PATVIRTINTA
Kauno technologijų mokymo centro
direktoriaus 2025 m. rugsėjo 10 d.
įsakymu Nr. 01-293

DIRBTINIO INTELKTO TAIKYMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Dirbtinio intelekto taikymo politika (toliau – Politika) nustato dirbtinio intelekto (toliau – DI) atsakingo naudojimo Kauno technologijų mokymo centro (toliau – Kautech) veikloje principus, užtikrinant informacijos saugumą, privatumą, etiką, atskaitomybę, skaidrumą ir teisėtumą.

2. Politikos tikslas – nustatyti pagrindines Kautech DI taikymo sritis ir principus, užtikrinant Kautech veiklos optimizavimą, atsižvelgiant į Kautech veiklą, procesus, teisės aktais priskirtas funkcijas, strateginius tikslus, teikiamas paslaugas bei teisės aktus, reglamentuojančius DI taikymą.

3. DI taikymo tikslai:

3.1. optimizuoti Kautech veiklą, procesus bei vidaus administravimą;

3.2. užtikrinti efektyvų ir kokybišką Kautech informacinių technologijų (toliau – IT), IT infrastruktūros, informacinių sistemų (toliau – IS), priemonių, duomenų valdymą ir Kautech paslaugų teikimą.

3.3. padėti Kautech valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau kartu – darbuotojai) efektyviai ir kokybiškai vykdyti priskirtas funkcijas, pavedimus, užduotis.

4. DI taikymo sritys:

4.1. Kautech administravimas:

4.1.1. personalo valdymas;

4.1.2. biudžeto planavimas, finansų analizė, prognozavimas;

4.1.3. darbotvarkių, susitikimų planavimas ir protokolavimas;

4.2. Kautech dokumentacijos (administracinės, teisinės, techninės ir kitos) tvarkymas:

4.2.1. dokumentų rengimas, vertimas, analizė, klasifikavimas, santraukų kūrimas, paieška ir tūrinio tikrinimas (pvz., šablonų ataskaitų, sutarčių generavimas);

4.2.2. teisinių rizikų analizė ar atitikties tikrinimas;

4.2.3. techninės dokumentacijos generavimas (pvz., IT sistemų aprašymų sudarymas, schemų rengimas ir kita).

4.3. Kautech IT infrastruktūros, IS, duomenų ir teikiamų paslaugų priežiūra:

4.3.1. duomenų analitikos sprendimai (statistinė analizė, prognozės, anomalijų aptikimas).

4.3.2. IT pagalba ir paslaugų naudotojų konsultavimas;

4.3.3. informacinių sistemų pranešimų, užklausų, el. laiškų klasifikavimas, prioretizavimas, kategorizavimas ir kita;

4.3.4. informacijos saugumo informacinių sistemų pranešimų ir užklausų analizė, pažeidžiamumų aptikimas ir prevencija;

4.3.5. duomenų kokybės, nuoseklumo, tikslumo tikrinimas.

4.4. Kautech veiklos, procesų valdymas, teisės aktais priskirtų funkcijų vykdymas:

4.4.1. procesų, projektų, sutarčių valdymas;

4.4.2. paslaugų stebėsena, analizė ir prognozavimas;

4.4.3. skundų, prašymų, užklausų nagrinėjimas (pvz., skaitmeninis sprendimų priėmimas dėl paslaugų suteikimo, pakeitimo ar nutraukimo);

4.4.4. veiklos analizė ir ataskaitos.

4.5. kitų sričių, suderintų su Dirbtinio intelekto pareigūnu (toliau – DIP) ir patvirtintų VSSA vadovo valdymas:

4.5.1. tęstiniai, pilotiniai arba eksperimentiniai projektai ir DI sistemos;

4.5.2. nauji procesai ir (ar) funkcijos;

4.5.3. kitos suderintos ir patvirtintos sritys.

5. DI sistema – mašina grindžiama sistema, suprojektuota veikti įvairiais autonomijos lygiais, kuri po diegimo gali veikti prisitaikydama ir kuri, siekiant aiškių ar numanomų tikslų, naudodama gautos įvesties duomenis pati daro išvadą, kaip generuoti išvedinius, pavyzdžiui: predikcijas, turinį, rekomendacijas ar sprendimus, kurie gali turėti įtakos fizinei ar virtualiai aplinkai. Ji gali būti kuriama, diegiama ir (ar) taikoma vadovaujantis Politikoje nustatytais pagrindiniais DI taikymo principais.

6. Politika taikoma Kautech struktūriniams padaliniams, darbuotojams ir veikloms, susijusioms su DI taikymu (sprendimų kūrimas ir diegimas, viešieji pirkimai ir kt.).

7. Politikoje vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir 2024 m. birželio 13 d. Europos Parlamento ir Tarybos reglamente (ES) Nr. 2024/1689, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 ir direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas).

II SKYRIUS
DI TAIKYMO PRINCIPAI

8. Pagrindiniai DI taikymo principai:

8.1. Rizikingumas (rizikų valdymas) – visos DI sistemos klasifikuojamos pagal rizikos lygį, remiantis Reglamente (ES) Nr. 2024/1689 nustatytomis rizikų kategorijomis:

8.1.1. nepriimtina rizika (aukščiausio lygio rizika, kai yra draudžiami tokie DI naudojimo atvejai, kurie nesuderinami su ES vertybėmis ir pagrindinėmis žmogaus teisėmis, kaip socialinis reitingavimas ar kenksminga manipuliacija ir kt.);

8.1.2. didelė rizika (DI sistemos, galinčios paveikti asmens saugumą, sveikatą ar teises);

8.1.3. ribota rizika (vidutinės rizikos atvejai, kuriems taikomi skaidrumo reikalavimai);

8.1.4. maža (nedidelė arba minimali rizika būdinga daugumai įprastų DI taikymų, pvz., el. laiškų šlamšto filtrai).

8.1.5. nepriimtinos rizikos DI sistemos Kautech veikloje negali būti naudojamos. Didelės rizikos DI sistemoms taikomi griežti reikalavimai: privalomas rizikos vertinimas ir valdymas, aukštos kokybės mokymo duomenys, veiklos žurnalų (angl. *log files*) kaupimas rezultatų atsekamumui užtikrinti, išsami techninė dokumentacija, aiški informacija naudotojams, teisėtos ir tinkamos stebėsenos priemonės, didelis sistemos patikimumas, saugumas ir tikslumas. Ribotos rizikos DI (pvz.: pokalbių robotai, generatyvinis DI turinys) atvejais turi būti užtikrinamas skaidrumas – naudotojai informuojami, kad sąveikauja su DI, o generuojamas turinys yra atitinkamai pažymėtas. Minimalios rizikos DI naudojimas nėra ribojamas, tačiau net ir tokie projektai turėtų vadovautis atsargumo ir gerosios praktikos principais.

8.2. Informacijos saugumas (kibernetinis saugumas ir asmens duomenų apsauga) – Kautech darbuotojai privalo naudoti tik Kautech leidžiamas ir DI politikos reikalavimus atitinkančias dirbtinio intelekto priemones bei paslaugas, siekiant užtikrinti informacijos saugumą (kibernetinį saugumą ir asmens duomenų apsaugą).

8.3. Pagrindinių žmogaus teisių apsauga – VSSA užtikrina, kad DI sistemos būtų taikomos su pagarba pagrindinėms žmogaus teisėms ir nepažeidžiant pagrindinių žmogaus teisių ar laisvių.

8.4. Naudotojų privatumas – DI sistemos turi nepažeisti naudotojų privatumo, o naudotojai, taikydami DI savo veikloje, turi gerbti privatumą.

8.5. Skaidrumas, paaiškinamumas ir teisė paaiškinimui– DI sistemos veikimas turi būti skaidrus, suprantamas tiek darbuotojams, tiek trečiųjų asmenų atstovams.

8.6. Žmogaus kontrolė ir sprendimų priežiūra – DI sistemos turi būti suprojektuotos taip, kad žmogus galėtų veiksmingai prižiūrėti jų veikimą, suprasti ir, prireikus, įsikišti (pakoreguoti, sustabdyti ar ignoruoti), kad sumažintų riziką.

8.7. Etika (bendroji etika) – DI sistemos turi su visais elgtis teisingai, o galimybes, išteklius ir informaciją paskirstyti teisingai naudotojų atžvilgiu, vadovaujantis etikos principais:

8.7.1. nediskriminavimas ir sąžiningumas;

8.7.4. socialinė nauda ir žalos nedarymas;

8.7.5. atitiktis etikos standartams ir teisės viršenybė.

8.8. Atskaitomybė (atsekamumas) – turi būti užtikrinama, kad už kiekvieną DI sistemos sukūrimą ir (ar) diegimą būtų aiškiai nustatyti atsakingi asmenys – tiek techniniu, tiek sprendimų priėmimo lygmeniu. DI sistemų priežiūra integruojama į Kautech valdymo struktūrą: paskiriami atsakingi darbuotojai, kurie prižiūri DI sistemų gyvavimo ciklą, rizikų valdymą ir atitikimą Politikoje nustatytiems principams.

8.9. Teisėtumas (pagrįstumas) – DI taikymas turi būti teisiškai pagrįstas, naudotojas taikydamas DI sistemas savo veikloje turi vadovautis tiek Kautech vidiniais teisės aktais, tiek kitais galiojančiais teisės aktais, nepažeidžiant nustatytų teisės aktų normų.

III SKYRIUS
ATSAKOMYBĖ

9. Kautech vadovas atsako už bendrą DI taikymą ir už Politikos įgyvendinimą.

10. Už Politikos įgyvendinimo organizavimą, koordinavimą ir kontrolę atsako asmuo, atsakingas už Kautech DI taikymą – DI pareigūnas (toliau – DIP), vadovaudamasis DI taikymo principais ir užtikrindamas rizikų valdymą, informacijos saugumą ir teisėtumą. DIP skiriamas Kautech vadovo sprendimu, kartu nurodant ir DIP pavaduojantį asmenį. DIP atlieka savo funkcijas padedant Kautech saugos įgaliotiniui (-iams) (toliau – SĮ), duomenų apsaugos pareigūnui ir kibernetinio saugumo vadovui.

11. DIP atlieka šias pagrindines funkcijas:

11.1. vertina ir prižiūri Politikos įgyvendinimą;

11.2. identifikuoja DI taikymo rizikas, apie jas informuoja Kautech vadovą ir (ar) atsakingus darbuotojus – Kautech IS ir (ar) aplikacijų (programinės įrangos) savininkus bei administratorius, taip pat siūlo technines ir (ar) organizacines priemones;

11.3. dalyvauja DI sistemų poveikio vertinime;

11.4. dalyvauja tiriant ir sprendžiant incidentus, susietus su DI taikymu;

11.5. komunikuoja su teisės aktais nustatytomis nacionalinėmis DI kompetentingomis institucijomis (notifikuojančioji, rinkos priežiūros, kitos);

11.6. konsultuoja Kautech darbuotojus DI taikymo klausimais;

11.6. organizuoja Kautech darbuotojų DI mokymus ir reguliarius mokymus;

11.7. informuoja Kautech vadovą DI taikymo klausimais;

11.8. ne rečiau kaip vieną kartą per metus atsiskaito Kautech vadovui apie DI taikymo veiklas, identifikuotas rizikas ir rizikos mažinimo priemones.

12. Už Politikos įgyvendinimą atsako Kautech IS ir (ar) programinės įrangos savininkai ir administratoriai, padedant SĮ.

13. SĮ atlieka šias funkcijas:

13.1. dalyvauja šios Politikos įgyvendinime;

13.2. dalyvauja sprendžiant įvykius, incidentus ir problemas (pažeidžiamumus), susietus su DI taikymu;

13.3. dalyvauja su DI taikymu susietų techninių ir (ar) organizacinių priemonių diegime;

13.4. inicijuoja ir organizuoja Kautech darbuotojų informacijos saugumo mokymus ir reguliarų instruktavimą;

13.5. inicijuoja Politikos pakeitimus.

14. Už DI sistemų taikymą vadovaujantis Politika, bei kitais DI taikymą reglamentuojančiais teisės aktais, tiesiogiai atsakingi Kautech darbuotojai. Kautech skyrių vadovai privalo imtis reikiamų priemonių, kad užtikrintų Politikos bei kitų DI taikymą reglamentuojančių teisės aktų nuostatų laikymąsi skyrių veikloje.

15. Už techninių ir organizacinių priemonių įgyvendinimą, įskaitant informacijos saugumo užtikrinimą, rizikų, poveikio asmens duomenų apsaugai vertinimą ir (ar), esant būtinumui, poveikio vertinimą (atliekamas didelės rizikos DI sistemoms, vadovaujantis Reglamento (ES) Nr. 2024/1689 nuostatomis), taikant DI sistemas, atsakingi IS, aplikacijų (taikomųjų programų) savininkai ir administratoriai.

16. Kautech darbuotojai privalo laikytis šios Politikos nuostatų ir informuoti atsakingus asmenis apie identifikuotus neatitikimus, rizikas bei informacijos saugumo incidentus (pažeidimus).

IV SKYRIUS
VIEŠIEJI PIRKIMAI, STEBĖSENA IR INFORMACIJOS SAUGUMAS

17. Vykdant viešuosius pirkimus dėl DI sistemų bei įgyvendinant DI sistemų viešųjų pirkimų sutartis, turi būti:

17.1. viešųjų pirkimų dokumentuose nustatyti reikalavimai dėl DI, kartu numatant reikalavimus dėl DI sistemų atitikties Reglamento (ES) Nr. 2024/1689 nuostatų užtikrinimo;

17.2. sutartinių įsipareigojimų vykdymo priežiūra ir rizikų valdymas;

17.3. užtikrinamas bendradarbiavimas su DI sistemų tiekėjais.

18. DI informacijos saugumą, sprendimų atsekamumą, skaidrumą ir tobulinimą užtikrina:

18.1. DI sistemų inventorizacija;

18.2. reguliarios DI sistemų peržiūros ir (ar) auditai;

18.3. DI sistemų etikos vertinimai;

18.4. incidentų, susijusių su DI taikymu, valdymas.

19. Taikant DI sistemas, informacijos saugumas užtikrinamas vadovaujantis:

19.1. Reglamentu (ES) Nr. 2024/1689;

19.2. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (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);

19.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;

19.4. Lietuvos Respublikos kibernetinio saugumo įstatymu;

19.5. Lietuvos Respublikos valstybės informacinių išteklių įstatymu;

19.6. kitais informacijos saugumą reglamentuojančiais teisės aktais.

20. Kautech užtikrina tinkamą informacinių sistemų saugumo lygį, naudojant visas DI sistemas. Taikant DI, įgyvendinamos informacijos saugumui užtikrinti būtinos ir proporcingos techninės bei organizacinės priemonės, atsižvelgiant į galimas grėsmes (pvz.: duomenų nutekėjimą, modelio perėmimą ar klaidingų duomenų įdiegimą). Kiekvienai DI sistemai atliekamas atskiras informacijos saugumo rizikos vertinimas, įtraukiant informacijos saugumo specialistus. Minimalūs reikalavimai apima: prieigos kontrolę (tik įgalioti naudotojai gali pasiekti DI sistemas ir duomenis), duomenų šifravimą perdavimo ir saugojimo metu (ypač jautriems duomenims), reguliarų pažeidžiamumų testavimą, atnaujinimų diegimą, atsarginį kopijavimą.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

21. Politikos nuostatų privalo laikytis visi Kautech darbuotojai.
22. Politika peržiūrima ne rečiau kaip vieną kartą per metus.
23. Už Politikos peržiūrą ir atnaujinimą atsakingas Politikos savininkas – DIP.

SUDERINTA
Kauno technologijų mokymo centro
įstaigos tarybos (savivaldos institucijos)
2025-09-08 posėdžio protokolu Nr. 21-9

SUDERINTA
Kauno technologijų mokymo centro
Darbo tarybos 2025-09-09
posėdžio protokolu Nr. 29-6