PATVIRTINTA
Kauno maisto pramonės ir prekybos
mokymo centro direktoriaus
2026 m. balandžio 23 d. įsk. Nr. V-144

KAUNO MAISTO PRAMONĖS IR PREKYBOS MOKYMO CENTRO INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKA

I. BENDROSIOS NUOSTATOS

1. Informacijos ir kibernetinio saugumo politika (toliau – Politika) apibrėžia Kauno maisto pramonės ir prekybos mokymo centro (toliau – Centras) poziciją ir atsakomybę informacijos ir kibernetinio saugumo srityje bei yra skirta nustatyti vieningus saugumo valdymo principus ir užtikrinti efektyvų Centro informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą, atsižvelgiant į Centre vykdomą bendrąjį ugdymą ir profesinį mokymą**.**

II. POLITIKOS TAIKYMO SRITIS

2. Ši Politika privaloma visiems Centro darbuotojams, taip pat tiekėjams, rangovams ir kitiems asmenims, turintiems ar galintiems turėti prieigą prie Centro informacinių išteklių.
3. Politika taikoma visoms Centro valdomoms, naudojamoms ar prižiūrimoms informacinėms sistemoms, informaciniams ištekliams ir su jais susijusiems procesams, nepriklausomai nuo jų formos ar laikmenos, įskaitant informacijos kūrimą, tvarkymą, saugojimą, perdavimą ir naikinimą.

III. TEISINIS PAGRINDAS

4. Politika parengta vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatymu, kuris nustato kibernetinio saugumo principus, kibernetinio saugumo politikos formavimo ir įgyvendinimo institucijas, jų įgaliojimus kibernetinio saugumo srityje, kibernetinio saugumo subjektų pareigas bei tarpinstitucinį bendradarbiavimą, taip pat kitais kibernetinį saugumą reglamentuojančiais teisės aktais, įskaitant Kibernetinio saugumo reikalavimų aprašą ir Nacionalinį kibernetinių incidentų valdymo planą.
5. Centro kibernetinio saugumo rizikų valdymas vykdomas vadovaujantis patvirtintu Rizikos veiksnių vertinimo ir valdymo žemėlapiu. Rizikų žemėlapis yra reguliariai peržiūrimas ir atnaujinamas.

IV. SĄVOKOS IR APIBRĖŽTYS

6. **Informacija** – bet kokie duomenys ar žinios, pateikti forma, tinkama naudoti, saugoti, perduoti ar apdoroti. Informacija gali būti žodinė, rašytinė, audiovizualinė, skaitmeninė ar kitokia forma išreikšti duomenys.
7. **Informacijos saugumas** – informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas. Prireikus gali būti taikomi ir papildomi kriterijai, tokie kaip autentiškumas, atsekamumas, nepaneigiamumas ir privatumas.
8. **Informacinė aplinka** – naudotojų, organizacijų, informacinių sistemų ir pačios informacijos visuma, kurioje informacija yra kuriama, tvarkoma ar perduodama.

9. **Informacinė sistema** – tarpusavyje susijusių techninių, programinių, organizacinių priemonių ir procesų visuma, skirta informacijai rinkti, saugoti, apdoroti ir teikti naudotojams.
10. **Informaciniai ištekliai** – Centro valdoma ar naudojama informacija, informacinės sistemos, programinė įranga, techninė įranga, duomenų laikmenos, ryšių priemonės, taip pat su jomis susijusios paslaugos ir žmogiškieji ištekliai.
11. **Išorės šalys** – paslaugų teikėjai, partneriai, praktikų vietos, tiekėjai ir kiti asmenys, turintys ar galintys turėti prieigą prie Centro informacinių išteklių.
12. **Kibernetinė erdvė** – aplinka, kurią sudaro informacinių technologijų ir ryšių įranga bei joje kuriama, apdorojama ir perduodama elektroninė informacija.
13. **Kibernetinis saugumas** – teisinių, organizacinių ir techninių priemonių visuma, skirta užtikrinti informacinių sistemų ir jose tvarkomos informacijos konfidencialumą, vientisumą, prieinamumą ir atsparumą kibernetinėms grėsmėms, taip pat atkurti sistemų veiklą po incidentų.
14. **Konfidencialumas** – užtikrinimas, kad informacija prieinama tik įgaliotiems asmenims, kuriems ji reikalinga jų funkcijoms vykdyti.
15. **Vientisumas** – užtikrinimas, kad informacija yra tiksli, nepažeista ir nepakeista neteisėtu ar atsitiktiniu būdu.
16. **Prieinamumas** – užtikrinimas, kad informacija ir informacinės sistemos yra prieinamos įgaliotiems naudotojams, kai jų reikia.

V. INFORMACIJOS IR KIBERNETINIO SAUGUMO TIKSLAI

17. Užtikrinti saugią ir patikimą Centro informacinę ir kibernetinę aplinką.
18. Užtikrinti informacijos saugumą, garantuojant informacijos konfidencialumą, vientisumą ir prieinamumą.
19. Užtikrinti Centro veiklos tęstinumą, garantuojant informacinių sistemų, ryšių tinklų, mokymo ir praktinio mokymo procese naudojamos įrangos bei programinės įrangos nepertraukiamą veiklą.
20. Įgyvendinti organizacines ir technines priemones, skirtas kibernetinių grėsmių prevencijai, nustatymui ir valdymui, užtikrinant saugų ir patogų informacinių sistemų naudojimą.
21. Užtikrinti atitiktį informacijos saugumo, kibernetinio saugumo ir asmens duomenų apsaugos reikalavimus nustatantiems teisės aktams bei jų įgyvendinimą Centro veikloje.

VI. INFORMACIJOS IR KIBERNETINIO SAUGUMO VALDYMO PRINCIPAI

22. Centras, siekdamas užtikrinti informacijos ir kibernetinį saugumą, vadovaujasi šiais principais:
    22.1. **Saugumo kultūros užtikrinimas -** Centre užtikrinamas nuoseklus informacijos ir kibernetinio saugumo kultūros formavimas ir palaikymas. Darbuotojai ir mokiniai yra informuojami apie kibernetines grėsmes, jų poveikį Centro veiklai bei mokomi taikyti saugaus elgesio praktikas, siekiant mažinti žmogiškųjų klaidų ir incidentų riziką.
    22.2. **Atitiktis teisės aktams -** užtikrinama atitiktis informacijos ir kibernetinį saugumą reglamentuojantiems teisės aktams, taip pat sutartiniams įsipareigojimams su trečiosiomis šalimis, taikant rizikos vertinimu pagrįstas organizacines ir technines saugumo priemones.
    22.3. **Incidentų ir pažeidžiamumų valdymas -** užtikrinamas sistemingas kibernetinių incidentų ir pažeidžiamumų nustatymas, registravimas, valdymas ir analizė, siekiant operatyviai reaguoti į grėsmes, mažinti jų poveikį ir užkirsti kelią pasikartojimui.

22.4. **Prieigos kontrolė ir mažiausios privilegijos principas -** prieiga prie informacijos ir informacinių sistemų suteikiama tik tiems asmenims, kuriems ji būtina jų funkcijoms vykdyti, užtikrinant mažiausios būtinos prieigos teises.
22.5. **Atsakomybės ir atskaitomybės principas -** kiekvienas Centro darbuotojas ir kitas asmuo, turintis prieigą prie informacinių išteklių, yra atsakingas už saugų jų naudojimą, o visi veiksmai informacinėse sistemose turi būti identifikuojami ir, kai taikoma, registruojami.
22.6. **Nuolatinio tobulinimo principas -** informacijos ir kibernetinio saugumo valdymas Centre yra nuolat peržiūrimas ir tobulinamas, atsižvelgiant į kintančias grėsmes, technologinę aplinką ir teisės aktų reikalavimus.

VII. CENTRO ĮSIPAREIGOJIMAI

23. Siekdamas įgyvendinti nustatytus informacijos ir kibernetinio saugumo valdymo principus, Centras įsipareigoja:
23.1. **Užtikrinti atitiktį teisės aktams -** laikytis visų informacijos ir kibernetinio saugumo reikalavimų, nustatytų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartiniuose įsipareigojimuose, taip pat užtikrinti nuolatinį informacijos saugumo valdymo sistemos veiksmingumo vertinimą ir tobulinimą.
23.2. **Vykdyti kibernetinių grėsmių prevenciją -** diegti ir taikyti organizacines ir technines priemones, skirtas kibernetinių incidentų prevencijai, bei užtikrinti darbuotojų ir mokinių informacijos saugumo kultūros ir kibernetinės higienos ugdymą.
23.3. **Užtikrinti išteklių pakankamumą -** skirti reikiamus žmogiškuosius, techninius ir organizacinius išteklius informacijos saugumo valdymo sistemai įgyvendinti ir palaikyti.
23.4. **Užtikrinti duomenų atsarginių kopijų sudarymą ir atkūrimą -** užtikrinti, kad Centro informacinėse sistemose tvarkomiems duomenims būtų reguliariai daromos atsarginės kopijos, jos saugiai laikomos ir periodiškai tikrinamas ir testuojamas duomenų atkūrimo veiksmingumas.
23.5. **Organizuoti mokymus ir kompetencijų ugdymą -** sudaryti sąlygas darbuotojams tobulinti žinias informacijos ir kibernetinio saugumo bei asmens duomenų apsaugos srityse.
23.6. **Užtikrinti incidentų valdymą ir bendradarbiavimą -** užtikrinti savalaikį kibernetinių incidentų nustatymą, registravimą ir valdymą bei, esant poreikiui, bendradarbiauti su kompetentingomis institucijomis, įskaitant Nacionalinį kibernetinio saugumo centrą.

VIII. POLITIKOS PERŽIŪROS IR SKLAIDOS TVARKA

24. Politika tvirtinama, keičiama ar naikinama Centro direktoriaus įsakymu. Politiką rengia, peržiūri ir prireikus atnaujina Centro informacinių technologijų (IT) specialistas ar kitas direktoriaus įsakymu paskirtas atsakingas asmuo.
25. Politika yra skelbiama Centro interneto svetainėje ir prieinama visoms suinteresuotoms šalims.
26. Politika peržiūrima ne rečiau kaip kartą per metus arba pasikeitus teisės aktams, technologinei aplinkai ar įvykus reikšmingiems kibernetiniams incidentams.
27. Politikos nuostatos įgyvendinamos priimant Centro vidaus teisės aktus, procedūras ir kitus dokumentus, atitinkančius Centro veiklos pobūdį, strateginius tikslus, teisės aktų reikalavimus bei gerąją informacijos ir kibernetinio saugumo praktiką.

28. Politikos nuostatos detalizuojamos šios Politikos 1 priede „Kibernetinio saugumo rizikos ir jų valdymo priemonės“.

Kauno maisto pramonės ir prekybos
mokymo centro informacijos
ir kibernetinio saugumo politikos
1 Priedas

KAUNO MAISTO PRAMONĖS IR PREKYBOS MOKYMO CENTRO KIBERNETINIO SAUGUMO RIZIKOS IR JŲ VALDYMO PRIEMONĖS

Kibernetinio saugumo rizikų vertinimas grindžiamas Centro patvirtintu rizikų žemėlapiu, kuriame identifikuotos reikšmingiausios veiklos, informacinių sistemų, duomenų apsaugos ir organizacinės rizikos. Šiame priede detalizuojamos su kibernetiniu saugumu susijusios rizikos, nustatytos rizikų žemėlapyje. Kibernetinio saugumo rizikos Centre vertinamos kaip mažos, atsižvelgiant į tai, kad Centras nėra priskirtas kibernetinio saugumo subjektams, o taikomos organizacinės ir techninės kontrolės priemonės mažina šių rizikų tikimybę ir poveikį.

KIBERNETINIO SAUGUMO RIZIKOS TIPAI CENTRE

Centre išskiriamos šios pagrindinės kibernetinio saugumo rizikų grupės:

1. **Grėsmės internete:** tai viena didžiausių kibernetinio saugumo rizikų grupių. Tai įvairūs tiesioginiai ir netiesioginiai išpuoliai, įsilaužimai, atakos. Internetinių grėsmių pavyzdžiai yra virusai, įsilaužimai, šlamšto el. laiškai, apgaulingos SMS žinutės.
2. **Vidinės grėsmės:** tai grėsmės, kylančios dėl darbuotojų ir mokinių veiksmų. Šios grėsmės gali būti tyčinės arba netyčinės. Tai slaptažodžių atskleidimas, slaptos informacijos aptarimas su kolegomis, sąmoningas neskelbtinos informacijos atskleidimas.
3. **Fizinės grėsmės:** tai materialaus Centro turto (kompiuterių, serverių, kitų įrenginių) pažeidimas arba vagystė. Fizinės grėsmės kyla dėl stichinių nelaimių, teroristinių išpuolių ar tyčinio fizinio turto sugadinimo arba vagystės.

RIZIKOS LYGIO NUSTATYMAS

Šiame priede pateiktos rizikos atitinka Centro rizikų žemėlapyje identifikuotas kibernetinio saugumo, informacinių sistemų, duomenų apsaugos ir su skaitmeninėmis technologijomis susijusias rizikas.

Lygis	Tikimybės apibrėžimas	Pavyzdys
Aukštas	Grėsmės šaltinis yra labai motyvuotas ir pakankamai pajėgus, o kontrolės priemonės, kuriomis siekiama užkirsti kelią pažeidžiamumui, yra neveiksmingos	Neteisėtas kenkėjiškas informacijos atskleidimas, kenkimas ar sunaikinimas
Vidutinis	Grėsmės šaltinis yra motyvuotas arba pajėgus, tačiau kontrolės priemonės gali trukdyti sėkmingai pasinaudoti pažeidžiamumu	Netyčinės klaidos ir pažeidimai

Žemas	Grėsmės šaltiniui trūksta motyvacijos ar gebėjimų, o taikomos kontrolės priemonės gali užkirsti kelią pažeidžiamumui	IT sutrikimai dėl stichinių ar žmogaus sukeltų nelaimių

DAŽNIAUSIAI GALINČIOS PASITAIKYTI RIZIKOS IR JŲ LYGIS

Rizika	Rizikos lygis	Rekomendacijos
Darbuotojas ar mokinys paspaudė įtartiną nuorodą (phishing)	Žema rizika	Reguliariai organizuoti mokymus apie kibernetines grėsmes ir sukčiavimo atpažinimą. Diegti el. pašto filtravimo priemones (antispam, antivirus). Skatinti naudotojus tikrinti nuorodų adresus prieš jas atidarant. Nustatyti aiškią pranešimo apie įtartinus laiškus tvarką.
Prisijungimo duomenų atskleidimas	Žema rizika	Taikyti stiprių slaptažodžių politiką (ilgis, sudėtingumas, periodinis keitimas). Naudoti dviejų veiksnių autentifikavimą. Drausti slaptažodžių dalinimąsi. Vykdyti darbuotojų ir mokinių informavimą apie saugų prisijungimo duomenų naudojimą.
Kenkėjiškos programinės įrangos įdiegimas	Žema rizika	Riboti programinės įrangos diegimo teises (tik administratoriams). Naudoti antivirusines ir apsaugos sistemas su automatiniu atnaujinimu. Vykdyti reguliarius įrenginių patikrinimus. Užtikrinti operacinių sistemų ir programų atnaujinimus.
Virusų patekimas per laikmenas	Žema rizika	Riboti išorinių laikmenų naudojimą. Naudoti antivirusines programas su realaus laiko apsauga. Informuoti naudotojus apie saugų laikmenų naudojimą. Esant galimybei – naudoti USB prieigos kontrolę.
Informacinių sistemų (el. dienyno, DBIS) sutrikimai	Žema rizika	Užtikrinti sistemų techninę priežiūrą ir atnaujinimus. Turėti sutartis su paslaugų teikėjais dėl gedimų šalinimo. Numatyti alternatyvius darbo būdus (pvz., laikinas duomenų fiksavimas). Stebėti sistemų veikimą ir registruoti sutrikimus.

Duomenų praradimas (techniniai gedimai, virusai)	Žema rizika	Reguliariai daryti atsargines duomenų kopijas. Laikyti kopijas atskiroje ar izoliuotoje aplinkoje. Periodiškai testuoti duomenų atkūrimą. Užtikrinti atsarginių kopijų apsaugą nuo neteisėtos prieigos.
Asmens duomenų pažeidimai (BDAR)	Žema rizika	Taikyti prieigos kontrolės principus. Riboti prieigą prie asmens duomenų tik įgaliotiems asmenims. Organizuoti BDAR mokymus. Naudoti saugias duomenų perdavimo priemones. Registruoti ir analizuoti duomenų saugumo incidentus.
Netinkamas DI įrankių naudojimas	Žema rizika	Parengti DI naudojimo gaires darbuotojams ir mokiniams. Informuoti apie akademinio sąžiningumo principus. Riboti jautrios informacijos įvedimą į DI sistemas. Vykdyti švietimą apie DI naudojimo rizikas.
Vidaus komunikacijos trūkumai (informacijos nepasiekimas)	Žema rizika	Naudoti vieningas komunikacijos priemones (vidinės sistemos, dokumentų valdymo sistemos). Nustatyti aiškią informacijos perdavimo tvarką. Organizuoti reguliarius susirinkimus. Užtikrinti informacijos prieinamumą darbuotojams.
Įrangos sugadinimas ar praradimas	Žema rizika	Vykdyti turto apskaitą ir inventorizaciją. Užtikrinti fizinę įrangos apsaugą (rakinamos patalpos, stebėjimas). Paskirti atsakingus asmenis. Registruoti incidentus ir analizuoti jų priežastis.
Elektros tiekimo ar infrastruktūros sutrikimai, galintys paveikti informacinių sistemų veikimą	Žema rizika	Užtikrinti techninę infrastruktūros priežiūrą. Esant galimybei naudoti nepertraukiamo maitinimo šaltinius (UPS). Numatyti veiklos tęstinumo priemones. Informuoti atsakingus asmenis apie sutrikimus ir užtikrinti operatyvų reagavimą.

KIBERNETINIO SAUGUMO RIZIKŲ MAŽINIMO PRIEMONĖS CENTRO LYGMENIU

Slaptažodžių politika - užtikrinti saugių slaptažodžių naudojimą (pakankamą sudėtingumą, periodinį keitimą, nenaudojimą keliuose įrenginiuose) ir drausti jų atskleidimą tretiesiems asmenims.

Kelių žingsnių autentifikacija - esant galimybei, taikyti kelių žingsnių autentifikaciją (MFA) svarbiausioms informacinėms sistemoms ir paskyroms apsaugoti.
Apsauga nuo kenkėjiškos programinės įrangos - naudoti antivirusines ir kitas apsaugos priemones, užtikrinti jų nuolatinį atnaujinimą ir veikimą visuose Centro įrenginiuose.
Atsarginės duomenų kopijos - užtikrinti reguliarių atsarginių duomenų kopijų sudarymą, jų saugų saugojimą ir periodinį atkūrimo testavimą.
Prieigos kontrolė - taikyti prieigos teisių valdymą, užtikrinant, kad prieiga prie informacijos suteikiama tik tiems asmenims, kuriems ji būtina jų funkcijoms vykdyti.
Darbuotojų ir mokinių informavimas bei mokymai - organizuoti mokymus ir informavimo priemones, skirtas kibernetinio saugumo sąmoningumui didinti ir žmogiškųjų klaidų rizikai mažinti.
Programinės įrangos atnaujinimai - užtikrinti, kad visos naudojamos informacinės sistemos ir programinė įranga būtų reguliariai atnaujinamos.
Darbo ir asmeninių įrenginių naudojimo kontrolė - nustatyti saugaus darbo ir asmeninių įrenginių naudojimo reikalavimus, užtikrinant duomenų apsaugą ir saugų prisijungimą prie Centro sistemų.
Tinklo apsauga (ugniasienės) - naudoti ugniasienes ir kitas tinklo apsaugos priemones, siekiant apsaugoti Centro informacines sistemas nuo išorinių grėsmių.
Belaidžio tinklo saugumas - užtikrinti saugų bevielio tinklo veikimą (naudoti stiprius slaptažodžius, šifravimą, prieigos ribojimą ir įrangos priežiūrą).

KIBERNETINIO SAUGUMO RIZIKŲ MAŽINIMO PRIEMONĖS DARBUOTOJŲ LYGMENIU

Nenaudoti nepatikimų laikmenų - neprijungti nežinomų ar nepatikimų USB atmintinių ir kitų išorinių laikmenų prie Centro kompiuterių.
Darbo vietos saugumas - nepalikti neužrakinto kompiuterio be priežiūros. Naudoti automatinio užrakinimo funkciją.
Prisijungimo duomenų apsauga - saugoti prisijungimo duomenis ir juos naudoti tik asmeniškai, laikantis nustatytų saugumo reikalavimų.
Slaptažodžių saugojimas - nelaikyti prisijungimo duomenų matomose vietose (pvz., ant darbo stalo, monitoriaus ar kituose lengvai prieinamuose paviršiuose).
Konfidencialumo užtikrinimas - niekam neatskleisti prisijungimo duomenų ir kitos konfidencialios informacijos.
Atsargus elgesys su el. laiškais - nespausti įtartinų nuorodų ar neatidaryti neaiškių priedų, ypač gautų iš nežinomų siuntėjų.
Informacijos apsauga - neatskleisti pašaliniams asmenims jautrios asmeninės ar Centro informacijos.
Darbo pabaigos saugumo veiksmai - baigus darbą, uždaryti naudojamas programas, atsijungti nuo informacinių sistemų, išjungti kompiuterį ir nepalikti darbo vietoje dokumentų ar duomenų laikmenų.

Parengė
IT specialistas
Tomas Pečiulis