PATVIRTINTA
UAB „Vilniaus vandenys“
Reg. data: 2026-06-18 Reg. Nr.: VTA-PL26-7
Valdybos posėdžio protokolu Nr.: PR-V26-10

Vilniaus vandenys

GENERATYVINIO DIRBTINIO INTELEKTO NAUDOJIMO POLITIKA

Tikslas	Politikos tikslas – nustatyti generatyvinio dirbtinio intelekto (toliau – DI) naudojimo UAB „Vilniaus vandenys“ principus, atsakomybes ir aukšto lygio reikalavimus, užtikrinančius saugų, atsakingą, teisėtą ir skaidrų DI taikymą. Bendrovė siekia skatinti DI naudojimą, kuris kuria vertę įmonei, jos akcininkams ir interesų dalininkams, kartu valdant su tuo susijusias rizikas. Politika apibrėžia DI naudojimo valdymo sistemą, o detalūs organizaciniai ir techniniai reikalavimai nustatomi vidaus teisės aktuose.
Taikymo sritis	Politika taikoma visiems Bendrovės darbuotojams, vadovams, kolegialių organų nariams, partneriams ir kitiems asmenims, turintiems prieigą prie Bendrovės informacinių išteklių ar duomenų ir naudojantiems generatyvinio DI įrankius darbo funkcijoms atlikti, nepriklausomai nuo naudojamo DI įrankio tipo (vidinio ar išorinio). Politika taikoma visiems DI naudojimo atvejams, susijusiems su Bendrovės veikla.
Susiję teisės aktai	Politika taikoma, vadovaujantis teisės aktais, reglamentuojančiais dirbtinio intelekto naudojimą, duomenų apsaugą, kibernetinį saugumą ir informacinių technologijų valdymą. *Europos Sąjungos teisės aktai:* • 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (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 - BDAR); • Europos parlamento ir tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS2 direktyva); • Europos Parlamento ir Tarybos reglamentas (ES) 2024/1689 dėl dirbtinio intelekto taisyklių (ES Dirbtinio intelekto aktas). *Lietuvos Respublikos teisės aktai:* • 2026–2035 metų nacionalinės dirbtinio intelekto strateginės gairės, patvirtintos LR ekonomikos ir inovacijų ministro 2026 m. balandžio 20 d. įsakymu Nr. 4-156; • Lietuvos Respublikos kibernetinio saugumo įstatymas ir jį įgyvendinantys teisės aktai; • Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Savivaldybės dokumentai:* • Dirbtinio intelekto naudojimo principų Vilniaus miesto savivaldybėje ir jai pavaldžiose organizacijose aprašas, patvirtintas Vilniaus miesto savivaldybės mero 2026 m. sausio 12 d. potvarkiu Nr. 955-47/26. *Bendrovės vidaus dokumentai:* • Informacijos saugumo politika; • Konfidencialios informacijos valdymo politika; • Rizikų valdymo politika;

	• Asmens duomenų tvarkymo ir saugumo politika ir jos įgyvendinimo taisyklės; • kiti su informacijos saugumu, technologijų naudojimu ir rizikų valdymu susiję Bendrovės vidaus teisės aktai. Politika taip pat taikoma, atsižvelgiant į tarptautines gerąsias praktikas ir standartus, susijusius su dirbtinio intelekto valdymu.
Savininkas	Kokybės ir inovacijų tarnybos direktorius (-ė)
Pirminės politikos sukūrimo data	2026-06-18 Valdybos posėdžio protokolas Nr. PR-V26-10

TURINYS

1. SĄVOKOS IR SUTRUMPINIMAI

Sąvoka/ Sutrumpinimas	Paaiškinimas
Bendrovė	UAB „Vilniaus vandenys“
BDAR	Bendrasis duomenų apsaugos reglamentas (Reglamentas (ES) 2016/679)
Dirbtinis intelektas (DI)	Technologijos ir sistemos, galinčios atlikti užduotis, paprastai reikalaujančias žmogaus intelekto, įskaitant turinio generavimą, analizę ir sprendimų palaikymą
DI agentas	Autonomiškai ar pusiau autonomiškai veikiantis generatyvinio DI įrankis, skirtas atlikti konkrečias užduotis pagal nustatytas taisykles ar instrukcijas
DI asistentas	Asmeninis generatyvinio DI įrankis, skirtas padėti darbuotojui atlikti kasdienes užduotis, automatizuoti procesus ir kurti turinį
DI išeitis	DI generuojamas turinys (tekstas, vaizdas, garsas ir kt.)
DI įrankis	DI sistema arba programa, skirta atlikti tam tikras užduotis
DI naudojimo gairės	Dokumentas, nustatantis praktinius generatyvinio DI naudojimo, saugojimo ir rizikų valdymo reikalavimus Bendrovėje
DI sprendimas	DI įrankio, asistento ar agento taikymas konkrečiame procese ar paslaugoje
Generatyvinis DI	DI, galintis kurti naują turinį (tekstą, vaizdą, garsą ir kt.)
Kibernetinio saugumo vadovas (angl. *Chief Information Security Officer,* toliau – CISO)	Už kibernetinio saugumo valdymą atsakingas Bendrovės darbuotojas arba trečiosios šalies, teikiančios paslaugas, darbuotojas

Licencijuotas DI įrankis	DI įrankis, kurį Bendrovė oficialiai leidžia naudoti darbo funkcijoms atlikti ir kuris yra valdomas Bendrovės IT aplinkoje arba, jeigu nėra valdomas IT aplinkoje, patvirtintas IT ir CISO
Politika	Generatyvinio dirbtinio intelekto naudojimo politika
Skaidrumas	Principas, pagal kurį aiškiai nurodoma, kada ir kokiu tikslu naudojamas dirbtinis intelektas, ypač – kai DI generuotas turinys pasiekia išorinius naudotojus

2. BENDRIEJI REIKALAVIMAI

2.1. Ši Politika reglamentuoja Generatyvinio dirbtinio intelekto (toliau – DI) naudojimą Bendrovės viduje.
2.2. Politikos nuostatos yra suderintos su išorės teisės aktų, reglamentuojančių dirbtinio intelekto naudojimo principus, nuostatomis, ir Dirbtinio intelekto naudojimo principų Vilniaus miesto savivaldybėje ir jai pavaldžiose organizacijose aprašo reikalavimais.
2.3. Jei DI Išeitis yra naudojama Bendrovės išorinei komunikacijai ar paslaugų teikimui, turi būti aiškiai nurodyta, kad turinys ar sprendimas sugeneruotas naudojant DI.
2.4. Darbuotojų pareigos, leidžiami ir draudžiami DI naudojimo atvejai, taip pat techniniai saugumo reikalavimai nustatomi Bendrovės vidaus teisės akte (DI naudojimo gairėse).

3. PAGRINDINIAI PRINCIPAI

3.1. DI Bendrovėje naudojamas, vadovaujantis šiais principais:
- 3.1.1. ***Atsakomybės*** – galutinė atsakomybė už DI sprendimus ir sugeneruotą turinį tenka žmogui;
- 3.1.2. ***Žmogaus priežiūros*** – prieš naudojant sugeneruotas DI turinys tikrinamas žmogaus;
- 3.1.3. ***Saugumo*** – DI naudojimas turi atitikti informacijos saugumo (įskaitant kibernetinį saugumą ir asmens duomenų apsaugą) reikalavimus;
- 3.1.4. ***Teisėtumo*** – DI naudojimas turi atitikti galiojančius teisės aktus, įskaitant BDAR ir ES Dirbtinio intelekto aktą;
- 3.1.5. ***Skaidrumo*** – kai DI generuotas turinys turi poveikį išoriniams asmenims, turi būti užtikrinamas aiškus DI vaidmens atskleidimas;
- 3.1.6. ***Proporcingumo*** – DI naudojimas turi būti pagrįstas verslo poreikiu ir neviršyti būtinos apimties;
- 3.1.7. ***Atsakingos inovacijos*** – DI naudojimas Bendrovėje skatinamas, kai jis kuria vertę įmonei, jos akcininkams ir interesų dalininkams, didina efektyvumą ar gerina paslaugų kokybę, užtikrinant teisėtą, skaidrų ir proporcingą taikymą bei tinkamą rizikų valdymą;
- 3.1.8. ***DI kompetencijų ugdymo ir įgalinimo*** – Bendrovė sistemingai skatina darbuotojų gebėjimų naudoti DI plėtrą, sudarydama sąlygas įgyti reikiamas kompetencijas, dalintis gerąja praktika ir taikyti DI sprendimus kasdienėje veikloje, laikantis šios Politikos ir vidaus teisės aktų reikalavimų.

4. GENERATYVINIO DIRBTINIO INTELEKTO ĮRANKIŲ NAUDOJIMAS IR ATSAKOMYBĖ

4.1. DI įrankiai Bendrovėje naudojami laikantis šios Politikos ir Bendrovės vidaus teisės aktų nuostatų.
4.2. DI naudojimas yra pagalbinė priemonė, skirta padėti darbuotojui atlikti užduotis, tačiau galutinė atsakomybė už sprendimus ir parengtą turinį tenka žmogui. DI sprendimai negali būti naudojami kaip galutinio sprendimo priemonė tais atvejais, kai jie gali turėti teisinį, finansinį ar reputacinį poveikį Bendrovės veiklai.
4.3. Išorinių DI įrankių naudojimo sąlygos ir ribojimai nustatomi Bendrovės vidaus teisės akte – DI naudojimo gairėse.
4.4. DI naudojimas Bendrovėje valdomas, laikantis aiškaus atsakomybių pasiskirstymo, užtikrinant priežiūrą, rizikų valdymą ir operacinį įgyvendinimą. DI naudojimas Bendrovėje valdomas, taikant trijų lygių valdymo modelį:

4.4.1. Strateginis lygmuo, kuriame Bendrovės valdyba nustato pagrindines DI naudojimo kryptis ir ribas Bendrovėje;
4.4.2. Valdymo ir priežiūros lygmuo, kuriame užtikrinama DI naudojimo atitiktis teisės aktams, rizikų valdymo ir kibernetinio saugumo reikalavimams;
4.4.3. Operacinis lygmuo, kuriame DI sprendimai inicijuojami, diegiami ir naudojami konkrečiuose procesuose pagal DI naudojimo gaires.

4.5. Bendrovės valdyba tvirtina DI naudojimo politiką, nustatydama DI naudojimo kryptis ir ribas Bendrovėje.

4.6. Bendrovės generalinis direktorius ir vadovybė privalo:
4.6.1. užtikrinti nuoseklų šios Politikos įgyvendinimą Bendrovėje;
4.6.2. užtikrinti, kad DI naudojimas būtų integruotas į Bendrovės valdymo, rizikų ir vidaus kontrolės sistemas;
4.6.3. skirti atsakingus padalinius ir (ar) asmenis DI naudojimo koordinavimui, priežiūrai ir kontrolei;
4.6.4. užtikrinti, kad DI naudojimui būtų skiriami pakankami organizaciniai, žmogiškieji ir finansiniai ištekliai.

4.7. Siekdama skatinti saugų ir vertę kuriantį DI naudojimą, Bendrovė:
4.7.1. sudaro galimybes darbuotojams naudotis patvirtintais ir licencijuotais DI įrankiais ir proaktyviai kelia darbuotojų kompetencijas, siekiant efektyvaus DI įrankių naudojimo;
4.7.2. skatina DI taikymą procesų efektyvinimui, paslaugų kokybės gerinimui ir sprendimų priėmimo palaikymui;
4.7.3. palaiko eksperimentinius ir pilotinius DI taikymo atvejus, kai jie vykdomi laikantis šios Politikos ir rizikų valdymo reikalavimų;
4.7.4. užtikrina, kad DI naudojimas būtų siejamas su nuosekliu organizaciniu mokymusi ir inovacijų valdymu.

5. RIZIKŲ IR INCIDENTŲ VALDYMAS

5.1. DI naudojimas Bendrovėje grindžiamas rizikų vertinimu. DI naudojimo rizikos įtraukiamos į Bendrovės rizikų valdymo sistemą.

5.2. DI naudojimo rizikos klasifikuojamos pagal jų poveikį ir reikšmingumą, o klasifikavimo kriterijai nustatomi šią Politiką įgyvendinančiame Bendrovės vidaus teisės akte – DI naudojimo gairėse.

5.3. Rizikų vertinimas atliekamas prieš diegiant naujus ar reikšmingai keičiant esamus DI sprendimus, taip pat periodiškai, ne rečiau kaip kartą per metus.

5.4. DI naudojimo rizikų valdymo priemonės taikomos proporcingai DI naudojimo pobūdžiui, apimčiai ir galimam poveikiui.

5.5. Su DI susiję incidentai, turintys poveikį informacijos ar kibernetiniam saugumui, laikomi kibernetinio saugumo incidentais ir valdomi pagal galiojančias Bendrovės incidentų valdymo procedūras.

6. POLITIKOS ĮGYVENDINIMO VALDYMAS

6.1. DI naudojimas Bendrovėje turi atitikti galiojančius Europos Sąjungos ir Lietuvos Respublikos teisės aktus, reglamentuojančius duomenų apsaugą, kibernetinį saugumą, dirbtinio intelekto naudojimą ir kitus su technologijų taikymu susijusius reikalavimus.

6.2. Naudojant DI turi būti užtikrinama:
6.2.1. Asmens duomenų apsauga pagal BDAR;
6.2.2. DI sistemų naudojimo atitiktis ES Dirbtinio intelekto akto reikalavimams;
6.2.3. Kibernetinio saugumo reikalavimų laikymasis pagal taikomus nacionalinius ir Europos Sąjungos teisės aktus;
6.2.4. Bendrovės vidaus teisės aktų laikymasis.

6.3. DI sprendimų diegimas ir naudojimas turi būti vykdomas, laikantis atsakingo technologijų taikymo principų ir užtikrinant, kad DI sistemos nekeltų nepagrįstos rizikos asmenų teisėms, Bendrovės veiklos patikimumui ar reputacijai.

6.4. Kai DI naudojimas gali turėti reikšmingą poveikį asmenų teisėms, Bendrovės veiklai ar sprendimų priėmimui, prieš tokį naudojimą atliekamas papildomas rizikos ir atitikties vertinimas.
6.5. DI naudojimo atitikties užtikrinimo priemonės ir vertinimo procedūros detalizuojamos Bendrovės vidaus teisės akte – DI naudojimo gairėse.
6.6. DI naudojimas turi būti dokumentuojamas ir pagrindžiamas, kai to reikalauja teisės aktai arba rizikos lygis.
6.7. Atsakomybė už DI naudojimo atitikties užtikrinimą paskirstoma pagal šioje Politikoje nustatytą atsakomybių ir valdymo modelį.
6.8. DI naudojimas negali pakeisti sprendimų priėmimo, kontrolės ar atsakomybės, nustatytų teisės aktais ar Bendrovės vidaus dokumentais.
6.9. Procesuose, kuriuose DI naudojimas turi poveikį išoriniams naudotojams, turi būti užtikrintas skaidrumas ir galimybė paaiškinti DI vaidmenį.

7. POLITIKOS STEBĖSENA

7.1. DI naudojimo stebėsena vykdoma, siekiant ne tik užtikrinti šios Politikos laikymąsi, bet ir vertinti bei skatinti atsakingą, efektyvų ir vertę kuriantį DI naudojimą Bendrovėje.
7.2. Už DI naudojimo Bendrovėje koordinavimą atsakingas Strategijos ir inovacijų skyriaus vadovas, veikdamas kartu su IT skyriaus vadovu ir CISO, vykdo nepriklausomą DI naudojimo kibernetinio saugumo ir su tuo susijusių rizikų priežiūrą.
7.3. Stebėsena vykdoma naudojant apibendrintus naudojimo rodiklius, apimančius:
  7.3.1. darbuotojų kompetencijas, mokymų apimtį ir pasirengimą naudoti DI;
  7.3.2. DI faktinio naudojimo apimtį;
  7.3.3. su DI naudojimu susijusias rizikas, incidentus, Politikos reikalavimų laikymąsi ir nustatytus pažeidimus;
  7.3.4. DI naudojimo skaidrumą išorinėje komunikacijoje;
  7.3.5. DI taikymo brandą Bendrovėje, įskaitant taikymo atvejus ir sprendimus, pilotines iniciatyvas, darbuotojų įsitraukimą, dalijimąsi gerąja praktika bei grįžtamąjį ryšį dėl DI įrankių ir palaikymo pakankamumo.
7.4. Stebėsenos rezultatai ne rečiau kaip kasmet pristatomi Bendrovės valdybai. Stebėsenos rezultatai naudojami sprendžiant dėl DI įrankių plėtros ar licencijavimo, darbuotojų mokymų ir kompetencijų stiprinimo bei procesų ar veiklos sričių, kuriose DI gali būti taikomas platesniu mastu, identifikavimo.
7.5. Bendrovė turi taikyti proporcingas organizacines ir technines priemones DI naudojimo kontrolei užtikrinti.

8. BAIGIAMOSIOS NUOSTATOS

8.1. Politiką tvirtina, keičia ir panaikina Bendrovės valdyba.
8.2. Politika peržiūrima ne rečiau kaip kas trejus metus arba esant reikšmingiems technologiniams, teisiniams ar organizaciniams pokyčiams.
8.3. Už Politikos parengimą ir atnaujinimą atsakingas Kokybės ir inovacijų tarnybos direktorius (-ė).
8.4. Politika taikoma visiems Bendrovės padaliniams.
8.5. Politikos nuostatų įgyvendinimas detalizuojamas Generatyvinio dirbtinio intelekto naudojimo gairėse ir kituose Bendrovės vidaus dokumentuose.
8.6. Ši politika skelbiama viešai Bendrovės interneto svetainėje https://www.vv.lt.
8.7. Bendrovės padalinių, kurių darbuotojai savo veikloje turi vadovautis šia Politika, vadovai atsakingi už darbuotojų supažindinimą su Politika.