2. naudotis svetimu prisijungimo vardu;

33.3. taisyti, laužyti ir gadinti Kompiuterinę įrangą, kitaišduota Mokyklos IT turtą;

33.4. savavališkai keisti jam priskirtą Kompiuterinę įrangą (pakeisti kompiuterį, spausdintuvą, monitorių, klaviatūrą, pelę ir pan.), taip pat savarankiškai perkelti sumontuotą Kompiuterinę įrangą į kitą vietą (visus techninių priemonių perkėlimus darbo vietoje bei tarp Kompiuterių tinko naudotojų vykdo Administratorius);

33.5. išnešti iš Mažeikių politechnikos mokyklos patalpų Kompiuterinę įrangą iš skyrus naudojantiems nešiojamuosius kompiuterius ar kitą Kompiuterinę įrangą, kai tai būtina tiesioginėms darbo funkcijoms vykdyti. Šis draudimas netaikomas, vykdant Kompiuterinės įrangos taisymo ir priežiūros funkcijas, kurias atlieka atsakingas darbuotojas;

33.6. naudoti Kompiuterinę įrangą veiklai, kuri nesuderinama su darbuotojo atliekamomis funkcijomis, etika;

33.7. Atlikti veiksmus, pažeidžiančius fizinio ar juridinio asmens teises, kurias saugo autorių, gretutinių ir intelektualios nuosavybės (pvz.: dainos, filmai ir kt.)teisių apsaugos įstatymai. Tarp tokių veiksmų yra savavališkas Programinės įrangos diegimas, naudojimas, saugojimas arba platinimas, neturint licencijos, neleistas autorių teisėmis apsaugotų kūrinių kopijavimas;

33.8. vykdyti ar atidarinėti piktybines programas (t.y. kompiuterinius virusus, kirminus „Trojaus arklius“ ir pan.);

33.9. atskleisti prisijungimo duomenis prie kompiuterio, Mokyklos naudojamų sistemų ir informacijos išteklių prisijungimo vardus, slaptažodžius arba leisti naudotis savo prisijungimo duomenis kitiems asmenims;

33.10. naudoti programas ir atlikti bet kokio pobūdžio veiksmus, kurie sunkina ar trikdo kompiuterio veikimą arba gali sukelti incidentą kompiuterių tinkluose;

33.11. savavališkai leisti suteiktus kompiuterio tinklo parametrus (IP adresą ir ap.);

33.12. savavališkai trinti. Manipuliuoti ir iškreipti darbo metu gautą, naudojamą bei sukurtą informaciją siekiant pakenkti Mažeikių politechnikos mokyklai ar jos darbuotojams;

34.13. naršyti pornografiniuose, smurtą, terorizmą bei kitokią nusikalstamą veiklą programuojančiuose tinklapiuose, elektroniniu paštu platinti elektronines šiukšles, piktybines programas, virusus, įsilaužti į kitas kompiuterines sistemas;

33.14. vykdyti failų mainus tarp interneto vartotojų naudojant lygiavertiškumo (angl. Peer to peer, P2P) tipo programas (pvz.: „uTorrent“, „eMule“, „DC++“, „BitComet“ ir kt.);

33.15. įdiegti ir pašalinti taikomąsias ar kitokio pobūdžio programas, išskyrus, kai tai daro Administratorius;

33.16. nesankcionuotai naudotis svetimais kompiuterių ir kitais informacinių technologijų ištekliais (kopijuoti ir naudotis programomis ir duomenimis be išteklių savininko žinios ir sutikimo, jungtis prie svetimų kompiuterių be atitinkamo leidimo ir pan.), išskyrus Administratoriams, kurie turi tokią teisę. Mažeikių politechnikos mokyklos darbo tikslais, užtikrinant konfidencialios informacijos apsaugą ir kitus informacijos saugos aspektus;

33.17. atlikti bet kokius kitus veiksmus, pažeidžiančius ES ir nacionalinės teisės aktus;

34. Kompiuterio naudotojas privalo:

34.1. įvykus incidentui ar kilus klausimams dėl kompiuterio naudojimo kreiptis/informuoti Administratorių;

34.2. leisti administratoriui įvertinti kompiuterio būklę;

34.3. naudoti jam skirtą Kompiuterinę įrangą efektyviai ir pagal paskirtį, taupyti išteklius;

34.4. apsaugoti kompiuterį asmeniniu slaptažodžiu aprašo VI dalyje nustatyta tvarka;

34.5. baigus darbą, uždaryti visas programas, išsiregistruoti iš savo Kompiuterio naudotojo aplinkos ir išjungti kompiuterį.

V SKYRIUS

NEŠIOJAMŲ KOMPIUTERIŲ IR MOBILIŲJŲ ĮRENGINIŲ NAUDOJIMAS

35. Nešiojamų kompiuterių ir mobiliųjų įrenginių naudojimui (toliau – Nešiojami įrenginiai), įskaitant asmeninius įrenginius, naudojamus darbui Aprašo 60 punkto atveju, taikomi Aprašo IV dalyje nurodyti naudojimosi reikalavimai ir žemiau nurodytos papildomos apsaugos priemonės:

35.1. prisijungimas prie nešiojamo kompiuterio operacinės ir BIOS sistemos turi būti apsaugotas slaptažodžiu, Aprašo VI dalyje nustatyta tvarka;

35.2. nenaudojant Wi-Fi, Bluetooth ar kitų belaidžių technologijų – jų funkcijos turi būti išjungtos;

36. Administratorius kartą per pusę metų privalo atlikti Nešiojamų įrenginių patikrą ir priežiūrą. Patikrą galima atlikti nuotoliniu būdu, prisijungus prie Nešiojamo įrenginio (kai

Nešiojamas įrenginys prijungtas prie vidinio kompiuterių tinklo), naudojant Nešiojamų įrenginių valdymo sistemą arba darbuotojui fiziškai pristatius Nešiojamą įrenginį.

37. Administratorius Darbuotojų grąžintuose nenaudojamuose Nešiojamuose įrenginiuose esančią informaciją suarchyvuoja, patalpina į tam skirtą vietą serveryje bei ištrina iš Nešiojamo įrenginio taip, kad jos negalima būtų atkurti.

38. Darbuotojai jiems Mokyklai suteiktus Nešiojamus įrenginius privalo naudoti tik Mokyklos darbo funkcijoms vykdyti.

39. Darbuotojai privalo laikytis šių Nešiojamų įrenginių naudojimo reikalavimų:

39.1. saugoti Nešiojamą įrenginį nuo aplinkos poveikio – dulkių, vibracijos, cheminių medžiagų, elektromagnetinio spinduliavimo;

39.2. saugoti nuo didelių temperatūros pokyčių;

39.3. nepalikti Nešiojamo įrenginio be priežiūros viešose vietose;

39.4. kelionių metu registruoti Nešiojamą įrenginį kaip rankinį bagažą;

39.5. pasitraukus nuo nešiojamo kompiuterio, įjungti ekrano užsklandą su slaptažodžiu;

39.6. nesinaudojant mobiliuoju įrenginiu, apsaugoti jį slaptažodžiu arba biometrinėmis apsaugos priemonėmis;

39.7. nenaudojamus Nešiojamus įrenginius grąžinti atsakingam Mokyklos darbuotojui;

39.8. pametus Nešiojamą įrenginį ar įvykus jo vagystei, nedelsiant informuoti Administratorių, Informacijos saugos įgaliotinį ir įrenginį išdavusį Mokyklos darbuotoją;

40. Darbuotojams draudžiama:

40.1. mėtyti, laužyti, daužyti, ardyti Nešiojamus įrenginius, dėti ant jų sunkius daiktus;

40.2. bandyti šalinti, apeiti ar išjungti įrenginyje nustatytas saugumo priemones;

40.3. leisti naudotis nešiojamu įrenginiu kitiems žmonėms;

40.4. išimti Nešiojamo įrenginio bateriją jo neišjungus ar kitaip pažeisti gamintojo nustatytas eksploataavimo rekomendacijas.

VI SKYRIUS

SLAPTAŽODŽIŲ NAUDOJIMAS

41. Darbuotojai privalo saugoti slaptažodžius, neatskleisti jų kitiems asmenims, nelaikyti matomose ir lengvai kitiems asmenims prieinamose vietose ir laikytis šių reikalavimų:

41.1. unikalūs, sudaryti iš ne mažiau kaip 8 simbolių, slaptažodyje turi būti bent 1 didžioji raidė, bent 1 mažoji raidė, bent 1 skaičius arba specialusis simbolis. Fiksuojama 24 (dvidešimt keturių) prieš tai buvusių slaptažodžių kombinacija, kuri negali pasikartoti;

41.2. leistinas prisijungimų prie savo kompiuterinės darbo aplinkos (paskyros) bandymų skaičius – 5. Po 5 nesėkmingų bandymų prisijungti prie savo kompiuterinės darbo aplinkos (paskyros) paskyra blokuojama, paskyros valdytojas privalo kreiptis į Administratorių.

41.3. slaptažodžiams sudaryti negalima naudoti asmeninio pobūdžio informacijos (vardų, pavardžių, gimimo datų, naminių gyvūnų vardų);

41.4. negalima naudoti kompiuterio klaviatūros sekos, pvz.: 123321, qwerty ar pan.;

41.5. kilus įtarimui, kad slaptažodis gali būti žinomas kitiems asmenims jį būtina pasikeisti;

41.6. draudžiama keisti prisijungimo vardais, prisijungti prie informacinių išteklių, naudojantis kito naudotojo prisijungimo duomenimis;

41.7. gavus laikiną slaptažodį privaloma jį iš karto pasikeisti;

41.8. slaptažodį naudotojui galima keisti antrą kartą ne anksčiau kaip po 1 dienos;

41.9. slaptažodis gali galioti ne daugiau kaip 60 dienų;

41.10. apie slaptažodžio galiojimo termino pabaigą sistema turi informuoti naudotoją prieš 7 dienas;

41.11. nenaudoti to paties slaptažodžio registruojantis interneto svetainėse ir Mokyklos informacinėse sistemose, kompiuteryje.

42. Prieigai prie padidinto konfidencialumo informacijos, sistemų administravimui ir privilegijuotų prieigų naudojamiems slaptažodžiams keliami papildomi reikalavimai:

42.1. slaptažodžiai turi būti sudaryti iš ne mažiau kaip 12 ženklų, parinktų atsitiktine tvarka;

42.2. neidentifikuotos prieigos (pvz.: info@mazeikiupm.lt, info.vieksniai@mazeikiupm.lt) turi būti apsaugotos slaptažodžiu, sudarytu iš ne mažiau kaip 12 simbolių.

42.3. slaptažodžių tvarkymui rekomenduojama naudoti slaptažodžių tvarkymo Programinę įrangą.

VII SKYRIUS

PRIEIGOS VALDYMAS

43. Darbuotojams prieiga prie informacinių išteklių suteikiama Darbuotojo pareigų ir vaidmenų Mažeikių politechnikos mokyklos veiklos procesuose pagrindu.

44. Darbuotojams suteikiama tiek prieigos teisių, kiek jiems būtina atlikti Mažeikių politechnikos mokyklos darbo funkcijoms.

45. Darbuotojo ir Administratoriaus prieigos teisės turi būti atskirtos, naudojant skirtingas paskyras.

46. Privilegiuotos prieigos teisių nenaudoti įprastai veiklai, kurią galima vykdyti turint Darbuotojo prieigos teises, atlikti. Privilegiuotos prieigos teisės negali apimti prieigos prie konfidencialios informacijos arba padidinto konfidencialumo informacijos, išskyrus atvejus, kai to reikia jų įprastai IT pagalbos veiklai atlikti.

47. Privilegiuotos prieigos teisės paskiriamos Mažeikių politechnikos mokyklos direktoriaus įsakymu.

48. Prieiga prie Mažeikių politechnikos mokyklos informacinių išteklių suteikiama Darbuotojo tiesioginio vadovo prašymu. Informaciją apie reikalingas suteikti prieigas asmeniui, Administratorius gauna tiesiogiai iš priimamo Darbuotojo tiesioginio vadovo po to, kai Mažeikių politechnikos mokyklos direktorius pasirašo įsakymą dėl prieigos suteikimo.

49. Kai keičiasi Darbuotojo pareigos ar vaidmenys Mažeikių politechnikos mokykloje arba Darbuotojas atleidžiamas iš darbo, tiesioginis Darbuotojo vadovas nedelsiant elektroniniu paštu informuoja apie tai Administratorių, kuris atsakingas už prieigos suteikimą.

50. Prieigos teisės turi būti suteikiamos, vadovaujantis tiesioginio Darbuotojo vadovo pavedimu pagal jame nurodytas Darbuotojo pareigas ir vaidmenį.

51. Trečiosioms šalims prieiga prie Mažeikių politechnikos mokyklos informacinių išteklių suteikiama sutartyse su trečiosiomis šalimis nustatyta tvarka ir tik pasirašius konfidencialumo susitarimus.

52. Visi prieigų teisių turėtojų registravimo ar šios informacijos pakeitimai turi būti išsaugomi IS audito žurnale.

53. Informacijos saugos įgaliotinis periodiškai, ne rečiau kaip kartą per metus, organizuoja naudotojų prieigos teisių turėtojų ir slaptažodžių naudojimo reikalavimų laikymosi peržiūrą.

VIII SKYRIUS

NEŠIOJAMŲ LAIKMENŲ NAUDOJIMAS

54. Darbuotojams draudžiama jungti ne Mažeikių politechnikos mokyklos duomenų laikmenas (CD ir DVD įrenginius, išorinius kietuosius diskus, USB atminties korteles) prie Mažeikių politechnikos mokyklos kompiuterių, išskyrus Mažeikių politechnikos mokyklos išduotas ir Administratoriaus patikrintas laikmenas. Esant tarnybiniam poreikiui, ne Mažeikių politechnikos mokyklos išduotą duomenų laikmeną galima įjungti į Mažeikių politechnikos mokyklos Kompiuterinę įrangą, prieš tai patikrinus Administratoriui.

55. Nešiojamose duomenų laikmenose saugoma padidinto konfidencialumo, konfidenciali informacija, asmenų, susijusių darbo santykiais su reguliuojamomis įmonėmis, taip pat reguliuojamų įmonių valdybos narių, akcininkų duomenys turi būti šifruojami.

56. Nenaudojamas arba sugedusias keičiamas duomenų laikmenas Darbuotojai turi grąžinti Administratoriui, kuris yra atsakingas už saugų laikmenose esančios informacijos sunaikinimą.

57. Darbuotojai turi užtikrinti, kad perdavimo metu duomenų laikmenos su įrašyta informacija patektų nurodytam informacijos gavėjui ir būtų apsaugotos nuo neteisėtos prieigos ar sugadinimo.

58. Nesant galimybei duomenų laikmenų perduoti asmeniškai informacijos gavėjui, turi būti naudojami patikimi siuntų vežėjai, užtikrinantys duomenų laikmenos pristatymą nurodytam gavėjui.

IX SKYRIUS

NUOTOLINIS DARBAS

59. Darbuotojai prisijungti prie Mažeikių politechnikos mokyklos informacinių išteklių nuotoliniu būdu gali tik gavę tiesioginio vadovo leidimą. Nuotolinis prisijungimas turi būti autorizuotas ir galimas tik naudojant šifruoto ryšio kanalus, išskyrus Mažeikių politechnikos mokyklos darbuotojo elektroninį pašta.

60. Darbuotojams jungiantis prie Mažeikių politechnikos mokyklos Dokumentų valdymo sistemos ir Mažeikių politechnikos mokyklos Darbuotojui suteiktos elektroninio pašto paskyros iš Mažeikių politechnikos mokyklos nepriklausančių kompiuterio ar mobiliojo telefono, Darbuotojas privalo informuoti Administratorių ir laikytis būtinų saugumo priemonių bei informacijos konfidencialumo apsaugos.

X SKYRIUS

KOMPIUTERIŲ TINKLO NAUDOJIMAS

61. Galimybė naudotis Mažeikių politechnikos mokyklos kompiuterių tinklu ir Kompiuterių tinklo ištekliais suteikiama tik darbo Mažeikių politechnikos mokyklos laikotarpiu.

62. Mokyklos kompiuterių tinklo ištekliai skirti profesiniam darbui, kvalifikacijos kėlimui. Asmeniniais tikslais kompiuterių tinklo ištekliais Darbuotojai gali naudotis tiek, kiek tai netrukdo jam atlikti pareigas Mokykloje ir neprieštarauja etiško elgesio normoms.

63. Bevielio tinklo prieigai (WI-FI) Mokyklos patalpose yra sukonfigūruotos stotelės, kurios skirtos Darbuotojams ir Mokyklos svečiams. Bevielio tinklo slaptažodžius suteikia ir keičia Mažeikių politechnikos mokykloje atsakingas darbuotojas.

64. Informacijos saugumo užtikrinimui Mokyklos svečiams suteikiamas tik (svečiams skirtas) prisijungimo prie bevielio tinklo slaptažodis.

65. Darbuotojai atsako už veiksmus, kurie kenkia kompiuterinei, kompiuterių tinklo įrangai ir informacijai, atliktus pasinaudojus disponuojamais ištekliais arba atliktus jo vardu.

66. Kompiuterių tinkle draudžiama:

66.1. leisti naudotis Mažeikių politechnikos mokyklos kompiuterių tinklo ištekliais ir teikiamomis paslaugomis juridiniams ir fiziniams asmenims, kurie tiesiogiai nesusiję su Mažeikių politechnikos mokykla ar jos veikla;

66.2. naudoti tinklo išteklius tarptautinėje teisėje ir praktikoje pripažinti neteisėtai veiklai vykdyti, taip pat Lietuvos Respublikos įstatymų ir kitų teisės aktų draudžiamai veiklai;

66.3. kompiuterio tinklo išteklius naudoti komercinei veiklai, smurto, amoralaus elgesio skatinimui, komentarų rašymui, įžeidžiančių dalykų skleidimui ir pan.

66.4. žiūrėti, kaupti arba platinti pornografinę, rasinę, tautinę neapykantą ar smurtą propaguojančią medžiagą, Komisijos vardą diskredituojančią medžiagą, kitus juridinius ir fizinius asmenis ar valstybę įžeidžiančią informaciją;

66.5. dalyvauti lažybose ir azartiniuose lošimuose internetu, žaisti internetinius žaidimus;

66.6. komentuoti interneto svetainėse;

66.7. užsiimti veikla, kuri nesuderinama su Darbuotojo etika;

66.8. parsisiųsti arba platinti Programinę įrangą arba kitą informaciją, kurios diegimas, naudojimas arba platinimas prieštarautų Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo reikalavimams arba Komisijos teisės aktų nuostatoms;

66.9. skelbti Komisijos Kompiuterių tinklo ištekliuose su Komisijos veikla nesusijusius ir asmeninius tinklalapius;

66.10. savavališkai keisti Kompiuterių tinklo išteklių parametrus, susijusius su apsauga, arba prisijungiant apeiti bet kurį iš įdiegtų saugumo mechanizmų;

66.11. darbo vietos kompiuteryje blokuoti antivirusines priemones;

66.12. atskleisti bevielio tinklo prisijungimo duomenis tretiesiems asmenims;

66.13. instaliuoti programas bei savavališkai šalinti svetimas bylas, kopijuoti, laikyti ir žaisti žaidimus;

66.14. perduoti Kompiuterio tinklo naudotojui suteiktas teises bei išteklius ar teikti kompiuterių tinklo paslaugas tretiesiems asmenims;

66.15. naudotis neskirtais ištekliais, kopijuoti įdiegtas programas, kitais būdais pažeidinėti saugumą, privatumą, tvarką ir kitų kompiuterių naudotojų teises;

66.16. skleisti melagingą informaciją, įžeidinėti ar priekabauti prie kitų asmenų naudojant Mokyklos kompiuterių tinklo sistemas arba siųsti tokią informaciją, pasinaudojant Mokyklos vardu;

66.17. naudoti programas ar atlikti bet kokio pobūdžio veiksmus, kurie sunkina ar trikdo tinklo veikimą arba gali sukelti incidentą kompiuteriuose ar kompiuterių tinkle (neautorizuotas servisų naudojimas, konfidencialios informacijos atskleidimas ar pakeitimas, servisų darbo sutrikdymas, kompiuterių virusai, tinklo skenavimo programos, tinklo blokavimo programos ir kt.);

66.18. pasirašyti apsimečius kitu asmeniu, ar kompanija;

66.19. be išankstinės Administratoriaus žinios naudoti asmeninę Kompiuterinę ir Programinę įrangą, jungti ją į Komisijos tinklą.

67. Kompiuterių tinklo naudotojas privalo:

67.1. laikytis etikos normų ir atsakyti už informaciją, pateiktą į kompiuterių tinklus;

67.2. laikytis Administratoriaus nurodymų, vykdyti visus nurodymus, susijusius su kompiuterių tinklo valdymu bei saugumu;

67.3. įvykus kompiuteriniam incidentui, nedelsiant informuoti Administratorių;

67.4. saugoti jam suteiktus prisijungimo vardus ir slaptažodžius;

67.5. naudoti jam skirtus Kompiuterių tinklo išteklius pagal paskirtį.

68. Kompiuterių tinklo naudotojo teisės:

68.1. blokuoti savo informaciją nuo kitų Kompiuterių tinklo naudotojų neleistino naudojimosi;

68.2. iškilus problemų dėl kompiuterių tinklo veikimo, kreiptis į Administratorių;

68.3. naudotis bendra vieta Failų serveryje, elektroniniu paštu, interneto tinklu ar kita informacine sistema, vykdant Komisijos darbo funkcijas.

XI SKYRIUS

LICENCIJUOTOS PROGRAMINĖS ĮRANGOS NAUDOJIMAS

69. Naudojama tik licencijuota ir legali Programinė įranga.

70. Programinę įrangą galima naudoti tik jos licencijoje nurodyta tvarka.

71. Programinė įranga negali būti perduota kitam Kompiuterių tinklo naudotojui be Administratoriaus žinios.

72. Licencijuotos Programinės įrangos naudojimo tvarkos laikymąsi užtikrina kiekvienas Kompiuterių tinklo naudotojas.

73. Už Programinės įrangos naudojimą be licencijų Kompiuterių tinklo naudotojai atsako įstatymų nustatyta tvarka.

XII SKYRIUS

ELEKTRONINIO PAŠTO NAUDOJIMAS

74. Kiekvienam Darbuotojui yra suteikiamas elektroninio pašto adresas.

75. Elektroninio pašto adresai Darbuotojams suteikiami tik darbo Mažeikių politechnikos mokykloje laikotarpiu.

76. Elektroninio pašto adresas sudaromas naudojant lotynišką raides pagal tokį šabloną: vardenis.pavardenis@mazeikiupm.lt, jei Darbuotojas turi du vardus ar pavardes, sudarant elektroninio pašto adresą pasirenkamas jo pirmas vardas ir nurodyta pavardė.

78. Administratorius, atsižvelgdamas į struktūrinio padalinio vadovo motyvuotą prašymą bei Apraše nustatytus reikalavimus, sukuria netipinius (bendrojo naudojimo) elektroninio pašto adresus. Juos rekomenduojama sudaryti laikantis šių nuostatų: pasirinkti vieną žodį (pvz.: duomenubazesadministratorius) arba žodžius jungti brūkšneliu (galima ir pabraukti, pvz.: asistema_administratoriai), naudoti departamento pavadinimo ir skyriaus pavadinimo santrumpas, atskirtas tašku, jeigu bendras pašto adresas kuriamas padalinio skyriui (pvz.: skyriaus trumpinis.skyriaustrumpinys@mazeikiupmlt).

79. Pasibaigus darbo santykiams su Darbuotoju (elektroninio pašto naudotoju) elektroninio pašto Administratorius išbraukia jį iš Mažeikių politechnikos mokyklos elektroninio pašto naudotojų sąrašo.

80. Nesant darbo vietoje elektroninį (darbinį) paštą galima pasiekti ir per internetinę naršyklę adresu: <https://www.gmail>. prisijungimo vardas yra Darbuotojo vardas, taškas, pavardė lotyniškais raidėmis ir @mazeikiupm.lt domenas (pvz.: vardenis.pavardenis@mazeikiupm.lt).

81. Mažeikių politechnikos mokyklos Darbuotojų darbo koordinavimui naudojamas elektroninio pašto paskyroje įdiegtas kalendorius. Kitus kalendorius naudojantis Darbuotojas, dėl nepilno funkcionalumo, nesuderinamumo, negautų priminimų, kitų dėl to atsiradusių problemų, atsako asmeniškai.

82. Mažeikių politechnikos mokyklos Darbuotojas (elektroninio pašto naudotojas) turi nuolat peržiūrėti savo informaciją elektroninio pašto dėžutėje, pašalinti iš sistemos tik pasenusius ir nebeaktualius laiškus, t. y. juos pašalinti ir iš „Deleted Items“ katalogo:

82.1. draudžiama iš elektroninio pašto trinti svarbius elektrinius laiškus, kurie reikalingi Mokyklos funkcijoms vykdyti, įskaitant, bet neapsiribojant, elektrinius laiškus, susijusius su viešųjų pirkimų vykdymu, sutarčių vykdymu, informaciją, susijusią su reguliuojamų įmonių veikla ir pan. Elektroninis paštas yra ryšio priemonė, skirta tiesioginėms funkcijoms atlikti, ir Darbuotojai turi naudoti šią priemonę atsakingai, veiksmingai ir teisėtais tikslais. Elektroniniam paštui taikomos tokios pačios taisyklės, kaip ir kitoms rašytinės informacijos perdavimo

priemonėms, todėl visi pranešimai turi atitikti raštvedybos standartus, skirtus bendrauti raštu. Darbuotojai turi žinoti, kad dėl elektroninių laiškų Mažeikių politechnikos mokyklos darbuotojams ir administracijai gali kilti teisinių padarinių, jeigu:

82.1.1. siunčiami ar persiunčiami elektroniniai laiškai, kuriuose yra prieštaraujančių įstatymams, neatitinkančių realybės, įžeidžiančių, užgaulių, rasistinių, propaguojančių smurtą, pornografinio pobūdžio ar nepadorių teiginių;

82.2. be autoriaus sutikimo persiunčiami autorinėmis teisėmis apsaugoti kūriniai;

82.3. išsiunčiamas elektroninis laiškas, kuriame yra virusas;

82.4. siunčiamuose elektroniniuose laiškuose yra informacija, teisės aktų nustatyta tvarka pripažįstama konfidenciali, padidinto konfidencialumo informacija ir asmens duomenys;

83. Elektroninis paštas turi būti naudojamas tik Mažeikių politechnikos mokyklos veiklos funkcijoms atlikti.

84. Mažeikių politechnikos mokyklos elektroninio pašto serveryje naudotojų elektroninio pašto dėžutėse esanti informacija kopijuojama ir saugoma. Iš elektroninio pašto serveryje esančių naudotojų elektroninio pašto dėžučių į darbo vietų kompiuterius perkelta informacija nekopijuojama.

85. Elektroninio pašto naudotojams privaloma:

85.1. elektroninės žinutės laukelyje „Subject“ trumpai ir aiškiai aprašyti laiško turinį ir, jeigu siunčiamas dokumentas pažymėtas konfidencialumo žyma arba žinutės turinyje yra konfidencialios ar padidinto konfidencialumo informacijos, nurodyti konfidencialumo žymą;

85.2. suprantamai ir etiškai suformuluoti laiško tekstą, laiške nurodyti siuntėjo duomenis pagal bendrą formą: vardas ir pavardė, pareigos, padalinio ir struktūrinio padalinio pavadinimas, Mažeikių politechnikos mokyklos pavadinimas, telefonas (automatinio parašo elektroniniuose laiškuose nustatymo aprašas pateiktas Mokyklos interneto vidaus svetainėje);

85.3. prieš išvykstant atostogauti arba į tarnybinę komandiruotę, aktyvuoti automatinio atsakymo siuntimo nustatymą (automatinio atsakymo elektroninio pašto nustatymo aprašas pateiktas Mokyklos vidaus svetainėje);

85.4. nenurodyti (nepateikti) Mažeikių politechnikos mokyklos elektroninio pašto asmeninių pažinčių svetainėse, elektroninėse parduotuvėse, komercinių pasiūlymų, nuolaidų, akcijų svetainėse ir pan. asmeniniais tikslais, pvz.: įsigyjant prekes arba nuolaidų korteles, laisvalaikio ir kitose su darbo funkcijomis nesusijusiose svetainėse – forumų, turizmo agentūrų, socialinių tinklų svetainėse, neatsakinėti į reklaminius laiškus (brukalus), kad šiuo adresu nepasinaudotų nepageidaujamų laiškų siuntėjai;

85.5. visada atidžiai užrašyti ir patikrinti elektroninio pašto adresą, kad apsirikus informacija nebūtų nusiųsta kitam (netinkamam) adresatui;

85.6. visada atidžiai peržiūrėti atsiųstų rinkmenų pavadinimus ir, jeigu atsiųsta informacija kelia įtarimų, nežinoma, nesuprantama, nepažįstamas ją atsiuntęs asmuo arba įtariama, kad gali būti atsiųstas virusas, nepaleisti programų, neatidarinėti rinkmenų, o nedelsiant kreiptis į kompiuterinę darbo vietą prižiūrintį Administratorių;

85.7. įsitikinti, ar tinkamas elektroniniu paštu gautos informacijos siuntėjas (žinoma tapatybė), ar tai jis siuntė konkrečią informaciją, jeigu abejojama elektroniniu paštu gauta informacija ir jos siuntėju. Pasitikrinti rekomenduojama alternatyviomis priemonėmis (pvz.: faksu, telefonu ir t. t.). Tik siuntėjo skaitmeniniu sertifikatu pasirašyti laišakai garantuoja siuntėjo tapatumą ir neiškraipytą informaciją;

85.8. baigiant darbą Mažeikių politechnikos mokykloje, peržiūrėti susirašinėjimą elektroniniu paštu. Svarbius elektroninius laiškus, užtikrinančius veiklos tęstinumą, persiųsti struktūrinio padalinio vadovo nurodytam Darbuotojui, o kitus elektroninius laiškus sunaikinti;

85.9. vadovautis Informacijos žymėjimo ir priežiūros procedūra ir Aprašu, siunčiant jose nustatytą informaciją elektroninėmis ryšio priemonėmis.

85.10. apsimesti svetimais arba neegzistuojančiais elektroninio pašto naudotojais perduodant duomenis arba kitą informaciją;

85.11. naudoti elektroninio pašto automatinio persiuntimo funkciją ne Mažeikių politechnikos mokyklos elektroninio pašto adresais;

85.12. kopijuoti ir platinti Mažeikių politechnikos mokyklos elektroninio pašto sistemoje pateikiamas kitų darbuotojų nuotraukas arba kitus asmens duomenis;

85.13. atidarinėti elektroninių laiškų priedus, kurie gauti iš nepatikimų siuntėjų ar atrodo įtartini;

85.14. siųsti elektroniniu paštu neužšifruotą padidinto konfidencialumo informaciją;

85.15. siųsti elektroniniu paštu asmenų, susijusių darbo santykiais su reguliuojamomis įmonėmis, taip pat reguliuojamų įmonių valdybos narių, akcininkų duomenis;

85.16. siųsti elektroniniu paštu informaciją apie informacijos saugumo užtikrinimo priemones ir slaptažodžius;

85.17. kurti ar persiųsti vadinamuosius grandinius elektroninio laiškus, kuriuose skatinama persiųsti elektroninio laišką savo draugams ar pan.;

85.18. vidaus ir išorės adresatams siųsti menkaverčio turinio elektroninius laiškus, įskaitant (bet neapsiribojant) nepageidaujamo turinio elektroninius laiškus.

86. Elektroninio pašto naudotojams draudžiama:

87. Draudžiama asmeninę elektroninę pašta naudoti Mažeikių politechnikos mokyklos veiklos funkcijoms atlikti.

XIII SKYRIUS

MOKYKLOS INTERNETO SVETAINĖ

88. Mažeikių politechnikos mokyklos interneto svetainė administruojama, vadovaujantis Bendrųjų reikalavimų valstybės ir savivaldybėms institucijų interneto svetainėms aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2003 m. balandžio 18 d. nutarimu Nr. 480 „Dėl bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms aprašo patvirtinimo“.

89. Mažeikių politechnikos mokykla ir skyriai administruoja šią Mažeikių politechnikos mokyklos interneto svetainėje skelbiamą informaciją:

89.1. **Veiklos valdymo skyrius** – interneto svetainės skyrius „Naujienos“, „Veikla“, „Teisinė informacija“, „Struktūra ir kontaktai“, „Nuorodos“, „Bendradarbiavimas“, „Karjera“, „Viešosios konsultacijos“ ir visus kitus, išskyrus 91.2 ir 91.3 papunkčiuose numatytus skyrius;

89.2. **Moksleiviams skyrius** – atnaujina informaciją apie moksleivių gyvenimą;

89.3. **Turto valdymo ir viešųjų pirkimų skyrius** – „Viešieji pirkimai“ ir kiti, reikalaujantys daugiau nei paprasto Kompiuterių naudotojo žinių, darbai.

90. Mažeikių politechnikos mokyklos direktorius, skyrių vedėjai paskiria atsakingus Darbuotojus už interneto svetainės skyrių administravimą bei informuoja Administratorių.

91. Už į Mažeikių politechnikos mokyklos interneto svetainę talpinamos informacijos patalpimą laiku atsakingas darbuotojas skyriaus, kurio kompetencijai priklauso atitinkamos informacijos (įskaitant teisės aktus ir jų projektus) rengimas.

XIV SKYRIUS

AUTOMATINIAI KOMPIUTERIO OPERACINĖS SISTEMOS ATNAUJINIMAI

92. Sėkmingam ir saugiam darbo vietų kompiuterių ir tarnybinių stočių darbui užtikrinti reikalinga, kad įrenginių operacinės sistemos būtų nuolat atnaujinamos. Šiam tikslui virtualiame serveryje *MultiSRV* įdiegta WSUS (*Windows Server Update Services*) tarnyba, kuri gauna aktuales atnaujinimus iš gamintojo portalo ir užtikrina jų pristatymą darbo vietų ir tarnybinių stočių kompiuteriams.

93. Kompiuteriui 11 val. automatiškai per WSUS diegiami atnaujinimai (dažniausiai kartą per savaitę). Įdiegus atnaujinimus gali reikėti kompiuterį paleisti iš naujo. Jeigu kompiuterio naudotojas į pasirodžiusį pranešimą/lentelę nereaguoja ir nepakeičia kompiuterio paleidimo iš naujo laiko į ilgesnį laiką nei standartinis – 10 min., tai kompiuteris bus paleistas iš naujo automatiškai praėjus konkrečiam laiko tarpui.

94. Rekomenduojama išsaugoti dokumentus prieš pasitraukiant nuo kompiuterio, nes kompiuteris gali būti paleistas iš naujo be kompiuterio naudotojo žinios, jeigu kompiuterio paleidimo iš naujo atidėjimo nustatymai nebus pakeisti.

XV SKYRIUS

ADMINISTRATORIAUS TEISĖS

95. Administratorius darbo tikslais turi teisę:

95.1. iš anksto neperspėjęs kompiuterio naudotojo prisijungti prie jo kompiuterio darbo vietoje ar nuotoliniu būdu, siekiant užtikrinti jam pavestų funkcijų atlikimą bei užtikrinant kompiuteryje esančios informacijos konfidencialumą;

95.2. Administratoriai negali piktnaudžiauti suteiktomis teisėmis;

95.3. įdiegti, pašalinti operacinę sistemą, taikomąją ar kitą Programinę įrangą kompiuterio naudotojo darbo vietoje ar nuotoliniu būdu;

95.4. kopijuoti, išsaugoti ar kitaip panaudoti darbinę informaciją (failus ir kitą informaciją) Mokyklos tikslams be išankstinio kompiuterio naudotojo sutikimo darbo vietoje ar nuotoliniu būdu, užtikrinant tokios informacijos konfidencialumą;

95.5. pastebėjęs veiksmus, galinčius daryti įtaką kompiuterių tinklo ar duomenų saugumui, Kompiuterinės įrangos naudotojui apriboti teises dirbti su jam priskirta Kompiuterine ir Programine įranga. Apie atliktus veiksmus informuojamas direktorius, tiesioginis vadovas, Administratorius ir Informacijos saugos įgaliotinis. Darbas su Kompiuterine ir Programine įranga atnaujinamas tik pašalinus pastebėtus sutrikimus.

XVI SKYRIUS

ATSAKOMYBĖ UŽ KOMPIUTERINĖS IR PROGRAMINĖS ĮRANGOS NAUDOJIMĄ

96. Materialiai atsakingas darbuotojas yra atsakingas už Kompiuterinės ir Programinės įrangos išdavimą bei priėmimą Mažeikių politechnikos mokyklos darbuotojams.

97. Mažeikių politechnikos mokyklos darbuotojai privalo saugiai, tinkamai ir ekonomiškai naudoti priskirtą Kompiuterinę ir Programinę įrangą.

98. Darbuotojas materialiai atsako už žalą, padarytą jo tyčiaisiais veiksmais, naudojant jam patikėtą kompiuterinę ir kitą IT techniką, įstatymų nustatyta tvarka.

99. Darbuotojas, įstaigos patalpose praradęs jam priskirtą Kompiuterinę ir Programinę įrangą, privalo nedelsdamas apie tai informuoti tiesioginį vadovą, Administratorių ir Informacijos

saugos įgaliotinį. Jei nešiojama Kompiuterinė ir Programinė įranga buvo prarasta ne Mokyklos patalpose, ją praradęs Darbuotojas papildomai turi dėl įvykio kreiptis į policiją.

100. Atleidžiamas iš darbo Darbuotojas jam priskirtą Kompiuterinę ir Programinę įrangą privalo grąžinti materialiai atsakingam darbuotojui.

XVII SKYRIUS TIEKĖJŲ VALDYMAS

101. Sutartyse su tiekėjais, kuriems yra suteikiama prieiga prie Mažeikių politechnikos mokyklos informacijos ir (ar) IT priemonių, turi būti įtraukti informacijos saugumo reikalavimai, susiję su veiklos ir techniniais reikalavimais, įskaitant ir nuostatas dėl konfidencialumo užtikrinimo. Tiekėjams prieiga prie Mažeikių politechnikos mokyklos informacinių išteklių gali būti suteikiama tik tokios apimties, kiek tai būtina sutarčiai įgyvendinti ir nedelsiant panaikinama, pasibaigus sutartiniams santykiams.

102. Pasibaigus sutartiniams santykiams iš tiekėjo turi būti reikalaujama grąžinti visą Mažeikių politechnikos mokyklos turtą ir gautą informaciją arba sunaikinti ją.

103. Tiekėjų teikiamos paslaugos turi būti stebimos ir kartą per metus turi būti atliekama tiekėjų paslaugų peržiūra, kurios metu atliekamas paslaugų įvertinimas, atsižvelgiant į sutartyse nustatytą informacijos saugumo reikalavimų laikymąsi.

104. Informacijos saugos įgaliotinis periodinio rizikos vertinimo metu turi įvertinti riziką, susijusią su esamais ir naujais tiekėjais ar tiekėjų paslaugų pasikeitimu ir numatyti priemones rizikai valdyti.

105. Tiekėjų atranka ir vertinimas atliekamas pagal laikantis Lietuvos Respublikos viešųjų pirkimų įstatymo, Lietuvos Respublikos valstybės informacinių išteklių įstatymo 42 punkto ir kitų teisės aktų reikalavimų.

106. Tiekėjai, kuriems sudaroma prieiga prie Mažeikių politechnikos mokyklos tvarkomų asmens duomenų, laikomi asmens duomenų tvarkytojais ir tokia prieiga gali būti suteikiama tik Mokyklai ir Tiekėjui pasirašius sutartį, reglamentuojančią Mokyklos, kaip duomenų valdytojo, ir Tiekėjo, kaip duomenų tvarkytojo, santykius.

XVIII SKYRIUS KEITIMŲ VALDYMAS

107. Turi būti užtikrinta, kad keitimai būtų valdomi. Poreikis keitimams gali iškilti dėl įvairių priežasčių, įskaitant, bet neapsiribojant žemiau išvardintomis:

107.1. naudotojų prašymai;

- 107.2. tiekėjų paslaugų pakeitimai;
- 107.3. esminiai pokyčiai Mažeikių politechnikos mokykloje;
- 107.4. techninės ir programinės įrangos atnaujinimai;
- 107.5. naujos techninės ir (ar) programinės įrangos diegimai;
- 107.6. techninės ir (ar) programinės įrangos gedimai;
- 107.7. infrastruktūros pasikeitimai;
- 107.8. nenumatyti įvykiai ir kt.

108. Atsiradus keitimo poreikiui, atsakingas už keitimą Darbuotojas registruoja keitimo datą, iniciatoriaus duomenis, siūlomą pakeitimą, pakeitimo priežastis, reikalingą pakeitimo datą.

109. Atsakingas už keitimą Darbuotojas įvertina tokio keitimo būtinumą ir galimą poveikio mastą bei suderina su informacijos saugos įgaliotiniu. Jei keitimo naudos/rizikos santykis yra teigiamas, keitimas tvirtinamas. Jei keitimas gali turėti poveikį kritiniams IT infrastruktūros vienetams, jo įgyvendinimas turi būti testuojamas, numatomi atsitraukimo planai.

110. Ištestavus keitimą, turi būti koordinuojamas jo įgyvendinimas, surenkami keitimui būtini techninės ir programinės įrangos elementai, pasiruošiama diegimui.

111. Apie keitimus, kurie gali turėti įtaką sistemos darbui, iš anksto, ne vėliau kaip prieš 1 darbo dieną, įspėjami susiję vartotojai.

112. Atliekant keitimą svarbūs sistemos pranešimai turi būti fiksuojami ir žymimi keitimo įrašė.

113. Atlikus keitimą, keitimo įrašė turi būti nurodyta keitimo atlikimo data ir, jei reikia, papildomos pastabos.

114. Po keitimo įgyvendinimo rekomenduojama kurį laiką stebėti konfigūracijos vienetus, kuriems keitimas galėjo turėti įtakos.

115. Didelių keitimų diegimui papildomai taikomos Aprašo 116–122 punktų nuostatos. Dideliais keitimais laikomi:

115.1. visi taikomųjų programų ir jų naujinimų keitimai;

115.2. kiti keitimai, kai:

115.2.1. keletas keitimų yra tarpusavyje susiję, priklauso nuo kitų konfigūracinių vienetų arba gali daryti įtaką kitų konfigūracinių vienetų funkcionavimui;

115.2.2. keitimas yra sudėtingas, jo rizika yra didelė ir reikia šią riziką sumažinti;

115.2.3. keitimas atliekamas daugelyje IT infrastruktūros elementų.

116. Administratorius, kuris koordinuos diegimo įgyvendinimą, gavęs diegimo užduotį ją užregistruoja, suformuodamas naują rinkmeną ir įrašo diegimo numerį.

117. Administratorius, kuris koordinuos diegimo įgyvendinimą, kartu su kitais Darbuotojais pagal kompetenciją, sudaro diegimo aprašą, kuriame nustatoma diegimo sąranka (diegimą sudarantys konfigūraciniai vienetai ir jų tarpusavio priklausomybė), sąrankos sukūrimo veiksmai, įvertinta diegimo gamybinėje infrastruktūroje rizika ir galimas poveikis IT paslaugoms, sąrankos priimtinumui kriterijai, numatyta diegimo strategija ir tvarkaraštis. Diegimo aprašas teikiamas tvirtinti Mažeikių politechnikos mokyklos direktoriui.

118. Pagal diegimo apraše nustatytą planą įsigyjami, sukuriama, sukonfigūruojami ir (arba) išbandomi testinėje aplinkoje visi diegimo apraše numatyti IT infrastruktūros elementai (taikomosios programos, operacinės sistemos, kompiuterinė, tinklo įranga ir kt.). Parengiami ar patikslinami eksploataavimo dokumentai. Jei reikia, papildomas ir (arba) patikslinamas diegimo aprašas.

119. Visi diegimai ir jų įgyvendinimas turi būti išbandyti testinėje aplinkoje (Mokyklos serveryje ir (arba) kompiuterinėje darbo vietoje sukuriama testinė aplinka, joje diegiama programinė įranga, jei reikia, vartotojams leidžiama prisijungti prie testinės aplinkos ir išbandyti pokyčius.)

120. Testavimas vykdomas, vadovaujantis diegimo aprašu, jame nustatyta bandymų tvarka ir priimtinumui kriterijais.

121. Mažeikių politechnikos mokyklos administratorius, remdamasis testavimo rezultatais ir įvertinta pokyčių visumos rizika, patvirtina galutinį diegimo aprašą ir autorizuoja diegimą gamybinėje aplinkoje, arba nusprendžia dėl reikalingų papildomų korekcinių veiksmy.

122. Patvirtinta sąranka diegiama gamybinėje aplinkoje (informacinių sistemų serveriuose, darbo vietų kompiuteriuose ir kitose IT infrastruktūros dalyse).

XIX SKYRIUS

ŠIFRAVIMO PRIEMONIŲ NAUDOJIMAS IR VALDYMAS

123. Šifravimo priemonių tikslas – užtikrinti tinkamą ir efektyvų šifravimo priemonių panaudojimą, kad būtų apsaugotas informacijos konfidencialumas, vientisumas ir prieinamumas.

124. Administratorius atsakingas už šifravimo priemonių parinkimą, šifravimo raktų tvarkymą ir kontrolę.

125. Šifravimo priemonės turi būti taikomos, perduodant padidinto konfidencialią informaciją elektroniniu paštu, keičiamose laikmenose, duomenų teikimo sutartyse numatytais būdais, dirbant nuotoliniu būdu. Darbuotojas, ketinantis perduoti ar tvarkyti padidinto konfidencialumo informaciją šiame punkte numatytais būdais, privalo kreiptis į Administratorių, kad šis parinktų tinkamas šifravimo priemones. Asmenų, susijusių darbo santykiais su

reguliuojamomis įmonėmis, taip pat reguliuojamų įmonių valdybos narių, akcininkų duomenys gali būti perduodami tik keičiamomis laikmenomis, jas šifruojant.

126. Saugaus elektroninės informacijos teikimo ir (arba) gavimo užtikrinimui duomenys turi būti teikiami šifruotais duomenų perdavimo kanalais, naudojant specialius protokolus.

127. Žemiau pateikiamos rekomendacijos, kuriomis reikia vadovautis, pasirenkant ar konfigūruojant šifravimo sprendimus:

127.1. Simetriniai šifrai – šifrai, naudojantys tą patį raktą duomenų šifravimui ir dešifravimui. Jį gauna duomenų siuntėjas ir gavėjas. Duomenims užšifruoti prieš siunčiant ir gautiems užšifruotiems duomenims iššifruoti naudojamas tas pats šifras (raktas). Simetriniai šifrai turi naudoti ne mažesnę nei 128 bitų raktą. Komisijos veikloje turi būti naudojami šie simetriniai šifrai:

127.1.1. Blokiniai:

127.1.1.1. AES (*Advanced Encryption Standard*). Rakto dydis 128 bitai ir daugiau;

127.1.1.2. *Triple-DES* (3DES arba TDEA). Esant galimybei turėtų būti keičiamas į AES.

127.1.2. srautiniai (kai srautas šifruojamas po vieną bitą vienu metu): *Rivest Cypher 4* (RC4) su 128 bitų raktu, jei nėra galimybės migruoti į AES blokinį šifrą.

127.2. Asimetriniai šifrai – šifrai, naudojantys šifravimui viešą ir privatų raktus. Šiame šifravimo metode generuojami du tarpusavyje susiję raktai. Jei duomenys užšifruojami vienu raktu, tai juos iššifruoti įmanoma tik kitos poros raktu. Žinant tik vieną poros raktą, neįmanoma atstatyti kito rakto.

127.2.1. Asimetriniam šifravimui gali būti naudojami šie asimetriniai šifrai;

127.2.1.1. RSA su ne trumpesniu nei 1024 bitų raktu;

127.2.1.2. ECC su 224 arba 256 bitų raktu.

127.2.2. Rekomenduojama naudoti šiuos maišos (angl. *hash*) algoritmus: 128.2.2.1. SHA – 256;

127.2.2.2. SHA – 384;

127.2.2.3. SHA – 512;

127.2.2.4. Whirlpool (10 ir daugiau etapų);

127.2.2.5. RIPEMD – 160.

127.2.3. Šifravimui negali būti naudojami šių maišų algoritmai: 128.2.3.1. SHA – 1;

127.2.3.2. MD5.

128. Visi šifravimo raktai turi būti apsaugoti nuo modifikacijų, praradimų, neautorizuoto panaudojimo ir atskleidimo.

129. Techninė įranga, naudojama raktų generavimui, saugojimui ir archyvavimui, turi būti fiziškai apsaugota.

130. Šifravimo raktai turi būti generuojami tokiu būdu, kuris nebūtų praktiškai nuspėjamas, o sugeneruoti raktai būtų sunkiai atspėjami.

131. Šiam tikslui turi būti naudojami atsitiktinių ar pseudo-atsitiktinių skaičių generatoriai.

132. Šifravimo raktai neturi būti saugomi kompiuterio atmintyje, jei kompiuteris leidžia kelių naudotojų darbą vienu metu, nebent raktai yra šifruojami.

133. Nešifruoti šifravimo raktai turi būti apsaugoti nuo atskleidimo tretiesiems asmenims.

134. Šifravimo raktų perdavimo metu turi būti užtikrinta, kad:

134.1. raktai yra perduoti tinkamiems gavėjams;

134.2. raktai gauti ir (arba) perduoti su atitinkamomis ir nepažeistomis apsaugos priemonėmis;

134.3. išlaikytas raktų integralumas.

135. Šifravimo raktai negali būti siunčiami ir saugomi toje pačioje laikmenoje, kaip ir šifruota informacija.

136. Pasibaigus naudojimo laikotarpiui šifravimo raktai turi būti sunaikinti be galimybės atstatyti.

XX SKYRIUS

INFORMACIJOS APDOROJIMO PRIEMONIŲ NAUDOJIMO STEBĖSENA

137. Informacijos apdorojimo priemonių naudojimo stebėseną vykdoma, reguliariai analizuojant žurnalinius įrašus apie naudotojų atliktus veiksmus bei IT infrastruktūros veikimą, siekiant nustatyti neteisėtus ir (ar) neleistinus naudotojų atliekamus veiksmus Komisijos IT infrastruktūroje, IT infrastruktūros gedimus, klaidas bei potencialius įsilaužimo veiksmus.

138. Vykdoma šių informacijos apdorojimo priemonių naudojimo įvykių stebėseną:

138.1. tarnybinių stočių, informacinės sistemos taikomosios programinės įrangos įjungimas, išjungimas, sėkmingi ir nesėkmingi bandymai registruotis tarnybinėse stotyse, informacinės sistemos taikomojoje programinėje įrangoje;

138.2. naudotojų atliekami veiksmai su valdomų ir (arba) tvarkomų informacinių sistemų ir registro duomenimis (įvedimas, peržiūra, keitimas, naikinimas ir kt.), naudotojų ar jų grupių bei Administratorių teisių naudotis posistemio ištekliais pasikeitimai, audito įrašų trynimai, kūrimas ar keitimas, posistemio parametrų, laiko ir (ar) datos pakeitimai;

138.3. tinklo įrangos įvykiai (analizuojamos ryšio ir tinklo priežiūros paslaugos teikėjo ataskaitos);

138.4. bandymai vykdyti kibernetines atakas (analizuojamos ryšio ir tinklo priežiūros paslaugos teikėjo ataskaitos);

138.5. Administratorių bei IT infrastruktūros priežiūrą vykdančių darbuotojų atliekami veiksmai;

138.6. Programinės įrangos, skirtos apsaugai nuo kenksmingos Programinės įrangos, įvykiai;

138.7. IT infrastruktūros darbiniai parametrai: procesoriaus apkrovimas, atminties apkrovimas, laisvos diskinės vietos kiekis, pasiekiamumas.

140.1. naudotojo/Administratoriaus ar įrenginio, susijusio su įvykiu, vardas (identifikatorius);

140.2. įvykio rūšis/pobūdis;

140.3. tikslus laikas;

140.4. trukmė;

140.5. įvykio rezultatas.

144.1. kai Darbuotojo daugiau nei 3 darbo dienas dėl nežinomos priežasties nėra darbe arba pasibaigia darbo santykiai, o būtina užtikrinti Mažeikių politechnikos mokyklos veiklos tęstinumą;

144.2. Darbuotojo ligos, mirties ar nelaimingo atsitikimo atveju, kai būtina užtikrinti Mažeikių politechnikos mokyklos veiklos tęstinumą;

144.3. kai reikia patikrinti informaciją apie Darbuotojo veiksmus, turinčius reikšmės juridinių faktų darbo, civilinės, administracinės ar baudžiamosios teisės šakose (įskaitant teisinius procesus, arbitražą ir pan.) nustatymui ir kurių patvirtinimą ar paneigimą galima įrodyti tik peržiūrint Darbuotojo siųstų arba gautų elektroninių laiškų ir jų priedų turinį;

144.4. kai Mažeikių politechnikos mokykla yra atsakinga už Darbuotojo atliktų veiksmų padarinius ir reikia ginti Mažeikių politechnikos mokyklos interesus, siekiant gauti patvirtinimą ar paneigimą dėl galimai neteisėtų Darbuotojo veiksmų;

144.5. kai Darbuotojas elektroninį paštą galimai naudoja ne tarnybos Mažeikių politechnikos mokyklos tikslais ir tai trukdo jam atlikti pareigas Mokykloje ar kenkia Mokyklos reputacijai;

144.6. kai Darbuotojo veikla galimai neatitinka etiško elgesio normų;

144.7. siekiant patikrinti, kaip Darbuotojai laikosi Mažeikių politechnikos mokyklos teisės aktuose nustatytų reikalavimų užtikrinant konfidencialios ir padidinto konfidencialumo

informacijos ir asmens duomenų apsaugą, apsaugant Mažeikių politechnikos mokyklą nuo šios informacijos neteisėto atskleidimo.

145.1. Tikrinimo komisija turi teisę peržiūrėti Darbuotojų elektroniniu paštu siųstų ir gautų elektroninių laiškų ir jų priedų turinį vienu iš 144 punkte nustatytu tikslu, tik gavusi motyvuotus rašytinius asmenų (Darbuotojų, trečiųjų asmenų ar institucijų) prašymus, kuriuose privalo būti Mažeikių politechnikos mokyklos direktoriaus rezoliucija atlikti Patikrinimą. Mažeikių politechnikos mokyklos direktorius, gavęs motyvuotą rašytinį prašymą, atsižvelgdamas į būtinumo, proporcingumo bei teisėtumo principus, rezoliucijoje nurodo, su kiek duomenų leidžiama susipažinti Tikrinimo komisijai, arba priima sprendimą neleisti susipažinti su prašomais duomenimis ir nurodo motyvus. Tikrinimo komisija apie atliktą elektroninio pašto laiškų ir priedų turinį Patikrinimą informuoja tikrintą Darbuotoją, jeigu su juo nėra pasibaigę darbo santykiai, jam pateikia patikrinimo išvadų išrašą, nurodo patikrinimo mastą, išvadas ar (ir) rekomendacijas.

145.2. Tikrinimo komisija, gavusi Mažeikių politechnikos mokyklos direktoriaus priimtą rezoliuciją leisti susipažinti su prašomais duomenimis, surenka juos ir pateikia prašomus duomenis tokią teisę turintiems asmenims tokia apimtimi, kuri reikalinga tolimesniems veiksams atlikti, kartu užtikrinant konfidencialios informacijos apsaugą. Tikrinimo komisija pateikia duomenų tik tiek, kiek nurodyta rezoliucijoje, ir baigusi vykdyti užduotį nereikalingą informaciją / duomenis sunaikina. Specializuotų prieigos teisės Tikrinimo komisijos nariams prie elektroninio pašto duomenų suteikiamos bendra prieigos suteikimo tvarka.

145.3. Tikrinimo komisija atlikdama Darbuotojų naudojamo elektroninio pašto laiškų ir jų priedų Patikrinimą turi teisę gauti Darbuotojų paaiškinimus, jeigu su Darbuotojais nėra pasibaigę darbo santykiai. Tikrinimo komisija, peržiūrėjusi elektroninio pašto laiškų ir jų priedų turinį, reikalingus duomenis naudoja tyrimui užtikrinti.

145.4. Tikrinimo komisija privalo saugoti konfidencialią ir padidinto konfidencialumo informaciją ir asmens duomenis, su kuriais susipažino atlikdami Darbuotojų elektroninio pašto laiškų ir jų priedų Patikrinimą, ir neatskleisti jų Apraše nenurodytais tikslais.

145.5. Darbuotojų elektroninio pašto duomenų srautai, susirašinėjimo turinys, įskaitant pridedamus elektroninio laiško dokumentus, kopijuojami ir saugomi 10 (dešimt) metų nuo laiškų gavimo (siuntimo) momento. Už nurodytos informacijos išsaugojimą atsakingas Mažeikių politechnikos mokyklos IT Administratorius..

145.6. Mažeikių politechnikos mokyklos išeinančių ir įeinančių elektroninio pašto laiškų gavėjai turi būti informuoti, kad Mokykloje elektroninio pašto srauto duomenys, susirašinėjimo turinys, įskaitant pridedamus elektroninio laiško dokumentus, kopijuojami ir saugomi 10 (dešimt) metų nuo laiškų gavimo ir, vadovaujantis Aprašo nustatytais pagrindais ir atvejais, gali būti atliktas elektroninio pašto laiškų ir jų priedų Patikrinimas.

XXI SKYRIUS

ĮRANGOS IR INFORMACIJOS NAIKINIMAS, TAISYMAS IR PAKARTOTINIS NAUDOJIMAS

146. Kompiuterinė įranga nurašoma bendra Mažeikių politechnikos mokyklos ilgalaikio turto nurašymo tvarka.

147. Už nurašytos Kompiuterinės įrangos utilizavimą atsakingas Mažeikių politechnikos mokyklos darbuotojas. Gavus nurašytos technikos sąrašą, Mažeikių politechnikos mokyklos darbuotojas privalo:

147.1. sutvarkyti duomenų laikmenas, t. y. mechaniškai sugadinti laikmeną arba suformatuoti, naudojant specializuotą Programinę įrangą, kuri užkirstų kelią atstatyti duomenis;

147.2. suorganizuoti Kompiuterinės įrangos išvežimą į utilizavimu užsiimančią įmonę;

147.3. pristatyti į buhalteriją pažymą apie priduoatą įrangą.

148. Nebereikalinga popierinė informacija turi būti naikinama dokumentų naikikliu, o elektroninė – programinėmis priemonėmis tokiu būdu, kad jos nebūtų galima atkurti.

149. Panaudojant Kompiuterinę įrangą pakartotinai, turi būti atliktas duomenų perrašymas.

150. Sugedusią Kompiuterinę įrangą Darbuotojai turi atiduoti atsakingam Mažeikių politechnikos mokyklos Darbuotojui, kuris rūpinasi saugiu įrangos naikinimu arba taisymu ir užtikrina, kad nebūtų galimybės neleistinai prieigai prie Kompiuterinės įrangos.

151. Atiduodant taisyti sugedusią įrangą iš jos turi būti išimamos atmintinės, kuriose gali būti svarbios informacijos.

XXII SKYRIUS

ATSARGINĖS INFORMACIJOS KOPIJOS

152. Administratorius yra atsakingas už reguliarių informacijos atsarginių kopijų darymą, užtikrinimą, kad jos būtų daromos numatytu laiku ir numatyta apimtimi, taip pat už reguliarių atsarginių kopijų atstatymo testavimą.

153. Duomenų atsarginių kopijų darymo ir valdymo principai:

153.1. atsarginės duomenų kopijos daromos automatiškai būdu;

153.2. atsarginių kopijų tipai:

153.2.1. pilna kopija – saugomi visi duomenys nuo atitinkamo laiko taško;

153.2.2. inkrementinė kopija – saugomi tik nuo pradiniu laiko momentu padarytos pilnos kopijos pakitę duomenys.

153.3. atsarginės duomenų kopijos daromos reguliariai, pagal Informacinių sistemų testinumo ir vartotojų prieigos teisių administravimo procese numatytą dažnumą;

153.4. atsarginės duomenų kopijos testuojamos reguliariai, pagal numatytus laiko intervalus;

153.5. atsarginės kopijos turi būti saugomos numatytą laikotarpį (ne mažiau kaip 12 mėn.), vėliau jas sunaikinant arba užrašant naujesnėmis kopijomis;

153.6. atsarginės kopijos saugomos šifruotu pavidalu;

153.7. realūs duomenys ir jų atsarginės kopijos saugomi atskirtose fizinėse vietose;

153.8. atsarginės kopijos turi būti apsaugotos nuo nesankcionuoto priėjimo, jų panaudojimo ar sunaikinimo;

153.9. nebenaudojamos atsarginių kopijų laikmenos turi būti saugiai išvalomos ar sunaikinamos, be galimybės atkurti jose buvusius duomenis (juostų išmagnetinimas arba fizinis sunaikinimas);

153.10. visi veiksmai (darymo, testavimo, atstatymo, pervežimo, sunaikinimo), atliekami su atsarginėmis kopijomis, turi būti fiksuojami įvykių žurnale.

154. Atsakingas už atsarginių kopijų darymą Administratorius privalo:

154.1. laikytis nustatytos atsarginių kopijų darymo tvarkos;

154.2. tikrinti duomenų vientisumą, atliekant duomenų atstatymo testavimą;

154.3. įvykus pasikeitimams, perkonfigūruoti automatiškai nustatytus įrenginius;

154.4. kartą per savaitę peržiūrėti atsarginių kopijų ir atstatymo įrašus;

154.5. kartą per metus testuoti galimybę atstatyti duomenis iš atsarginių kopijų.

155. Jeigu Administratoriaus teisės perduodamos vykdyti Tiekėjui sutartyje nustatytais pagrindais, tiekėjas turi būti supažindinamas su šiuo Aprašu tiek, kiek šis Aprašas jam taikomas arba Aprašo reikalavimai, susiję su teikiamomis paslaugomis, turi būti įtvirtinti paslaugų techninėje specifikacijoje.

XXIII SKYRIUS

BAIGIAMOSIOS NUOSTATOS

156. Informacijos saugos įgaliotinis kasmet organizuoja Darbuotojų mokymus šio Aprašo reikalavimų ir kitais informacijos saugos klausimais, nuolat jiems primena informacijos saugos reikalavimus (elektroniniu paštu, atmintinėmis ir pan.).

157. Darbuotojai, pažeidę šios tvarkos nuostatas atsako Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.

158. Visi kiti šiame Apraše nenumatyti veiksmai, susiję su Kompiuterinės ir Programinės įrangos naudojimu Mažeikių politechnikos mokykloje privalo būti derinami su Mažeikių politechnikos mokyklos direktoriumi..

159. Išimtys valdomos pagal Informacijos saugumo išimčių valdymo procedūrą.
