PATVIRTINTA
Marijampolės kolegijos direktoriaus
2021 m. rugsėjo 1 d. įsakymu Nr. 1V-114

MARIJAMPOLĖS KOLEGIJOS INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Marijampolės kolegijos informacinės sistemos duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Marijampolės kolegijos (toliau – Kolegija) informacinės sistemos (toliau – Informacinė sistema) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Informacinės sistemos elektroninės informacijos saugos politikos tikslas – užtikrinti Informacinės sistemos elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

3. Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų elektroninės informacijos saugos reikalavimų aprašas), ir Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ (toliau – Techniniai elektroninės informacijos saugos reikalavimai).

4. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

4.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

4.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

4.3. vykdyti elektroninės informacijos saugos (kibernetinių) incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos (kibernetinius) incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

5. Informacinės sistemos elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Informacinės sistemos elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė;

5.2. Informacinės sistemos elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.3. Informacinės sistemos tvarkymo kontrolė;

5.4. Informacinės sistemos paslaugų ir naudojimosi Informacinės sistemos elektronine informacija kontrolės užtikrinimas;

5.5. Informacinės sistemos tvarkomų asmens duomenų apsauga;

5.6. Informacinės sistemos veiklos tęstinumo užtikrinimas;

5.7. Informacinės sistemos naudotojų mokymas.

6. Už elektroninės informacijos saugą (kibernetinį saugumą) pagal kompetenciją atsako Informacinės sistemos valdytojas ir tvarkytojas – Kolegija.

7. Kolegija atsako už elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir politikos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą. Taip pat atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimo užtikrinimą saugos politiką įgyvendinančiuose dokumentuose (toliau – saugos dokumentai) nustatyta tvarka.

8. Saugos nuostatai taikomi Informacinės sistemos valdytojui ir tvarkytojui Kolegijai, įstaigos adresas P. Armino g. 94-2, Marijampolė, Informacinės sistemos saugos įgaliotiniui, Informacinės sistemos administratoriams, Informacinės sistemos naudotojams, Informacinei sistemai funkcionuoti reikalingų paslaugų teikėjams.

9. Kolegijos funkcijos:

9.1. organizuoti ir vadovauti informacinių sistemų veiklai;

9.2. rengti ir tvirtinti teisės aktus, susijusius su duomenų sauga, ir prižiūrėti, kaip jų laikomasi;

9.3. kontroliuoti, kad Informacinė sistema būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, Saugos nuostatais ir kitais teisės aktais;

9.4. tvirtinti Saugos nuostatus, saugos dokumentus ir kitus teisės aktus, susijusius su Informacinės sistemos elektroninės informacijos sauga (kibernetiniu saugumu) ir užtikrinti jų įgyvendinimą;

9.5. nagrinėti Informacinės sistemos tvarkytojų pasiūlymus dėl Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo ir priimti dėl jų sprendimus;

9.6. skirti Informacinės sistemos saugos įgaliotinį ir Informacinės sistemos administratorius;

9.7. užtikrinti nepertraukiamą Informacinės sistemos veiklą;

9.8. užtikrinti saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

9.9. pagal kompetenciją prižiūrėti Informacinės sistemos duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, įsilaužimų aptikimo sistemas, elektroninės informacijos perdavimo tinklus ir kitus Informacinės sistemos komponentus, užtikrinti jų veikimą;

9.10. pagal kompetenciją užtikrinti Informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą);

9.11. ne rečiau kaip kartą per metus organizuoti saugos dokumentų peržiūrėjimą ir aktualizavimą.

10. Informacinės sistemos saugos įgaliotinio funkcijos:

10.1. koordinuoti ir prižiūrėti elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimą saugos dokumentuose nustatyta tvarka;

10.2. teikti Kolegijos vadovui siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo;

10.3. atlikti Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas), nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

10.4. teikti Kolegijos vadovui siūlymus dėl Saugos nuostatų ir Informacinės sistemos saugos dokumentų priėmimo arba keitimo;

10.5. organizuoti Informacinės sistemos rizikos įvertinimą ir parengti rizikos įvertinimo ataskaitą;

10.6. supažindinti Informacinės sistemos administratorius ir Informacinės sistemos naudotojus su Saugos nuostatų ir saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą;

10.7. organizuoti Informacinės sistemos naudotojų mokymus elektroninės informacijos saugos klausimais, informuoti juos apie elektroninės informacijos saugos problemas;

10.8. duoti Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Saugos nuostatų ir saugos dokumentų įgyvendinimu;

10.9. teikti Kolegijos vadovui pasiūlymus dėl koordinuojančio Informacinės sistemos administratoriaus paskyrimo ir reikalavimų jam nustatymo;

10.10. koordinuoti elektroninės informacijos saugos (kibernetinių) incidentų tyrimą Kolegijoje ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos (kibernetinius) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetiniais) incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos (kibernetinio saugumo) darbo grupės;

10.11. teikti Informacinės sistemos administratoriams ir Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimo;

10.12. atlikti kitas Kolegijos vadovo pavestas Saugos nuostatuose ir saugos dokumentuose jam priskirtas funkcijas.

11. Informacinės sistemos administratoriaus funkcijos:

11.1. užtikrinti Informacinės sistemos techninės ir programinės įrangos įdiegimą ir funkcionavimą;

11.2. diegti ir prižiūrėti programinę įrangą, reikalingą Informacinės sistemos naudotojų funkcijoms vykdyti;

11.3. suteikti teisę Informacinės sistemos naudotojams naudotis elektronine informacija, kurios reikia jų funkcijoms atlikti;

11.4. užtikrinti Informacinės sistemos komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimo aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą, pagal kompetenciją nustatyti Informacinės sistemos pažeidžiamas vietas;

11.5. pagal kompetenciją dalyvauti vykdant saugumo reikalavimų įgyvendinimo stebėseną;

11.6. pagal kompetenciją teikti Kolegijos vadovui siūlymus dėl Informacinės sistemos palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

11.7. informuoti Informacinės sistemos saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikti siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

11.8. daryti Informacinės sistemos duomenų bazės atsargines kopijas ir atsakyti už archyve esančių kopijų saugojimą;

11.9. atlikti kitas Kolegijos vadovo ir Informacinės sistemos saugos įgaliotinio pavestas Saugos nuostatuose ir saugos dokumentuose nustatytas funkcijas.

12. Teisės aktai, kuriais vadovaujamasi tvarkant informacinių sistemų elektroninę informaciją ir užtikrinant jos saugą:

12.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

12.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

12.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

12.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

12.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

12.6. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Elektroninės informacijos svarbos nustatymo gairių aprašas);

12.7. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

12.8. Techniniai elektroninės informacijos saugos reikalavimai;

12.9. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Informacinių technologijų saugos atitikties vertinimo metodika);

12.10. Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, nustatantys saugų elektroninės informacijos tvarkymą;

12.11. Saugos nuostatai, saugos dokumentai ir kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 7–10 punktais, Informacinės sistemos tvarkoma informacija priskiriama prie mažiausios svarbos informacijos kategorijos.

14. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašo 12 punktu, Informacinė sistema priskiriama prie ketvirtosios kategorijos.

15. Informacinės sistemos saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, kasmet organizuoja Informacinės sistemos rizikos įvertinimą. Pasikeitus Informacinės sistemos duomenų bazės struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų pašalinimas ir kt.) ar po esminių organizacinių ar sisteminių pokyčių, nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis Informacinės sistemos rizikos įvertinimas. Informacinės sistemos rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu.

16. Organizuojant rizikos vertinimą turi būti paskirtas už rizikos vertinimo proceso priežiūrą ir tobulinimą atsakingas asmuo arba asmenys ir nustatyti jiems taikomi kvalifikaciniai reikalavimai. Atsakingu asmeniu gali būti skiriamas Kolegijos darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugas teikiančiu subjektu.

17. Informacinės sistemos rizikos vertinimo metu įvertinami rizikos veiksniai, galintys turėti įtakos Informacinės sistemos elektroninės informacijos saugai, jų galima žala, pasireiškimo tikimybė, galimi rizikos valdymo būdai. Svarbiausieji rizikos veiksniai:

17.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais sutrikimai, programinės įrangos klaidos, netinkamas veikimas ir kita);

17.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

17.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

18. Informacinės sistemos rizikos veiksniams vertinti naudojama dvidešimt penkių balų rizikos vertinimo sistema, pagal kurią, nustačius rizikos veiksnių tikimybę ir poveikį, apskaičiuojamas rizikos laipsnis:

18.1. rizikos laipsnis nuo 1 iki 6 – maža rizika;

18.2. rizikos laipsnis nuo 8 iki 12 – vidutinė rizika;

18.3. rizikos laipsnis nuo 15 iki 25 – didelė rizika.

19. Kuo didesnė rizikos veiksnio tikimybė ir jo poveikis, tuo rizikos laipsnis aukštesnis. Rizikos veiksniams, kuriems nustatytas aukštas rizikos laipsnis, būtina skirti didžiausią dėmesį parenkant ir įgyvendinant tinkamas rizikos mažinimo priemones.

20. Informacinės sistemos rizikos įvertinimo rezultatai ir priemonės rizikos veiksniams išvengti išdėstomi Rizikos įvertinimo ataskaitoje, kuri pateikiama Kolegijos vadovui. Rizikos veiksniai rizikos įvertinimo ataskaitoje turi būti išdėstyti pagal prioritetus ir priimtiną rizikos lygį.

21. Atsižvelgdamas į rizikos vertinimo ataskaitą, Kolegijos vadovas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

22. Siekiant įvertinti Informacinės sistemos saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per metus, jei teisės aktuose nenustatyta kitaip, organizuojamas informacinių technologijų saugos atitikties vertinimas.

23. Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Kolegijos vadovui. Pastebėtų trūkumų šalinimo planą, atsakingus jo vykdytojus paskiria ir įgyvendinimo terminus nustato taip pat Kolegijos vadovas.

24. Informacinės sistemos atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

25. Elektroninės informacijos saugos (kibernetinio saugumo) priemonės (techninės, programinės, organizacinės ir kitos informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) priemonės) parenkamos vadovaujantis šiais principais:

25.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

25.2. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei;

25.3. kur galima, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės informacijos saugos (kibernetinio saugumo) priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

26. Elektroninės informacijos saugai užtikrinti yra taikomos šios bendrosios programinės įrangos naudojimo nuostatos:

26.1. turi būti naudojama tik legali Informacinės sistemos funkcijoms vykdyti būtina programinė įranga;

26.2. programinė įranga turi būti nuolatos atnaujinama laikantis gamintojo reikalavimų;

26.3. turi būti įdiegta prieigos prie Informacinės sistemos elektroninės informacijos per registravimą, teisių suteikimą ir slaptažodžius sistema;

26.4. turi būti įgyvendinta prievolė keisti slaptažodžius ne rečiau kaip kas 180 dienų.

27. Informacinės sistemos duomenų saugai užtikrinti tarnybinėse stotyse taikomos šios programinės įrangos naudojimo nuostatos:

27.1 operacinių sistemų ir taikomųjų programų sąranka parenkama taip, kad būtų užtikrintas didžiausias saugumo lygis, sustabdomi nereikalingi darbui procesai;

27.2. ribojama ar blokuojama prieiga prie operacinės sistemos prievadų;

27.3. programinę įrangą atnaujina ir kontroliuoja administratorius. Paslaugų tiekėjai programinę įrangą gali atnaujinti tik dalyvaujant administratoriui.

28. Duomenų saugai užtikrinti informacinės sistemos naudotojų, darbuotojų darbo vietose taikomos šios programinės įrangos naudojimo nuostatos:

28.1. įdiegiama programinė įranga, skirta apsisaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.). Antivirusinės sistemos virusų parašų duomenų bazė atnaujinama automatiškai. Ilgiausias leistinas neatnaujinimo laikas – 5 darbo dienos. Kompiuterio operacinė sistemos kritinės pataisos diegiamos automatiškai. Programinę įrangą atnaujina ir kontroliuoja administratorius;

28.2. informacinės sistemos naudotojų paskyros turi būti apribotų teisių, kurios neleidžia įdiegti papildomos programinės įrangos bei keisti sistemos, kompiuterio ar programinės įrangos sisteminių nustatymų. Programinę įrangą diegia administratorius.

29. Pagrindiniai atsarginių kopijų darymo ir atkūrimo reikalavimai:

29.1. Duomenų saugai užtikrinti daromos pagrindinių duomenų atsarginės duomenų kopijos;

29.2. atsarginės kopijos daromos reguliariai, kiekvieną darbo dieną;

29.3. atsarginės kopijos turi būti daromos automatiškai. Jas atkurti turi teisę tik administratorius.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

30. Informacinės sistemos saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti elektroninės informacijos saugos (kibernetinio saugumo) srities kvalifikaciją, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą (kibernetinį saugumą). Informacinės sistemos tvarkytojas turi sudaryti sąlygas saugos įgaliotiniui kelti kvalifikaciją.

31. Informacinės sistemos saugos įgaliotiniu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

32. Informacinės sistemos administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti Informacinės sistemos komponentus (stebėti Informacinės sistemos komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti Informacinės sistemos komponentų nepertraukiamą funkcionavimą ir pan.). Informacinės sistemos administratoriai turi būti susipažinę su saugos dokumentais.

33. Informacinės sistemos naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, informacinių sistemų elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo laikyti jų paslaptį ir būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

34. Informacinės sistemos naudotojų ir Informacinės sistemos administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo periodiškumo reikalavimai:

34.1. Informacinės sistemos naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos (kibernetinio saugumo) problemas (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems informacinių sistemų naudotojams, informacinių sistemų administratoriams ir pan.);

34.2. mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), saugos įgaliotinio, Informacinės sistemos naudotojų ar informacinių sistemų administratorių poreikius;

34.3. mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kt. teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.);

34.4. mokymai Informacinės sistemos naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už mokymų organizavimą atsakingas Informacinės sistemos saugos įgaliotinis. Mokymai Informacinės sistemos saugos įgaliotiniui ir Informacinės sistemos administratoriams turi būti organizuojami pagal poreikį.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

35. Informacinės sistemos naudotojai, Informacinės sistemos administratoriai ir saugos įgaliotinis, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

36. Pakartotinai su Saugos nuostatais ir saugos dokumentais Informacinės sistemos naudotojai supažindinami jiems pasikeitus.

37. Saugos nuostatai bei kiti dokumentai, reglamentuojantys saugų elektroninės informacijos tvarkymą, skelbiami Kolegijos interneto svetainėje www.marko.lt

38. Tvarkyti Informacinės sistemos elektroninę informaciją gali tik Informacinės sistemos naudotojai, kurie yra susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų. Informacinės sistemos naudotojai atsako už Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

39. Saugos nuostatai ir saugos dokumentai iš esmės turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

_____

PATVIRTINTA
Marijampolės kolegijos direktoriaus
2021 m. rugsėjo 1 d. įsakymu Nr. 1V-114

MARIJAMPOLĖS KOLEGIJOS SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS. BENDROSIOS NUOSTATOS

1. Marijampolės kolegijos (toliau – Kolegijos) saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Taisyklės) tikslas – nustatyti tvarką, užtikrinančią saugų Kolegijos informacinių sistemų techninės, programinės įrangos funkcionavimą, saugų duomenų tvarkymą ir jų teikimą kitoms institucijoms pagal teisės aktų nustatytus reikalavimus.

2. Taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, Kolegijos direktoriaus 2021 m. rugsėjo 1 d. įsakymu Nr. 1V-114 patvirtintais Kolegijos informacinės sistemos duomenų saugos nuostatais.

3. Šios Taisyklės yra privalomos visiems Kolegijos darbuotojams, dirbantiems pagal darbo sutartį, ir Kolegijos studentams, naudojantiems kompiuterinę įrangą darbo bei mokslo užduotims atlikti.

4. Šiose Taisyklėse vartojamos sąvokos:

Kolegijos informacinės sistemos (toliau – Informacinės sistemos) – informacinių technologijų pagrindu veikiančios sistemos, užtikrinančios kompiuterizuotą Kolegijos duomenų, dokumentų ir kitos informacijos kūrimą, tvarkymą ir saugojimą, tenkinančios kitus Kolegijos informacinius poreikius. Informacines sistemas sudaro techninė įranga (tarnybinės stotys, darbo vietų kompiuteriai, duomenų saugyklos, kompiuterių tinklo ir elektroninio ryšio priemonės, duomenų apsaugos priemonės), programinė įranga (operacinės sistemos, pagalbinės programos, taikomosios programinės įrangos), kompiuterizuotai tvarkoma Kolegijos veiklos informacija (elektroniniai dokumentai, įvairūs duomenys, duomenų bazės) ir kita informacija.

Saugos įgaliotinis – Kolegijos direktoriaus paskirtas darbuotojas, dirbantis pagal darbo sutartį, įgyvendinantis elektroninės informacijos saugą Kolegijos Informacinėse sistemose.

Informacinių sistemų administratorius (toliau **–** Administratorius) – Kolegijos darbuotojas, dirbantis pagal darbo sutartį, atliekantis Informacinių sistemų priežiūrą.

Informacinių sistemų naudotojas (toliau – Naudotojas) – Kolegijos darbuotojas, dirbantis pagal darbo sutartį, ir Kolegijos studentai, turintys teisę naudotis Informacinių sistemų ištekliais numatytoms funkcijoms atlikti.

Kitos Taisyklėse vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimus, Saugos dokumentų turinio gaires ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gaires patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 ir kituose Lietuvos Respublikos teisės aktuose vartojamas sąvokas.

5. Už Informacinių sistemų duomenų saugų tvarkymą atsakingi Informacinių sistemų naudotojai, Informacinių sistemų administratorius.

6. Už Taisyklių įgyvendinimo organizavimą ir kontrolę atsakingas Saugos įgaliotinis.

II SKYRIUS. TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

7. Saugiam elektroninės informacijos tvarkymui užtikrinti naudojamos kompiuterinės įrangos, programinės įrangos, fizinės, techninės ir organizacinės duomenų saugos priemonės.

8. Prieiga prie Informacinių sistemų suteikiama tik autorizuotiems Naudotojams. Kiekvienas Naudotojas Informacinėje sistemoje turi patvirtinti savo tapatybę vardu ir slaptažodžiu. Slaptažodžiai negali būti atskleidžiami kitiems asmenims.

9. Prieiga Naudotojams suteikiama tik prie tų išteklių, kurie yra būtini tiesioginėms pareigoms vykdyti.

10. Naudojama legali sisteminė ir taikomoji programinė įranga.

11. Programinės įrangos diegimą atlieka tik Informacinių sistemų administratoriai ar kiti įgalioti asmenys.

12. Naudojamos antivirusinės programos naudotojų kompiuteriuose, antivirusinės programos elektroninio pašto tarnybinėje stotyje, programinės ugniasienės naudotojų kompiuteriuose ir tinklo tarnybinėse stotyse apsaugai nuo virusų, šnipinėjimui skirtos programinės įrangos, nepageidaujamo elektroninio pašto ir pan.

13. Siekiant apsaugoti nuo žalingos programinės įrangos, ne rečiau kaip kartą per mėnesį turi būti atliekamas nuolatinis naudotojų ir tarnybinių stočių operacinių sistemų atnaujinimas.

14. Antivirusinių programų duomenų bazės turi būti atnaujinamos periodiškai – ne rečiau kaip kartą per dieną, jei atnaujinimą pateikia antivirusinės programos gamintojas.

15. Ne rečiau kaip kartą per metus Administratorius atlieka patikrinimą, siekdamas nustatyti, ar informacinėje sistemoje naudojama legali programinė įranga. Patikrinimą inicijuoja Saugos įgaliotinis.

16. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacijų tinklų naudojant ugniasienę.

17. Už tinklo ugniasienių administravimą, priežiūrą, operacinės sistemos atnaujinimą ir saugią ugniasienių konfigūraciją atsako Administratorius.

18. Saugiam elektroninės informacijos teikimui ir (ar) gavimui iš kitų valstybės institucijų užtikrinti naudojamas Saugus valstybės duomenų perdavimo tinklas (toliau – SVDPT).

19. Naudotojams kompiuterių operacinėse sistemose turi būti suteikiamos teisės, kurios būtinos tiesioginėms pareigoms vykdyti.

20. Duomenys nuo jų praradimo, iškraipymo, sunaikinimo, neteisėto panaudojimo galimybių apsaugomi techninėmis, organizacinėmis, programinėmis priemonėmis.

21. Fizinė prieiga prie Informacinių sistemų tarnybinių stočių suteikiama tik informacinių technologijų darbuotojams.

22. Techninė įranga apsaugoma nuo elektros srovės svyravimų, nuo neteisėtos prieigos prie techninės įrangos, jos sugadinimo ar neteisėto poveikio jai. Naudojami specialūs maitinimo šaltiniai, nenutrūkstamo maitinimo šaltinis su automatine apsauga nuo įtampos svyravimų.

23. Patalpa, kurioje veikia tarnybinės stotys atitinka priešgaisrinės saugos reikalavimus, jose yra gaisro gesinimo priemonės. Periodiškai atliekama gaisro gesinimo priemonių patikra.

24. Tarnybinių stočių patalpoje įrengta oro kondicionavimo sistema.

III SKYRIUS. SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

25. Informacinių sistemų duomenų keitimą, atnaujinimą ir naujų duomenų įvedimą turi teisę atlikti tik autorizuoti naudotojai, turintys teisę tai atlikti.

26. Naudotojų tapatybė ir veiksmai su Informacinių sistemų duomenimis fiksuojami programinėmis priemonėmis.

27. Už Informacinių sistemų duomenų atsarginių duomenų kopijų darymą, saugojimą ir duomenų atkūrimą iš atsarginių duomenų kopijų atsako Administratorius.

28. Atsarginės duomenų kopijos daromos periodiškai, bet ne rečiau kaip kartą per mėnesį, o kopijos tarnybinėse stotyse – automatiniu būdu į išorinius informacijos kaupiklius.

29. Prarasti, iškraipyti ar sunaikinti Informacinių sistemų duomenys atkuriami iš atsarginių duomenų kopijų.

30. Duomenų atstatymas iš atsarginių kopijų turi būti periodiškai išbandomas – ne rečiau kaip kartą per metus.

31. Atstatymų išbandymą inicijuoja Saugos įgaliotinis.

32. Duomenų perkėlimo ir teikimo kitoms Informacinėms sistemoms bei duomenų gavimo iš jų tvarka nustatoma atskiromis sutartimis.

33. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarką, priklausomai nuo konkretaus atvejo, derina Administratorius.

34. Operacinių sistemų ir taikomosios programinės įrangos keitimai turi būti valdomi: planuojami ir ištestuojami, numatomos atstatomosios procedūros nesėkmingų keitimų atvejams, įvertinamas keitimų poveikis saugumui.

35. Už operacinių sistemų ir taikomosios programinės įrangos keitimų valdymą atsakingas Informacinių sistemų administratorius.

36. Administratorius, užtikrindamas Informacinių sistemų duomenų vientisumą, privalo naudoti visas įmanomas fizines, programines ir organizacines priemones, skirtas Informacinei sistemai ir joje tvarkomiems duomenims apsaugoti nuo neteisėtų veiksmų.

37. Naudotojas, įtaręs, kad su Informacinių sistemų duomenimis buvo atlikti neteisėti veiksmai, privalo pranešti apie tai Administratoriui. Administratorius, įtaręs, kad su Informacinių sistemų duomenimis vykdomi neteisėti veiksmai, privalo apie tai pranešti Saugos įgaliotiniui. Saugos įgaliotinis, gavęs pranešimą apie vykdomus neteisėtus veiksmus su Informacinėmis sistemomis arba su Informacinių sistemų tvarkomais duomenimis, inicijuoja elektroninės informacijos saugos incidento valdymo procedūras.

IV SKYRIUS. REIKALAVIMAI, KELIAMI INFORMACINIŲ SISTEMŲ FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

38. Administratorius suteikia prieigos prie Informacinių sistemų duomenų teisę (peržiūrėti duomenis, atlikti užklausas, vykdyti veiksmus su duomenimis ir kt.) bei fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nurodytam laikotarpiui jam nustatytoms funkcijoms atlikti.

39. Administratorius, suteikdamas prieigos prie Informacinių sistemų duomenų teisę, paslaugų teikėjo įgaliotą fizinį asmenį supažindina su prieigos prie Informacinių sistemų duomenų sąlygomis.

40. Pasibaigus sutartyje nurodytam laikotarpiui, Administratorius panaikina paslaugų teikėjo įgalioto fizinio asmens prieigos prie Informacinių sistemų duomenų teisę ir apie tai jį informuoja.

41. Reikalavimai Informacinėms sistemoms, reikalingoms paslaugų teikėjams ir jų projektavimo, aptarnavimo ir priežiūros teikiamoms paslaugoms funkcionuoti nustatomi šių paslaugų teikimo sutartyse.

42. Paslaugų teikimo sutartyse turi būti nurodoma, kad paslaugų teikėjas kuria ar modifikuoja programinę įrangą naudodamas:

42.1. įgyvendintas elektroninės informacijos saugos priemones nuo sankcionuoto poveikio sistemoms, programinei įrangai ir patalpoms;

42.2. sertifikuotą sisteminę programinę įrangą.

V SKYRIUS. BAIGIAMOSIOS NUOSTATOS

43. Naudotojas privalo kuo greičiau informuoti Saugos įgaliotinį ar Informacinių sistemų administratorių apie pastebėtus saugumo incidentus: šių Taisyklių reikalavimų pažeidimus, informacinės sistemos veiklos sutrikimus arba neįprastą sistemos veikimą.

44. Naudotojai, pažeidę šių Taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____

PATVIRTINTA
Marijampolės kolegijos direktoriaus
2021 m. rugsėjo 1 d. įsakymu Nr. 1V-114

MARIJAMPOLĖS KOLEGIJOS INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Marijampolės kolegijos (toliau – Kolegijos) informacinių sistemų naudotojų administravimo taisyklių (toliau – Taisyklės) tikslas – reglamentuoti naudotojų administravimo tvarką, prieigos prie informacinių sistemų valdymą, taip užtikrinant informacijos saugumą informacinėse sistemose.

2. Taisyklės parengtos vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, Kolegijos direktoriaus 2021 m. rugsėjo 1 d. įsakymu Nr. 1V-114 patvirtintais Kolegijos informacinės sistemos duomenų saugos nuostatais.

3. Šiose Taisyklėse vartojamos sąvokos:

Kolegijos informacinės sistemos (toliau – Informacinės sistemos) – informacinių technologijų pagrindu veikiančios sistemos, užtikrinančios kompiuterizuotą Kolegijos duomenų, dokumentų ir kitos informacijos kūrimą, tvarkymą ir saugojimą, tenkinančios kitus Kolegijos administracijos informacinius poreikius. Informacines sistemas sudaro techninė įranga (tarnybinės stotys, darbo vietų kompiuteriai, duomenų saugyklos, kompiuterių tinklo ir elektroninio ryšio priemonės, duomenų apsaugos priemonės), programinė įranga (operacinės sistemos, pagalbinės programos, standartinė taikomoji programinė įranga ir specialioji taikomoji programinė įranga), kompiuterizuotai tvarkoma Kolegijos veiklos informacija (elektroniniai dokumentai, įvairūs duomenys, duomenų bazės) ir kita informacija.

Informacinės sistemos saugos įgaliotinis (toliau **–** Saugos įgaliotinis) **–** Kolegijos direktoriaus paskirtas darbuotojas, dirbantis pagal darbo sutartį, įgyvendinantis elektroninės informacijos saugą Kolegijos informacinėse sistemose.

Informacinių sistemų administratorius (toliau **–** Administratorius) – Kolegijos darbuotojas, dirbantis pagal darbo sutartį, atliekantis Informacinių sistemų priežiūrą.

Informacinių sistemų naudotojas (toliau – Naudotojas) – Kolegijos darbuotojas, dirbantis pagal darbo sutartį, ir Kolegijos studentai, turintys teisę naudotis Informacinių sistemų ištekliais numatytoms funkcijoms atlikti.

Kitos Taisyklėse vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimus, Saugos dokumentų turinio gaires ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gaires, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 ir kituose Lietuvos Respublikos teisės aktuose vartojamas sąvokas.

4. Taisyklės taikytinos visiems Kolegijos darbuotojams ir Kolegijos studentams, kurie naudojasi Informacinėmis sistemomis ir kurių prieigos prie duomenų teisės paremtos Informacinių sistemų duomenų saugumo, stabilumo, operatyvumo principais.

5. Naudotojams prieiga prie Informacinių sistemų suteikiama vadovaujantis šiais principais:

5.1. konfidencialumu – prieigą Informacinėse sistemose saugomų duomenų gali gauti tik tie Naudotojai, kuriems tokia teisė buvo išskirtinai suteikta;

5.2. vientisumu – Informacinėse sistemose saugomus duomenis gali keisti (sukurti, ištrinti ar papildyti) tik tokius įgaliojimus turintys Naudotojai;

5.3. pasiekiamumu – Naudotojai neturi savo veiksmais sutrikdyti nepertraukiamos Informacinių sistemų veiklos, nebent tokia teisė jiems buvo išskirtinai suteikta.

II. INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. Naudotojai gali naudotis tik tomis Informacinėmis sistemomis ar jų dalimis ir jose tvarkomais duomenimis, prie kurių prieigą jiems suteikė Administratorius.

7. Naudotojai privalo užtikrinti jų naudojamų Informacinių sistemų ir jose tvarkomų duomenų konfidencialumą bei vientisumą, savo veiksmais netrikdyti duomenų prieinamumo.

8. Naudotojai privalo nedelsdami pranešti Saugos įgaliotiniui ar Administratoriui apie Informacinių sistemų sutrikimus, neįprastą jų veikimą, esamus arba galimus informacijos saugumo reikalavimų pažeidimus bei kitų Naudotojų nederamus veiksmus.

9. Administratoriaus įgaliojimai, teisės ir pareigos:

9.1. Administratorius yra įgaliotas ir turi teisę:

9.1.1. fiziškai prieiti prie techninės ir sisteminės programinės įrangos;

9.1.2. vykdyti Informacinių sistemų techninės priežiūros funkcijas;

9.1.3. matyti visų Naudotojų identifikavimo ir suteiktų teisių duomenis;

9.1.4. matyti Naudotojų su tvarkomais duomenimis atliktus veiksmus;

9.1.5. atlikti užklausas Informacinėse sistemose pagal pasirinktus paieškos kriterijus.

9.2. Administratorius privalo:

9.2.1. registruoti naujus Naudotojus;

9.2.2. tvarkyti esamų Naudotojų duomenis;

9.2.3. konsultuoti Naudotojus dėl Informacinių sistemų veikimo ir kitais su Informacinėmis sistemomis susijusiais klausimais;

9.2.4. vykdyti kitas su Informacinėmis sistemomis susijusias funkcijas;

9.2.5. pagal kompetenciją užtikrinti nepertraukiamą Informacinių sistemų techninės ir sisteminės programinės įrangos veikimą.

9.3. Administratoriaus veiksmai reglamentuoti Informacinių sistemų duomenų saugos nuostatuose ir saugos politiką įgyvendinančiuose teisės aktuose.

10. Saugos įgaliotinio įgaliojimai, teisės ir pareigos:

10.1. Saugos įgaliotinis yra įgaliotas ir turi teisę:

10.1.1. teikti Kolegijos direktoriui pasiūlymus dėl:

10.1.1.1. Administratoriaus paskyrimo;

10.1.1.2. saugos dokumentų priėmimo, keitimo ar panaikinimo;

10.1.1.3. informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo organizavimo;

10.2. teikti Administratoriui privalomus vykdyti nurodymus ir pavedimus;

10.3. Saugos įgaliotinis privalo:

10.3.1. koordinuoti elektroninės informacijos saugos incidentų, įvykusių Informacinėse sistemose, tyrimą;

10.3.2. kasmet organizuoti rizikos vertinimą, rengti apibendrintą rizikos vertinimo ataskaitą;

10.3.3. periodiškai inicijuoti Naudotojų supažindinimą informacijos saugos klausimais, informuoti juos apie informacijos saugos problematiką;

10.4. Saugos įgaliotinio veiksmai reglamentuoti Kolegijos informacinių sistemų duomenų saugos nuostatuose ir saugos politiką įgyvendinančiuose teisės aktuose.

III. INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS TVARKA

11. Saugos įgaliotinis yra atsakingas už Informacinių sistemų naudotojų supažindinimą su Kolegijos informacinių sistemų duomenų saugos nuostatais, Kolegijos informacinių sistemų saugaus duomenų tvarkymo taisyklėmis, Kolegijos informacinių sistemų veiklos tęstinumo valdymo planu, Kolegijos informacinių sistemų naudotojų administravimo taisyklėmis ir kitais saugos politiką įgyvendinančiais teisės aktais.

12. Naudotojai su Kolegijos informacinių sistemų duomenų saugos nuostatais ir saugos politiką įgyvendinančiais teisės aktais bei atsakomybe už šių dokumentų reikalavimų nesilaikymą supažindinami pasirašytinai.

13. Saugos įgaliotinis organizuoja mokymus ir seminarus duomenų saugos klausimais.

14. Saugos įgaliotinis informuoja Naudotojus elektroniniu paštu ar kitu būdu apie priimtus naujus teisės aktus ir teisės aktų pakeitimus.

IV. SAUGAUS DUOMENŲ TEIKIMO INFORMACINIŲ SISTEMŲ NAUDOTOJAMS KONTROLĖS TVARKA

15. Naudotojų registravimo ir išregistravimo tvarka:

15.1. sukurtam Naudotojui suteikiamas unikalus prisijungimo prie Informacinės sistemos vardas ir pirminis slaptažodis;

15.2. Naudotojo tapatybė nustatoma pagal naudotojo vardą ir slaptažodį arba tapatybė nustatoma naudojantis Valstybės informacinių išteklių sąveikumo platformos (VIISP) teikiamomis paslaugomis;

15.3. 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 šifruoti kanalu ar saugiu elektroninių ryšių tinklu;

15.4. gavus suteiktą vardą ir slaptažodį ir pirmą kartą prisijungęs prie Informacinės sistemos duomenų bazės, Naudotojo yra reikalaujama pirminį slaptažodį nedelsiant pakeisti nauju;

15.5. kiekvienas Naudotojas privalo naudoti tik jam suteiktą naudotojo vardą, saugoti slaptažodį ir jo neatskleisti tretiesiems (neįgaliotiems) asmenims;

15.6. Naudotojų duomenys registruojami ir kaupiami Informacinės sistemos duomenų bazėje;

16. Slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimai:

16.1. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai (didžiosios ir mažosios raidės, skaičiai, specialieji simboliai);

16.2. slaptažodžiui sudaryti neturi būti naudojama asmeninio pobūdžio informacija;

16.3. programinės įrangos vartotojo autentifikavimo dalys turi drausti automatiškai išsaugoti slaptažodžius;

16.4. nustatytas didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius (5 kartai). Neteisingai įvedus slaptažodį didžiausią leistiną skaičių, Informacinė sistema turi užsirakinti ir neleisti Naudotojui identifikuotis 15 minučių;

16.5. slaptažodis turi būti keičiamas kas 3 mėnesius. Naudotojo teisės sustabdomos, jei slaptažodis nepakeičiamas laiku;

16.6. kilus įtarimui, kad slaptažodis galėjo būti atskleistas, Naudotojas turi nedelsdamas jį pakeisti;

16.7. Naudotojui pamiršus slaptažodį, jis turi kreiptis į Administratorių arba prisijungti prie Informacinės sistemos naudojantis Valstybės informacinių išteklių sąveikumo platformos (VIISP) teikiamomis paslaugomis;

16.8. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais;

16.9. pirmojo prisijungimo prie Informacinės sistemos metu iš Naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį;

16.10. keičiant slaptažodį informacinė sistema neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių;

16.11. papildomi reikalavimai Informacinės sistemos Administratoriaus slaptažodžiams:

16.11.1. slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius;

16.11.2. slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

16.11.3. keičiant slaptažodį Informacinės sistemos taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių;

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

17. Naudotojų teisių dirbti su Informacinės sistemos duomenimis ribojimas ir / arba naikinimas:

17.1. pasibaigus darbo santykiams, Naudotojo teisė naudotis Informacine sistema panaikinama;

17.2. teisė dirbti su Informacinės sistemos duomenimis sustabdoma, kai Naudotojas nesinaudoja informacine sistema ilgiau kaip 12 mėnesių, kai įstatymų nustatytais atvejais vidinis Naudotojas nušalinamas nuo darbo (pareigų); pasibaigus darbo ir studijų santykiams, vidinio Naudotojo teisė naudotis informacine sistema panaikinama nedelsiant;

17.3. keičiantis darbuotojo pareiginėms funkcijoms turi būti peržiūrimos jo prieigos prie Informacinės sistemos duomenų teisės;

17.4. apie Naudotojo prieigos teisių dirbti su Informacinės sistemos duomenimis panaikinimą ar laikiną sustabdymą Informacinės sistemos tvarkytojo paskirtas atsakingas asmuo elektroniniu laišku informuoja Administratorių iš anksto pranešdamas naudotojo prieigos panaikinimo datą ir laiką;

17.5. turi būti patvirtinti asmenų, kuriems suteiktos administratoriaus teisės prisijungti prie Informacinės sistemos, sąrašai, periodiškai peržiūrimi saugos įgaliotinio. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais Administratorius nušalinamas nuo darbo (pareigų).

18. Nuotolinis Naudotojų prisijungimas prie Informacinės sistemos duomenų bazės leistinas per internetinę naudotojo sąsają, naudojant saugius duomenų perdavimo protokolus.

V. BAIGIAMOSIOS NUOSTATOS

19. Naudotojai, pažeidę šių Taisyklių ir kitų saugos politiką įgyvendinančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____

PATVIRTINTA
Marijampolės kolegijos direktoriaus
2021 m. rugsėjo 1 d. įsakymu Nr. 1V-114

MARIJAMPOLĖS KOLEGIJOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. BENDROSIOS NUOSTATOS

1. Marijampolės kolegijos (toliau – Kolegija) informacinių sistemų veiklos tęstinumo valdymo plano (toliau – Valdymo planas) tikslas – nustatyti Kolegijos informacinių sistemų administratoriaus, informacinių sistemų saugos įgaliotinio, informacinių sistemų naudotojų ir kitų asmenų veiksmus, esant elektroninės informacijos saugos incidentui, kurio metu iškyla pavojus informacinių sistemų duomenims, techninės, programinės įrangos funkcionavimui.

2. Valdymo planas parengtas vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716, Kolegijos direktoriaus 2021 m. rugsėjo 1 d. įsakymu Nr. 1V-114 patvirtintais Kolegijos informacinės sistemos duomenų saugos nuostatais.

3. Vartojamos sąvokos:

Kolegijos informacinės sistemos (toliau – Informacinės sistemos) – informacinių technologijų pagrindu veikiančios sistemos, užtikrinančios kompiuterizuotą Kolegijos duomenų, dokumentų ir kitos informacijos kūrimą, tvarkymą ir saugojimą, tenkinančios kitus Kolegijos informacinius poreikius. Informacines sistemas sudaro techninė įranga (tarnybinės stotys, darbo vietų kompiuteriai, duomenų saugyklos, kompiuterių tinklo ir elektroninio ryšio priemonės, duomenų apsaugos priemonės), programinė įranga (operacinės sistemos, pagalbinės programos, taikomosios programinės įrangos), kompiuterizuotai tvarkoma Kolegijos veiklos informacija (elektroniniai dokumentai, įvairūs duomenys, duomenų bazės) ir kita informacija.

Informacinių sistemų saugos įgaliotinis (toliau – Saugos įgaliotinis) **–** Kolegijos direktoriaus paskirtas darbuotojas, dirbantis pagal darbo sutartį, įgyvendinantis elektroninės informacijos saugą Kolegijos Informacinėse sistemose.

Informacinių sistemų administratorius (toliau **–** Administratorius) – Kolegijos darbuotojas, dirbantis pagal darbo sutartį, atliekantis Informacinių sistemų ir jų infrastuktūros priežiūrą.

Informacinių sistemų naudotojas (toliau – Naudotojas) – Kolegijos darbuotojas, dirbantis pagal darbo sutartį, ir Kolegijos studentai, turintys teisę naudotis Informacinių sistemų ištekliais numatytoms funkcijoms atlikti.

Kitos Valdymo plane vartojamos sąvokos atitinka Bendrųjų elektroninės informacijos saugos reikalavimus, Saugos dokumentų turinio gaires ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gaires, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 ir kituose Lietuvos Respublikos teisės aktuose vartojamas sąvokas.

4. Valdymo planas įsigalioja įvykus elektroninės informacijos saugos incidentui, jo vykdymas yra privalomas elektroninės informacijos saugos incidentų atveju, kurių metu gali kilti pavojus Informacinių sistemų duomenims, Informacinių sistemų techninės, programinės įrangos funkcionavimui. Informacinių sistemų tvarkytojo padalinių vadovų, Saugos įgaliotinio,

Administratoriaus ir Naudotojų veiksmai yra nurodyti Kolegijos Informacinių sistemų veiklos tęstinumo valdymo detaliajame plane (1 priedas).

5. Už Valdymo plano įgyvendinimo organizavimą atsakingas Saugos įgaliotinis.

6. Už Valdymo plano įgyvendinimą atsakingi Informacinių sistemų tvarkytojo padalinių vadovai, Administratorius, Naudotojai.

7. Elektroninės informacijos saugos incidento metu patirti nuostoliai padengiami iš Kolegijos biudžeto ir kitų finansavimo šaltinių.

8. Kriterijai, pagal kuriuos nustatoma, kad Informacinės sistemos veikla yra atkurta:

8.1. Informacinės sistemos duomenų atnaujinimas;

8.2. Informacinės sistemos duomenų išsaugojimas.

II. ORGANIZACINĖS NUOSTATOS

9. Veiklos tęstinumo valdymo grupės sudėtis:

9.1. grupės vadovas – Kolegijos (toliau – KD) direktorius;

9.2. grupės vadovo pavaduotojas – KD pavaduotojas akademinei ir mokslo taikomajai veiklai;

9.3. grupės nariai:

9.3.1. Teisės, personalo ir viešųjų pirkimų skyriaus vadovas;

9.3.2. Verslo ir technologijų fakulteto dekanas;

9.3.3. Edukologijos ir socialinio darbo fakulteto dekanas;

9.3.4. Informacinės sistemos saugos įgaliotinis.

10. Veiklos tęstinumo valdymo grupės funkcijos:

10.1. analizuoti elektroninės informacijos saugos incidentus ir priimti sprendimus Informacinės sistemos veiklos tęstinumo valdymo klausimais;

10.2. bendrauti su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

10.3. bendrauti su kitų Informacinių sistemų veiklos tęstinumo valdymo grupėmis;

10.4. bendrauti su teisėsaugos ir kitomis institucijomis, atsakingomis už nacionalinį elektroninių ryšių tinklų ir informacijos saugumą;

10.5. kontroliuoti finansinių ir kitų išteklių, reikalingų Informacinės sistemos veiklai atkurti įvykus elektroninės informacijos saugos incidentui, naudojimą;

10.6. užtikrinti elektroninės informacijos fizinę saugą įvykus saugos incidentui;

10.7. organizuoti darbuotojų, daiktų, įrangos gabenimą;

10.8. vykdyti Informacinių sistemų veiklos atkūrimo priežiūrą ir koordinuoti veiklos atkūrimo veiksmus.

10.9. vykdyti kitas Veiklos tęstinumo valdymo grupei pavestas funkcijas.

11. Veiklos atkūrimo grupės sudėtis:

11.1. grupės vadovas – Kolegijos direktoriaus pavaduotojas akademinei ir mokslo taikomajai veiklai;

11.2. grupės vadovo pavaduotojas – Teisės, personalo ir viešųjų pirkimų skyriaus vadovas;

11.3. grupės nariai:

11.3.1. Informacinės sistemos administratorius;

11.3.2. Informacinės sistemos saugos įgaliotinis;

11.3.3. Dokumentų valdymo tarnybos administratorius.

12. Veiklos atkūrimo grupės funkcijos:

12.1. organizuoti Informacinių sistemų tarnybinių stočių veikimo atkūrimą;

12.2. organizuoti kompiuterių tinklo veikimo atkūrimą;

12.3. organizuoti Informacinių sistemų elektroninės informacijos atkūrimą;

12.4. organizuoti taikomųjų programų tinkamo veikimo atkūrimą;

12.5. organizuoti darbo kompiuterių veikimo atkūrimą ir prijungimą prie kompiuterių tinklo;

12.6. vykdyti kitas veiklos atkūrimo grupei pavestas funkcijas.

13. Įvykus elektroninės informacijos saugos incidentui patalpose, kuriose yra saugoma Informacinių sistemų techninė ir programinė įranga:

13.1. Informacinės sistemos administratorius nedelsdamas informuoja apie nenumatytą situaciją Saugos įgaliotinį;

13.2. Saugos įgaliotinis apie elektroninės informacijos saugos incidentą nedelsdamas informuoja Informacinės sistemos naudotojo padalinio vadovą;

13.3. Saugos įgaliotinis informaciją įrašo į Elektroninės informacijos saugos incidentų registravimo žurnalą (2 priedas), vadovauja veiklos tęstinumo detaliajame Marijampolės kolegijos informacinių sistemų veiklos tęstinumo valdymo plane (1 priedas) nurodytiems veiksmams;

13.4. Informacinės sistemos administratorius atkuria tarnybinės stoties, kompiuterių tinklo veiklą, duomenis, techninės, sisteminės ir taikomosios programinės įrangos funkcionavimą ir apie tai informuoja Informacinės sistemos naudotojo padalinio vadovą bei Saugos įgaliotinį;

13.5. Saugos įgaliotinis kartu su Administratoriumi organizuoja žalos Informacinės sistemos duomenims, techninei bei programinei įrangai vertinimą, koordinuoja Informacinės sistemos veiklai atkurti reikalingos techninės, sisteminės ir taikomosios programinės įrangos įsigijimą.

14. Kolegijos darbuotojų telefonų numeriai, jų elektroninio pašto adresai nuolat atnaujinami Kolegijos interneto svetainėje www.marko.lt.

15. Elektroninės informacijos saugos incidento metu sunaikinta techninė, sisteminė ir taikomoji programinė įranga įsigyjama Viešųjų pirkimų įstatymo nustatyta tvarka, panaudojant Kolegijos biudžeto išteklius ar kitus finansavimo šaltinius.

16. Įvykus nenumatytai situacijai Informacinių sistemų patalpose, jų veiklai atkurti naudojamoms patalpoms taikomi Kolegijos saugaus elektroninės informacijos tvarkymo taisyklėse nurodyti reikalavimai.

III. APRAŠOMOSIOS NUOSTATOS

17. Kolegijos informacinių technologijų darbuotojai saugo:

17.1. dokumentą, kuriame nurodyti kiekvieno pastato, kuriame yra informacinės sistemos įranga, aukšto patalpų brėžiniai ir juose pažymėti kompiuterių tinklo ir telefonų tinklo mazgai bei kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos;

17.2. dokumentą, kuriame nurodytos kompiuterių tinklo fizinio ar loginio sujungimo schemos;

17.3. dokumentą, kuriame nurodyti techninės ir programinės įrangos sąrašai;

17.4. Informacinių sistemų programinės įrangos sukūrimo, priežiūros ir modernizavimo, kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių kopijas;

17.5. Informacinių sistemų atsarginių duomenų kopijas. Programinės įrangos laikmenas ir laikmenas su atsarginėmis duomenų kopijomis.

18. Už Informacinių sistemų techninės ir programinės įrangos priežiūrą yra atsakingas Administratorius.

19. Už Informacinių sistemų atsarginių duomenų kopijų darymą, saugojimą, duomenų iš atsarginių kopijų atkūrimą atsakingas Administratorius.

IV. PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

20. Kolegijos Informacinių sistemų duomenų saugos įgaliotinis, per kalendorinius metus įvertinęs Informacinių sistemų naudotojų padaliniuose rizikos veiksnių galimybes, išnagrinėjęs Kolegijos Informacinių sistemų nenumatytų situacijų registravimo žurnale padarytus įrašus, kartą per metus (sausio mėn.) rengia Kolegijos Informacinių sistemų rizikos ataskaitą. Ataskaitą tvirtina Kolegijos direktorius.

21. Plano veiksmingumo išbandymo dieną imituojamas Elektroninės informacijos saugos incidentas. Jo metu už elektroninės informacijos saugos incidento padarinių likvidavimą atsakingi asmenys atlieka minėtų padarinių likvidavimo veiksmus.

22. Saugos įgaliotinis atsakingas už išbandymo metu Plano veiksmingumo pastebėtų trūkumų parengimą ir pateikimą Kolegijos direktoriui.

23. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

_____

Marijampolės kolegijos informacinių sistemų
veiklos tęstinumo valdymo plano
1 priedas

MARIJAMPOLĖS KOLEGIJOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO DETALUSIS PLANAS

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmių likvidavimo veiksmai	Pasekmių likvidavimo atsakingi vykdytojai
1. Oro sąlygos	1.1. Elektroninės informacijos saugos incidento pasekmės įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas	1.1.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Veiklos atkūrimo grupė
		1.1.2. Pavojaus sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas ir paskelbimas	Veiklos tęstinumo valdymo grupė
		1.1.3. Priemonių plano įgyvendinimas	Veiklos atkūrimo grupė
	1.2. Darbuotojų elektroninės informacijos saugos incidento pasekmei likviduoti paskyrimas	1.2.1. Žalą likviduojančių darbuotojų apmokymas	Veiklos atkūrimo grupė
		1.2.2. Žalą likviduojančių darbuotojų veiksmų koordinavimas	Veiklos tęstinumo valdymo grupė
	1.3. Oro prognozės sekimas	1.3.1. Žalą likviduojančių darbuotojų instruktavimas	Veiklos atkūrimo grupė
	1.4. Dirbantiesiems pavojaus vietoje rekomendacijų teikimas	1.4.1. Elektroninės informacijos saugos incidento pasekmes likviduojančių darbuotojų apmokymas	Veiklos atkūrimo grupė
		1.4.2. Darbuotojų informavimas apie elgseną pavojaus vietoje	Veiklos tęstinumo valdymo grupė
		1.4.3. Pirmosios pagalbos suteikimo organizavimas nukentėjusiems darbuotojams	Veiklos tęstinumo valdymo grupė
		1.4.4. Nukentėjusių darbuotojų gabenimo į gydymo įstaigą organizavimas	Veiklos tęstinumo valdymo grupė
	1.5. Pavojaus vietų ženklinimas	1.5.1. Darbuotojų informavimas	Veiklos tęstinumo valdymo grupė
		1.5.2. Žalą likviduojančių darbuotojų apmokymas	IS saugos įgaliotinis
2. Gaisras	2.1. Ugniagesių tarnybos informavimas	2.1.1. Įvykio vietos lokalizavimas, jei gauta rekomendacija	Veiklos tęstinumo valdymo grupė

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmių likvidavimo veiksmai	Pasekmių likvidavimo atsakingi vykdytojai
		2.1.2. Galimybių evakuoti darbuotojus paieška, jei yra rekomenduojama tai padaryti	Veiklos tęstinumo valdymo grupė
	2.2. Darbuotojų evakavimas (pagal ugniagesių tarnybos rekomendaciją)	2.2.1. Darbuotojų informavimas apie evakavimą, jei yra rekomendacija	Veiklos tęstinumo valdymo grupė
	2.3. Darbas pavojaus zonoje	2.3.1. Darbuotojų informavimas apie saugų darbą pavojaus zonoje	Veiklos tęstinumo valdymo grupė
	2.4. Komunikacijų, sukeliančių pavojų, išjungimas. Gaisro gesinimas ankstyvoje stadijoje, jei yra rekomendacija dirbti pavojaus zonoje	2.4.1. Ugniagesių tarnybos nurodymų vykdymas	Veiklos atkūrimo grupė
3. Patalpų užgrobimas	3.1.Teisėsaugos tarnybos informavimas	3.1.1. Įvykio vietos lokalizavimas, jei yra teisėsaugos tarnybos rekomendacijos	Veiklos tęstinumo valdymo grupė
		3.1.2. Galimybių evakuoti darbuotojus nagrinėjimas, jei gauta rekomendacija	Veiklos tęstinumo valdymo grupė
	3.2. Darbuotojų evakavimas, jei yra rekomendacija	3.2.1. Darbuotojų informavimas apie evakavimą	Veiklos tęstinumo valdymo grupė
	3.3. Patalpų užrakinimas, jei yra galimybė	3.3.1. Teisėsaugos tarnybos nurodymų vykdymas	IS naudotojų padalinio vadovas
	3.4. Teisėsaugos tarnybos nurodymų vykdymas, jei yra rekomendacija	3.4.1. Darbuotojų informavimas apie nurodymų vykdymą	Veiklos tęstinumo valdymo grupė
	3.5. Veiksmai išlaisvinus užgrobtas patalpas	3.5.1. Padarytos žalos įvertinimas	Veiklos atkūrimo grupė
		3.5.2. Padarytos žalos likvidavimo priemonių plano sudarymas, paskelbimas, vykdymas	Veiklos atkūrimo grupė
		3.5.3. Žalą likviduojančių darbuotojų apmokymas	Veiklos atkūrimo grupė
4. Patalpai padaryta žala		4.1.1. Rekomendacijų iš suinteresuotos tarnybos gavimas apie galimybę dirbti pavojaus zonoje	Veiklos tęstinumo valdymo grupė

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmių likvidavimo veiksmai	Pasekmių likvidavimo atsakingi vykdytojai
arba patalpos praradimas	4.1. Atitinkamos tarnybos informavimas apie pavojaus pobūdį	4.1.2. Darbuotojų informavimas apie rekomendacijas	Veiklos tęstinumo valdymo grupė
	4.2. Atsarginių patalpų įrengimas	4.2.1. Darbuotojų informavimas apie darbą patalpose	Veiklos tęstinumo valdymo grupė
5. Energijos tiekimo sutrikimai	5.1. Energijos tiekimo sutrikimo priežasčių nustatymas. Tarnybinės stoties, kitos techninės įrangos energijos maitinimo išjungimas	5.1.1. Sutrikimų šalinimo organizavimas	Veiklos tęstinumo valdymo grupė
	5.2. Kreipimasis į energijos tiekimo tarnybą dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių	5.2.1. Rekomendacijų iš energijos tiekimo tarnybos gavimas	Veiklos tęstinumo valdymo grupė
	5.3. Sutrikimų pašalinimas	5.3.1. Pavojaus sustabdymas, padarytos žalos likvidavimo priemonių plano sudarymas ir įgyvendinimas	Veiklos atkūrimo grupė
		5.3.2. Padarytos žalos įvertinimas	
		5.3.3. Žalą likviduojančių darbuotojų apmokymas	Veiklos atkūrimo grupė
6. Vandentiekio ir šildymo sistemos sutrikimai	6.1. Vandentiekio ar šildymo paslaugų teikėjų informavimas	6.1.1. Atitinkamos tarnybos paklausimas dėl leidimo dirbti ir rekomendacijų gavimas	Veiklos tęstinumo valdymo grupė
		6.1.2. Darbuotojų informavimas apie rekomendacijas	Veiklos tęstinumo valdymo grupė
	6.2. Sutrikimo šalinimo prognozės skelbimas, sutrikimo pašalinimas	6.2.1. Padarytos žalos įvertinimas. Sutrikimo sustabdymo ir padarytos žalos likvidavimo priemonių plano sudarymas, plano įgyvendinimas	Veiklos atkūrimo grupė
		6.2.2. Žalą likviduojančių darbuotojų apmokymas	Veiklos atkūrimo grupė
7. Ryšio sutrikimai	7.1. Ryšio sutrikimo priežasčių nustatymas	7.1.1. Kreiptis į ryšio paslaugos teikėją	Veiklos tęstinumo valdymo grupė

Pavojaus rūšys	Pirmaeiliai veiksmai	Pasekmių likvidavimo veiksmai	Pasekmių likvidavimo atsakingi vykdytojai
	7.2. Ryšio tarnybų informavimas, paklausimo dėl sutrikimo trukmės ir pašalinimo prognozės	7.1.2. Nustatyti ir įgyvendinti priemones, kad sutrikimai nesikartotų	
	7.3. Sutrikimo pašalinimas	7.1.3. Kreiptis į kitą ryšio paslaugos teikėją, jei sutrikimas nepašalintas	Veiklos tęstinumo valdymo grupė
8. Tarnybinės stoties, komutacinės įrangos sugadinimas	8.1. Pranešti teisėsaugos tarnybai, draudimo bendrovei apie įvykį	8.1.1. Darbuotojų elektroninės informacijos saugos incidento pasekmei likviduoti paskyrimas, apmokymas, jų veiksmų nustatymas	Veiklos tęstinumo valdymo grupė
	8.2. Elektroninės informacijos saugos incidento pasekmių šalinimas	8.2.1. Kreiptis į įrangos tiekėjus dėl įrangos remonto ar naujos įrangos įsigijimo	Veiklos atkūrimo grupė
		8.2.2. Įsigytos įrangos diegimas	Veiklos atkūrimo grupė
9. Programinės įrangos sugadinimas, praradimas	9.1. Elektroninės informacijos saugos incidento pasekmių įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas	9.1.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Veiklos atkūrimo grupė
		9.1.2. Priemonių plano sudarymas, paskelbimas ir įgyvendinimas	Veiklos tęstinumo valdymo grupė
	9.2. Darbuotojų elektroninės informacijos saugos incidento pasekmėms likviduoti paskyrimas. Žalą likviduojančių darbuotojų instruktavimas, jų veiksmų koordinavimas	9.2.1. Žalą likviduojančių darbuotojų apmokymas	
		9.2.2. Kreipimasis į teisėsaugos tarnybas dėl programinės įrangos sugadinimo ar praradimo ir jų nurodymų vykdymas	Veiklos tęstinumo valdymo grupė
10. Dokumentų praradimas	10.1. Elektroninės informacijos saugos incidento pasekmių įvertinimas	10.1.1. Prarastų dokumentų atkūrimas	Veiklos atkūrimo grupė
		10.1.2. Prarastų dokumentų atkūrimo kontrolė	Veiklos tęstinumo valdymo grupė
11. Darbuotojų praradimas	11.1. Elektroninės informacijos saugos incidento pasekmių įvertinimas	11.1.1. Trūkstamų darbuotojų paieška ir priėmimas į darbą	Veiklos tęstinumo valdymo grupė

Marijampolės kolegijos informacinių sistemų
veiklos tęstinumo valdymo plano
2 priedas

MARIJAMPOLĖS KOLEGIJOS INFORMACINIŲ SISTEMŲ ELEKTRONINĖS INFORMACIJOS SAUGOS INCIDENTŲ REGISTRAVIMO ŽURNALAS

Pildymo pradžia 20___m._____d.

Eil. Nr.	**Elektroninės informacijos saugos incidentas**						
	IS naudotojo padalinio pavadinimas	**Požymio kodas**	**Įvykio aprašymas**	**Pradžia (metai, mėnuo, diena, valanda)**	**Pabaiga (metai, mėnuo, diena, valanda)**	**Pašalino (vardas, pavardė)**	**Saugos įgaliotinis (vardas, pavardė, parašas)**
1.							
2.							
3.							
4.							
5.							
6.							

Elektroninės informacijos saugos incidento situacijos požymiai:
1. Oro sąlygos. 2. Gaisras. 3. Patalpų užgrobimas. 4. Patalpai padaryta žala arba patalpos praradimas. 5. Energijos tiekimo sutrikimai. 6. Vandentiekio ir šildymo sistemos sutrikimai; 7. Ryšio sutrikimai. 8. Tarnybinės stoties, komutacinės įrangos sugadinimas, praradimas. 9. Programinės įrangos sugadinimas, praradimas. 10. Duomenų pakeitimas, sunaikinimas, atskleidimas, dokumentų praradimas. 11. Darbuotojų praradimas.

_____