

POLITICA INSTITUȚIONALĂ PRIVIND GUVERNANȚA ȘI UTILIZAREA INTELIGENȚEI ARTIFICIALE

Cadru AI-first bazat pe autonomie proporțională cu riscul

Cod document	POL-AI-01
Versiune	1.0
Data elaborării	14 septembrie 2026
Statut	Proiect pentru aprobare instituțională
Aprobare	Hotărârea Senatului Universitar nr. <u>55</u> / <u>14.09.2026</u>
Intrare în vigoare	<u>15.09.2026</u>
Revizuire	Cel puțin anual și la modificări legislative/tehnologice semnificative

DOCUMENT INTERN DE GUVERNANȚĂ INSTITUȚIONALĂ

Documentul stabilește condițiile în care IA poate asista, executa, automatiza sau prelua integral activități, precum și situațiile în care controlul și decizia umană rămân obligatorii.

Controlul documentului

Prezenta politică reprezintă cadrul instituțional general. Procedurile, instrucțiunile, registrele, standardele tehnice și anexele aprobate în baza sa pot detalia cerințele fără a contrazice principiile stabilite prin politică.

Rol	Structură / persoană	Responsabilitate	Semnătură / dată
Elaborare	Comitetul de Guvernanță IA / structură desemnată	Elaborare și actualizare	
Avizare	DPO / responsabil protecția datelor	Protecția datelor și DPIA, după caz	
Avizare	Juridic / conformitate	Conformitate juridică	
Avizare	IT / securitate informațională	Securitate, integrare și control tehnic	
Avizare	Comisia de Etică Universitară	Integritate și etică academică	
Aprobare	Senatul Universitar	Aprobarea politicii	

Cuprins

1. Scop și obiective
2. Domeniu de aplicare
3. Temei normativ și relația cu alte reglementări
4. Definiții
5. Principii instituționale
6. Modelul de autonomie proporțională
7. Clasificarea riscului și impactului
8. Regimul didactic
9. Regimul administrativ
10. Medicină, stomatologie și contexte clinice
11. Date, confidențialitate și securitate
12. Integritate academică și evaluare
13. Transparență și informarea persoanelor
14. Achiziția, integrarea și aprobarea sistemelor IA
15. Guvernanță, roluri și responsabilități
16. Monitorizare, audit și managementul incidentelor
17. Nerespectarea politicii
18. Formare și alfabetizare IA
19. Implementare și dispoziții tranzitorii
20. Revizuire și intrare în vigoare
- Anexa 1. Matrice risc - autonomie
- Anexa 2. Niveluri de utilizare IA în evaluarea studenților
- Anexa 3. Declarație de utilizare IA
- Anexa 4. Fișa de înregistrare a unui sistem IA
- Anexa 5. Checklist de evaluare înainte de achiziție/implementare

Anexa 6. Raportarea incidentelor IA

Anexa 7. Exemple de utilizări permise, condiționate și interzise

Referințe normative și documentare

1. Scop și obiective

Prezenta politică stabilește cadrul instituțional pentru adoptarea, utilizarea, automatizarea și guvernarea sistemelor de inteligență artificială (IA) în activitățile didactice, de cercetare și administrative ale Universității Apollonia din Iași.

Politica pornește de la premisa că IA poate produce valoare nu numai ca instrument de asistență, ci și ca mecanism de delegare și automatizare. Universitatea poate transfera integral către sisteme IA activități cu risc redus, dacă acestea pot fi realizate mai eficient, mai consecvent, mai rapid sau mai scalabil și dacă există controale proporționale cu riscul.

Principiul strategic

Scopul politicii nu este conservarea activităților manuale existente. Universitatea urmărește automatizarea responsabilă a activităților delegabile, augmentarea activităților care necesită expertiză și păstrarea controlului uman acolo unde impactul asupra persoanelor, drepturilor, siguranței, evaluării academice sau responsabilității profesionale o impune.

Obiectivele politicii sunt:

- creșterea calității și capacității instituționale prin utilizarea IA;
- reducerea activităților repetitive și a timpului administrativ;
- personalizarea procesului educațional și extinderea accesului la suport academic;
- formarea competențelor de utilizare critică și responsabilă a IA;
- protejarea datelor, confidențialității, integrității academice și securității informaționale;
- prevenirea dependenței necritice de rezultate generate automat și a fenomenului de automation bias;
- stabilirea unui mecanism clar pentru aprobarea, auditarea, suspendarea și retragerea sistemelor IA;
- alinierea utilizării IA cu legislația Uniunii Europene și cu cadrul național aplicabil învățământului superior.

2. Domeniu de aplicare

Politica se aplică tuturor membrilor comunității universitare și tuturor persoanelor care utilizează sisteme IA în numele, pentru activitățile sau prin resursele Universității, inclusiv:

- cadre didactice și cadre didactice asociate;
- studenți, cursanți și alte categorii de beneficiari ai activităților educaționale;
- cercetători și personal implicat în proiecte de cercetare;
- personal administrativ și tehnic;
- conducerea Universității și structurile de management;
- colaboratori, contractori și furnizori, în măsura în care procesează informații sau operează sisteme IA pentru Universitate.

Politica se aplică atât instrumentelor furnizate sau contractate de Universitate, cât și instrumentelor externe utilizate în context instituțional. Utilizarea personală a IA, fără legătură cu activitatea Universității și fără utilizarea datelor sau resurselor instituționale, nu intră în domeniul prezentei politici.

3. Temei normativ și relația cu alte reglementări

Prezenta politică se interpretează și se aplică împreună cu legislația și reglementările instituționale în vigoare. În caz de conflict, prevalează norma juridică superioară și cerința mai strictă aplicabilă situației concrete.

- Regulamentul (UE) 2024/1689 privind inteligența artificială (AI Act), în forma consolidată și astfel cum a fost modificat, inclusiv prin Regulamentul (UE) 2026/1744;
- Regulamentul (UE) 2016/679 (GDPR), în special principiile de protecție a datelor și regulile privind deciziile bazate exclusiv pe prelucrare automatizată;
- Legea învățământului superior nr. 199/2023, cu modificările și completările ulterioare;
- Codul-cadru de etică și deontologie universitară aprobat prin H.G. nr. 305/2024;
- Regulamentul-cadru privind organizarea și funcționarea comisiilor de etică universitară, aprobat prin Ordinul nr. 6.869/2024, în forma în vigoare;
- legislația privind drepturile de autor, securitatea cibernetică, arhivarea, accesul la informații și orice alte norme sectoriale aplicabile.

Politica este un instrument de guvernanta internă și nu substituie analiza juridică, evaluarea de impact privind protecția datelor (DPIA), evaluarea impactului asupra drepturilor fundamentale sau alte evaluări obligatorii atunci când acestea sunt cerute de lege.

4. Definiții

Sistem IA: un sistem bazat pe mașină care, pentru obiective explicite sau implicite, deduce din intrările primite modul de generare a unor rezultate precum predicții, conținut, recomandări sau decizii ce pot influența medii fizice ori virtuale, în sensul legislației aplicabile.

IA generativă: sisteme capabile să genereze sau să transforme text, imagini, audio, video, cod sau alte forme de conținut.

Implementator / deployer: Universitatea sau structura care utilizează un sistem IA sub autoritatea sa, în sensul aplicabil al AI Act.

Proprietar de proces: persoana sau structura instituțională responsabilă pentru obiectivul, regulile, controlul și rezultatele unui proces în care este utilizată IA.

Autonomie IA: gradul în care un sistem IA poate executa o activitate fără intervenție umană asupra fiecărui rezultat individual.

Control uman: intervenția sau supravegherea realizată de o persoană cu competență și autoritate reală pentru a interpreta, opri, modifica, ignora sau inversa rezultatul sistemului, atunci când natura riscului o impune.

Shadow AI: utilizarea neautorizată a unor servicii IA externe pentru activități instituționale, în afara instrumentelor sau regulilor aprobate, atunci când sunt implicate date ori procese protejate.

Incident IA: eveniment în care utilizarea IA produce sau poate produce o încălcare a politicii, pierdere de date, rezultat discriminatoriu, eroare semnificativă, afectarea drepturilor, compromiterea securității sau alte prejudicii relevante.

Date sensibile instituțional: date personale, categorii speciale de date, date privind studenții, HR, date clinice, date financiare nepublice, secrete comerciale, documente confidențiale, credențiale, informații contractuale sau de cercetare nepublicate.

5. Principii instituționale

5.1. AI-first, nu AI-only

Atunci când IA poate îmbunătăți în mod demonstrabil un proces, Universitatea încurajează integrarea sa. IA nu devine însă singura modalitate de acces la servicii atunci când acest lucru ar crea bariere nejustificate, ar afecta drepturi sau ar exclude persoane.

5.2. Autonomie proporțională cu riscul

Nu se impune verificare umană individuală pentru fiecare rezultat IA. Nivelul de control se stabilește în funcție de impact, probabilitatea erorii, reversibilitate și sensibilitatea datelor.

5.3. Responsabilitate la nivel de proces

Pentru procese autonome cu risc redus, responsabilitatea nu înseamnă aprobarea manuală a fiecărui rezultat. Proprietarul de proces răspunde de proiectarea controalelor, monitorizarea performanței, audit și escaladare.

5.4. Control uman semnificativ acolo unde este necesar

În procese cu impact academic, juridic, profesional, financiar, medical sau similar semnificativ, controlul uman trebuie să fie real, informat și exercitat de o persoană cu autoritate de decizie.

5.5. Transparență

Persoanele trebuie informate atunci când interacționează direct cu un agent IA, dacă acest lucru nu este evident, și atunci când utilizarea IA influențează în mod relevant un proces care le privește.

5.6. Protecția datelor by design

Datele se utilizează numai în mediile autorizate și numai în măsura necesară scopului. Se aplică minimizarea, controlul accesului și regulile privind retenția.

5.7. Verificabilitate și trasabilitate

Procesele IA cu risc mai mare trebuie să permită identificarea instrumentului, versiunii sau configurației relevante, a regulilor de utilizare, a datelor esențiale și a intervențiilor umane relevante.

5.8. Proporționalitate și inovare

Controlul nu trebuie să blocheze experimentarea cu risc redus. Universitatea poate crea sandbox-uri și proiecte-pilot cu date adecvate și limite clare.

5.9. Calitate și critică

Rezultatul IA este tratat ca rezultat probabilistic sau automat, nu ca autoritate epistemică. Sursele, calculele și afirmațiile cu impact trebuie verificate în funcție de risc.

5.10. Accesibilitate și nediscriminare

Sistemele IA nu trebuie să creeze discriminări nejustificate și trebuie evaluate și din perspectiva accesibilității și a impactului asupra grupurilor vulnerabile.

6. Modelul de autonomie proporțională

Nivelul de autonomie se stabilește pentru fiecare proces sau caz de utilizare, nu pentru un instrument în abstract. Același instrument poate funcționa la niveluri diferite în procese diferite.

Nivel	Descriere	Control implicit	Exemple
A0 - Fără IA	Proces executat fără sisteme IA.	Control uman integral.	Evaluări sau activități în care obiectivul este demonstrarea competenței fără asistență IA.
A1 - Asistență	IA propune, explică sau redactează; omul execută sau finalizează.	Revizuire umană înainte de utilizare.	Brainstorming, structurare curs, draft comunicare.

Nivel	Descriere	Control implicit	Exemple
A2 - Delegare	IA execută o activitate; omul validează rezultatul individual sau prin eșantionare, în funcție de risc.	Validare proporțională; escaladare a excepțiilor.	Raport, feedback preliminar, analiză de documente.
A3 - Autonomie operațională	IA execută procesul fără aprobare umană a fiecărui rezultat.	Monitorizare, metrice, loguri, praguri de escaladare și audit.	FAQ, clasificare documente, rutare solicitări, reminder-e, generare de rapoarte standard cu date validate.
Regulă-cheie Nivelul A3 este permis numai dacă activitatea nu produce, prin ea însăși, o decizie semnificativă asupra drepturilor, statutului academic, raportului de muncă, stării de sănătate sau altor interese comparabile ale unei persoane și dacă există mecanisme de detectare și tratare a erorilor.			

7. Clasificarea riscului și impactului

Universitatea utilizează o clasificare internă de risc pentru a decide ce nivel de autonomie este adecvat. Clasificarea internă nu înlocuiește clasificările juridice prevăzute de AI Act.

Clasă	Impact	Exemple	Autonomie uzuală	Aprobare
R1 - redus	Eroare ușor reversibilă; fără date sensibile și fără impact asupra drepturilor.	Brainstorming, rezumare publică, FAQ general.	A1-A3	Conform reguli locale; înregistrare simplificată dacă este integrat.
R2 - moderat	Poate afecta calitatea serviciului sau activități interne, dar consecințele sunt reversibile.	Rapoarte interne, triere solicitări, feedback formativ.	A1-A3 cu controale	Proprietar proces + IT/DPO dacă sunt date personale.
R3 - ridicat	Poate influența în mod relevant o persoană sau un proces academic/HR/financiar.	Preselecție, recomandări privind performanța, evaluări cu impact.	A1-A2; A3 de regulă nepermis	Comitet IA + DPO/juridic/IT, după caz.
R4 - critic / reglementat	Efecte juridice sau similare semnificative, risc pentru sănătate/siguranță/drepturi ori caz juridic high-risk.	Admitere, evaluarea rezultatelor învățării cu efect academic, monitorizare la examene, decizii HR, utilizări clinice relevante.	Control uman obligatoriu; autonomia limitată de lege și de această politică.	Aprobare formală, evaluări de impact și condiții legale aplicabile.

7.1. Criterii de evaluare a riscului

- severitatea consecinței unei erori;
- probabilitatea și detectabilitatea erorii;
- reversibilitatea rezultatului;
- numărul de persoane afectate;
- caracterul personal, sensibil sau confidențial al datelor;
- gradul de autonomie;
- posibilitatea de contestare și remediere;
- dependența utilizatorului de rezultat;
- riscul de discriminare, bias sau excludere;
- riscurile de securitate cibernetică și de furnizor;
- încadrarea juridică a sistemului conform AI Act, GDPR și altor norme aplicabile.

8. Regimul didactic

8.1. Utilizarea IA de către cadrele didactice

Cadrele didactice pot utiliza IA pentru proiectarea, pregătirea, livrarea și îmbunătățirea activităților educaționale. Utilizarea poate varia de la asistență până la automatizarea unor activități repetitive, cu condiția ca rezultatele învățării, integritatea evaluării și responsabilitățile cadrului didactic să fie protejate.

- structurarea cursurilor și seminarelor;
- generarea de exemple, exerciții, cazuri, quiz-uri și materiale formative;
- adaptarea explicațiilor la niveluri diferite de pregătire;
- crearea de tutorare personalizată și trasee de remediare;
- traducerea și adaptarea materialelor;
- generarea și corectarea automată a exercițiilor cu răspuns obiectiv;
- feedback formativ automat sau semi-automat;
- simularea conversațiilor, pacienților sau scenariilor profesionale;
- analiza agregată a dificultăților întâmpinate de cohortă, dacă datele sunt procesate legal și securizat.

Automatizarea nu exonerează cadrul didactic sau structura academică de responsabilitatea pentru designul evaluării, validitatea criteriilor și corectitudinea procesului. Pentru evaluările cu efect academic semnificativ se aplică regulile din secțiunile 8.3 și 12.

8.2. IA ca tutor sau agent educațional

Universitatea poate pune la dispoziția studenților agenți IA pentru tutorare, recapitulare, simulare și feedback. Acești agenți pot opera autonom pentru activități formative cu risc redus, cu respectarea următoarelor condiții:

- studentul este informat că interacționează cu IA;
- agentul nu se prezintă drept profesor, medic sau altă persoană reală;
- limitele sistemului și modalitățile de escaladare către o persoană sunt clare;
- nu se introduc date sensibile în afara mediilor autorizate;
- performanța sistemului este monitorizată și reevaluată periodic.

8.3. Evaluarea academică

Utilizarea IA în evaluare se stabilește la nivelul fiecărei probe sau activități, nu neapărat la nivelul întregii discipline. Cadrul didactic comunică studenților nivelul permis înainte de evaluare, folosind clasificarea D0-D4 din Anexa 2.

IA poate corecta autonom teste sau exerciții obiective dacă baremul este determinist, procesul este validat și există mecanism de contestație. Pentru lucrări deschise, raționament clinic, eseuri, proiecte, performanțe practice sau alte rezultate a căror evaluare implică judecată complexă, IA poate furniza scoruri sau feedback preliminar, dar nota sau decizia cu efect academic se stabilește conform regulilor aprobate și nivelului de risc.

Regulă privind detectoarele de text IA

Un rezultat furnizat de un instrument de detectare a conținutului generat de IA nu constituie, singur, probă suficientă pentru sancționarea unui student. Orice suspiciune se analizează în context, cu respectarea procedurilor de etică, disciplină și a dreptului la apărare.

8.4. Redesignul evaluării

Utilizarea pe scară largă a IA impune adaptarea evaluării. Facultățile sunt încurajate să combine, după caz, produse scrise cu elemente de verificare a competenței reale: susținere orală, demonstrații practice, întrebări de transfer, justificarea surselor, reflecție asupra procesului și verificări în clasă.

9. Regimul administrativ

În activitatea administrativă, principiul de bază este automatizarea activităților delegabile și utilizarea personalului uman pentru excepții, decizii, relații complexe și activități cu valoare ridicată.

9.1. Activități eligibile pentru autonomie operațională A3

- răspunsuri la întrebări frecvente și orientare administrativă generală;
- clasificarea, etichetarea și rutarea documentelor și solicitărilor;
- extragerea de câmpuri din formulare și verificări formale de completitudine;
- programări, notificări și reminder-e;
- generarea de minute/sinteze ale ședințelor în medii autorizate;
- generarea rapoartelor standard pe baza unor date validate;
- transformarea și standardizarea documentelor;
- răspunsuri administrative repetitive pentru care există o bază de cunoștințe aprobată;
- monitorizarea unor termene și escaladarea automată a excepțiilor.

Un proces A3 trebuie să aibă: proprietar desemnat, set de reguli documentat, surse de date autorizate, praguri de escaladare, monitorizare de performanță, canal de corectare și plan de oprire/revenire la proces manual în caz de incident.

9.2. Activități administrative care necesită control uman

- decizii de admitere sau respingere care produc efecte asupra candidatului;
- decizii de sancționare, exmatriculare, acordare/retragere a unor drepturi sau facilități;
- decizii privind angajarea, promovarea, încetarea raporturilor de muncă, salarizarea sau evaluarea profesională cu efect semnificativ;
- decizii financiare individuale cu efect semnificativ;
- decizii bazate pe date sensibile sau profilare, dacă legea ori evaluarea de risc impune intervenție umană;
- orice decizie bazată exclusiv pe prelucrare automatizată care intră sub incidența art. 22 GDPR și nu beneficiază de o excepție legală corespunzătoare.

În aceste situații, persoana care exercită controlul trebuie să aibă competența, informațiile și autoritatea necesare pentru a respinge, modifica sau inversa rezultatul IA, nu doar să îl confirme formal.

10. Medicină, stomatologie și contexte clinice

Având în vedere profilul educațional medical și stomatologic, Universitatea aplică un standard suplimentar de prudență atunci când IA este utilizată cu date medicale, imagistică, cazuri reale sau în activități care pot influența diagnosticul, tratamentul ori siguranța pacientului.

10.1. Utilizări educaționale permise

- simularea pacienților și scenariilor clinice fictive;
- generarea de cazuri educaționale sintetice, etichetate ca atare;
- tutorare și explicații privind concepte medicale;
- antrenarea raționamentului clinic prin comparație între răspunsul studentului și alternative generate de IA;
- feedback formativ asupra structurii prezentării unui caz, fără substituirea evaluării profesionale.

10.2. Date și cazuri reale

Datele reale ale pacienților nu se introduc în servicii IA publice sau neaprobat. Anonimizarea/pseudonimizarea și baza juridică trebuie evaluate în funcție de context. Pentru cercetare, colaborări clinice sau sisteme integrate se aplică suplimentar procedurile de etică, protecția datelor și regulile partenerului clinic.

10.3. Decizie clinică

Niciun student nu poate trata rezultatul unui sistem IA drept substitut pentru supravegherea clinică autorizată. Atunci când IA este utilizată în activități clinice reale, utilizarea se supune normelor medicale, statutului profesional, instrucțiunilor dispozitivului/sistemului și procedurilor instituției medicale competente. Deciziile cu impact asupra pacientului necesită controlul profesionistului autorizat, conform legii și standardelor profesionale aplicabile.

11. Date, confidențialitate și securitate

11.1. Clasificarea datelor pentru utilizarea IA

Clasă date	Exemple	Instrumente permise	Regulă
P0 - Publice	site web, legislație, materiale publicate	Instrumente aprobate; uneori servicii publice, conform instrucțiunilor interne	Fără date confidențiale.
P1 - Interne	proceduri, drafturi, rapoarte fără date personale sensibile	Instrumente instituționale aprobate	Se respectă clasificarea internă și drepturile de acces.
P2 - Personale / confidențiale	date studenți, HR, contracte, date financiare individuale	Numai medii aprobate contractual și tehnic	DPO/IT stabilesc condițiile; minimizare și retenție.
P3 - Sensibile / clinice / critice	date medicale, categorii speciale, credențiale, cercetare confidențială	Numai soluții expres aprobate pentru scopul respectiv	Evaluare juridică/tehnică; controale stricte; poate fi interzisă introducerea în modele externe.

11.2. Reguli obligatorii

- Este interzisă introducerea parolelor, cheilor API, tokenurilor, secretelor de autentificare sau altor credențiale în prompturi ori instrumente IA neautorizate.
- Conturile personale nu se utilizează pentru procesarea datelor instituționale din clasele P2-P3, cu excepția unei aprobări exprese documentate.
- Utilizatorii trebuie să verifice dacă furnizorul utilizează datele pentru antrenarea modelelor, condițiile de retenție, transferurile internaționale și mecanismele de ștergere.
- Integrarea IA cu UMS, CRM, e-mail, cloud, baze de date sau sisteme clinice necesită controlul accesului pe principiul minimului necesar și jurnalizare proporțională.
- Prompturile și rezultatele IA pot constitui date instituționale și se supun politicilor de retenție, confidențialitate și acces aplicabile conținutului lor.

12. Integritate academică și evaluare

Utilizarea IA nu reprezintă automat abatere academică. Caracterul permis sau nepermis depinde de instrucțiunile evaluării, de declararea utilizării și de natura contribuției studentului.

12.1. Situații care pot constitui abatere

- utilizarea IA într-o evaluare declarată D0 sau peste nivelul permis;
- prezentarea ca activitate proprie a unui produs generat substanțial de IA atunci când declararea era obligatorie;
- fabricarea de surse, date, rezultate, citate, cazuri sau experimente;
- utilizarea IA pentru impersonare, fraudarea identității sau eludarea condițiilor examenului;
- utilizarea neautorizată a datelor unei alte persoane în sisteme IA;
- manipularea probelor sau a evidențelor pentru a ascunde o utilizare nepermisă.

12.2. Dovedire și procedură

Sancțiunile se aplică numai prin procedurile instituționale competente. Analiza trebuie să ia în considerare cerințele evaluării, produsul final, explicațiile studentului, sursele și orice alte probe relevante. Nicio estimare algoritmică privind probabilitatea ca un text să fie generat de IA nu este tratată drept probă concludentă în mod izolat.

13. Transparență și informarea persoanelor

- Atunci când un chatbot sau agent IA interacționează direct cu studenți, candidați, angajați sau publicul, utilizatorul este informat că interacționează cu IA, dacă acest lucru nu este evident.
- Conținutul sintetic folosit în comunicare publică se etichetează atunci când legislația sau riscul de inducere în eroare o impune.
- Atunci când IA contribuie material la o decizie sau evaluare cu impact asupra unei persoane, rolul sistemului și posibilitatea de contestare/revizuire umană se comunică în forma adecvată contextului.
- Universitatea evită formulările care induc impresia că un agent IA este o persoană reală sau un profesionist uman atunci când nu este cazul.

Obligațiile concrete de transparență se aplică în conformitate cu art. 50 AI Act și cu celelalte norme relevante, în forma aplicabilă la data utilizării.

14. Achiziția, integrarea și aprobarea sistemelor IA

14.1. Principiul „proces înainte de produs”

Înainte de achiziție, structura solicitantă definește problema, rezultatul dorit, categoria de date, nivelul de autonomie, clasa de risc și indicatorii de succes. Achiziția unui produs nu justifică automat utilizarea sa în orice proces.

14.2. Evaluarea furnizorului și a sistemului

- scop și funcționalități;
- clasificarea juridică posibilă conform AI Act;
- politica de utilizare a datelor pentru antrenare;
- localizarea și transferul datelor;
- subprocesatori;
- autentificare, SSO/MFA și controlul accesului;
- criptare și securitate;
- retenție, ștergere și export;
- jurnalizare și auditabilitate;
- drepturi de proprietate intelectuală asupra intrărilor și rezultatelor;
- capacitatea de a dezactiva anumite funcții sau de a limita datele;
- mecanisme de notificare a incidentelor și modificărilor semnificative;
- portabilitate și strategie de exit;
- cost total și dependență de furnizor (vendor lock-in).

14.3. Pilot și trecere în producție

Sistemele R2-R4 se testează înainte de utilizarea la scară, în măsura în care este fezabil. Pilotul definește datele permise, eșantionul, indicatorii, condițiile de oprire, responsabilul și durată. Trecerea în producție se aprobă pe baza rezultatelor și a avizelor necesare.

14.4. Registrul instituțional IA

Universitatea menține un Registru IA pentru sistemele și cazurile de utilizare instituționale relevante. Înregistrarea include cel puțin: denumire, furnizor, scop, proprietar de proces, nivel de autonomie, clasa de

risc, categoriile de date, utilizatori, integrare, avize, data ultimei evaluări, incidente și statusul (pilot / aprobat / restricționat / suspendat / retras).

15. Guvernanță, roluri și responsabilități

15.1. Senatul Universitar

- aprobă politica și modificările majore;
- primește, după caz, raportări de guvernanță și risc;
- aprobă regulile instituționale care necesită competența Senatului.

15.2. Rectoratul / conducerea executivă

- asigură resursele pentru implementare;
- stabilește structura responsabilă pentru guvernanța IA;
- dispune măsuri corective și priorități de digitalizare.

15.3. Comitetul de Guvernanță IA

Universitatea constituie sau desemnează o structură interdisciplinară pentru guvernanța IA. Componenta recomandată include reprezentanți ai conducerii academice, IT/securitate, DPO, juridic/conformitate, calitate, etică, cadre didactice și, după caz, studenți și experți externi.

- menține metodologia de risc și Registrul IA;
- analizează utilizările R3-R4 și excepțiile;
- emite standarde și ghiduri;
- monitorizează incidentele și performanța;
- propune suspendarea sau retragerea sistemelor;
- coordonează programul de alfabetizare IA;
- actualizează politica pe baza schimbărilor legislative și tehnologice.

15.4. DPO, IT și juridic

DPO evaluează implicațiile privind protecția datelor; IT/securitate evaluează arhitectura, accesul, integrarea și riscurile tehnice; juridicul/conformitatea evaluează obligațiile contractuale și normative. Aceste funcții pot stabili condiții obligatorii de utilizare în aria lor de competență.

15.5. Proprietarul de proces

- definește scopul și regulile procesului;
- stabilește metricile și pragurile de escaladare;
- asigură existența unui canal pentru corectarea erorilor;
- revizuieste performanța și decide continuarea, modificarea sau oprirea procesului;
- raportează incidentele conform procedurii.

15.6. Utilizatorii

Utilizatorii respectă clasificarea datelor, nivelul de autonomie aprobat, condițiile instrumentului și obligațiile de raportare. Utilizarea unui instrument neaprobat nu este permisă pentru date sau procese pentru care politica cere aprobare.

16. Monitorizare, audit și managementul incidentelor

16.1. Monitorizare

Procesele A2-A3 și sistemele R2-R4 sunt monitorizate proporțional. Indicatorii pot include: acuratețe, rată de eroare, rată de escaladare, timp de răspuns, cost per activitate, satisfacția utilizatorilor, incidente, diferențe între grupuri, disponibilitate și drift al performanței.

16.2. Audit

Auditul poate utiliza eșantionare și nu presupune verificarea fiecărui rezultat. Frecvența este stabilită în funcție de risc. Pentru procesele A3 trebuie să existe suficiente evidențe pentru a reconstrui modul de funcționare și a identifica tiparele de eroare, cu respectarea minimizării datelor.

16.3. Incidente

- scurgerea sau introducerea neautorizată de date;
- rezultat discriminatoriu sau sistematic incorect;
- decizie sau recomandare cu impact semnificativ eronată;
- încălcarea regulilor de transparență;
- utilizarea neautorizată a unui sistem;
- compromiterea contului, cheilor sau integrărilor;
- comportament imprevizibil care poate produce prejudicii;
- încălcări privind proprietatea intelectuală sau confidențialitatea.

În funcție de gravitate, răspunsul poate include: oprirea temporară, retragerea accesului, izolarea integrării, informarea DPO/IT/juridic, notificări legale, corectarea datelor, comunicarea către persoanele afectate, revalidare și reluare controlată.

17. Nerespectarea politicii

Nerespectarea prezentei politici se analizează conform statutului persoanei și reglementărilor instituționale aplicabile: regulamente studențești, codul de etică și deontologie, regulament intern, contracte, proceduri de securitate și legislația în vigoare.

Măsurile trebuie să fie proporționale cu gravitatea, intenția, impactul și caracterul repetitiv al faptei. Erorile de bună-credință se tratează distinct de fraudă, exfiltrare deliberată de date, eludarea controalelor sau alte conduite intenționate.

18. Formare și alfabetizare IA

Universitatea implementează un program de alfabetizare IA adaptat rolului, experienței, contextului și persoanelor asupra cărora sistemele sunt utilizate. Programul susține obligațiile instituției ca implementator de sisteme IA și cultura internă de utilizare competentă.

18.1. Nivel minim pentru întreg personalul

- ce poate și ce nu poate face IA;
- halucinații și limite;
- protecția datelor și clasificarea P0-P3;
- reguli privind sursele și drepturile de autor;
- securitate și phishing bazat pe IA;
- când este obligatorie escaladarea către o persoană.

18.2. Formare avansată

Cadrele didactice, personalul IT, DPO, juridic, managementul și proprietarii de procese primesc formare suplimentară relevantă rolului: design de evaluare, audit, bias, prompt/instruction design, securitate, achiziții, monitorizare, analiză de impact și managementul incidentelor.

19. Implementare și dispoziții tranzitorii

După aprobarea politicii, implementarea se realizează etapizat. Termenele de mai jos sunt recomandate și pot fi ajustate prin hotărârea de aprobare sau planul executiv de implementare.

Termen de la intrarea în vigoare	Acțiune	Responsabil principal
30 zile	Desemnarea Comitetului/structurii de guvernanță IA și a responsabililor.	Rectorat
60 zile	Inventarierea sistemelor și cazurilor de utilizare existente; identificarea Shadow AI relevant.	Comitet IA + structuri
90 zile	Registrul IA, lista instrumentelor aprobate/restricționate și clasificarea datelor.	Comitet IA + DPO + IT
120 zile	Programul minim de alfabetizare IA pentru personal.	HR / Comitet IA
Semestrul următor	Introducerea nivelurilor D0-D4 în cerințele de evaluare și ghidurile studenților.	Facultăți / cadre didactice
Permanent	Pilotare, automatizare, audit și revizuire pe baza riscului și valorii obținute.	Proprietari de procese

20. Revizuire și intrare în vigoare

Politica se revizuieste cel puțin anual, precum și ori de câte ori apar modificări legislative sau tehnologice semnificative, incidente relevante, modificări ale profilului instituțional de risc sau constatări de audit care impun schimbări.

Prezenta politică intră în vigoare la data stabilită prin hotărârea Senatului Universitar. Anexele fac parte integrantă din politică, iar formularele operaționale pot fi actualizate administrativ dacă nu modifică principiile, drepturile și obligațiile de fond stabilite prin prezentul document.

Anexa 1. Matrice risc - autonomie

Matricea este un instrument de decizie internă. Ea nu substituie analiza juridică specifică.

Risc / autonomie	A0	A1	A2	A3
R1 - redus	Permis	Permis	Permis	Permis, cu monitorizare de bază
R2 - moderat	Permis	Permis	Permis	Permis cu metrice, audit și escaladare
R3 - ridicat	Permis	Permis	Permis cu validare/oversight	În principiu nepermis; excepție formal aprobată dacă legea permite

Risc / autonomie	A0	A1	A2	A3
R4 - critic/reglementat	Permis	Permis dacă nu afectează cerința legală	Numai cu control uman și cerințe legale	Nepermis pentru decizie autonomă cu impact semnificativ, cu excepția cazurilor expres permise de lege și aprobate instituțional

Anexa 2. Niveluri de utilizare IA în evaluarea studenților

Nivel	Ce este permis	Obligația studentului	Exemplu
D0 - fără IA	Nicio utilizare IA pentru activitatea evaluată, cu excepțiile tehnice expres precizate.	Respectă condițiile probei.	Examen în sală, demonstrarea cunoștințelor fără asistență.
D1 - suport tehnic	Corectură, ortografie, formatare, traducere limitată dacă este permisă.	Nu delegă raționamentul sau conținutul substanțial.	Corectarea limbii unui text propriu.
D2 - tutorare și brainstorming	Explicații, întrebări, brainstorming, structurare, feedback.	Produsul final și raționamentul rămân ale studentului.	Plan pentru eseu, explicații suplimentare.
D3 - co-creare declarată	IA poate genera sau transforma părți substanțiale.	Declară instrumentul, scopul și modul de verificare; respectă cerințele temei.	Proiect cu analiză asistată de IA.
D4 - IA integrată în evaluare	Utilizarea IA este parte a obiectivului evaluării.	Documentează procesul și demonstrează capacitatea de validare critică.	Critica unui răspuns IA, agent clinic simulat, workflow automatizat.

Nivelul se menționează în cerința probei. În lipsa unei mențiuni explicite, cadrul didactic clarifică nivelul înainte de termenul de predare; nu se recomandă sancționarea retroactivă pe baza unei reguli necomunicate.

Anexa 3. Declarație de utilizare IA

Model standard pentru studenți / autori

Pentru realizarea acestei lucrări am utilizat [denumirea instrumentului/sistemului IA] pentru [scop: brainstorming, structurare, analiză, redactare, traducere, cod etc.]. Am verificat și, după caz, am modificat rezultatele generate. Îmi asum responsabilitatea pentru conținutul final și pentru respectarea cerințelor evaluării, a regulilor de citare și a integrității academice.

Cadrul didactic poate solicita, atunci când este relevant pentru obiectivele evaluării, o descriere scurtă a procesului, prompturilor reprezentative sau etapelor de verificare. Nu se solicită în mod implicit divulgarea datelor personale, a informațiilor confidențiale ori a întregului istoric de conversație.

Anexa 4. Fișa de înregistrare a unui sistem IA

Denumirea sistemului / furnizor	
Scop și proces	
Structura responsabilă	

Proprietar de proces	
Utilizatori	
Nivel autonomie A0-A3	
Clasă risc R1-R4	
Clasificare date P0-P3	
Integrații / sisteme conectate	
Bază juridică / DPIA / FRIA, după caz	
Măsuri de transparență	
Măsuri de supraveghere și escaladare	
Metrici și frecvența auditului	
Retenție / loguri	
Status: pilot / aprobat / restricționat / suspendat / retras	
Data ultimei revizuirii	

Anexa 5. Checklist de evaluare înainte de achiziție / implementare

- ☐ Problema și rezultatul dorit sunt definite independent de produs.
- ☐ Nivelul de autonomie și clasa de risc sunt stabilite.
- ☐ Este clar ce categorii de date intră în sistem.
- ☐ Este stabilit dacă furnizorul folosește datele pentru antrenare și dacă această opțiune poate fi dezactivată.
- ☐ Sunt analizate retenția, localizarea și transferurile datelor.
- ☐ Sunt verificați subprocesatorii și termenii contractuali.
- ☐ Sunt disponibile control de acces, MFA/SSO și loguri adecvate.
- ☐ Există un plan de testare și criterii de acceptare.
- ☐ Există mecanism de escaladare și contestare pentru persoanele afectate, dacă este cazul.
- ☐ Este stabilit cine poate opri sistemul și în ce condiții.
- ☐ Au fost evaluate bias-ul, accesibilitatea și impactul asupra grupurilor afectate.
- ☐ Sunt clarificate drepturile asupra datelor, prompturilor și outputurilor.
- ☐ Există plan de exit/export și evitarea dependenței excesive de furnizor.
- ☐ DPO, IT/securitate și juridic au fost implicați conform clasei de risc.
- ☐ Sistemul este înscris în Registrul IA înainte de utilizarea operațională, dacă politica o cere.

Anexa 6. Raportarea incidentelor IA

Data și ora	
Sistem / caz de utilizare	
Persoana care raportează	
Descrierea incidentului	
Date implicate	
Persoane potențial afectate	
Impact real / potențial	
Acțiune imediată întreprinsă	
Sistemul a fost suspendat?	
DPO / IT / juridic notificați?	
Măsuri de remediere	
Decizia de reluare / retragere	
Lecții învățate și schimbări de control	

Anexa 7. Exemple de utilizări permise, condiționate și interzise

Caz de utilizare	Regim orientativ	Condiții principale	Observație
Generare idei pentru curs	Permis	Fără date sensibile; profesorul adaptează materialul.	A1 / R1
FAQ secretariat pe baza procedurilor publice	Permis autonom	Informare că este IA; bază de cunoștințe aprobată; escaladare.	A3 / R1-R2
Clasificare automată a solicitărilor	Permis autonom	Monitorizare și corectarea rutării greșite.	A3 / R2
Corectare automată quiz cu răspuns fix	Permis	Barem validat; mecanism de contestație.	A2-A3 / R2
Feedback formativ pe eseu	Permis condiționat	Student informat; nu devine automat nota finală.	A2 / R2-R3
Notă finală la eseu stabilită exclusiv de LLM	Nepermis ca regulă	Necesită control uman real și analiză juridică/risc.	R4 / posibil high-risk
Admitere / respingere automată	Nepermis ca decizie autonomă	Poate exista suport IA, dar decizia trebuie să respecte cerințele legale și controlul aplicabil.	R4 / posibil high-risk

Caz de utilizare	Regim orientativ	Condiții principale	Observație
Monitorizarea comportamentului la examene cu IA	Restricționat	Evaluare juridică, proporționalitate, transparență, cerințe high-risk.	R4
Încărcarea unei baze cu date medicale într-un cont public de IA	Interzis	Se utilizează doar medii expres aprobate.	P3
Simulare pacient fictiv pentru studenți	Permis	Clar marcat ca simulare; nu este sfat medical real.	A3 / R1-R2
Preselecția CV-urilor cu IA	Restricționat	Evaluare juridică și de risc; control uman; reguli AI Act/HR.	R4
Proces verbal automat din ședință internă	Permis condiționat	Instrument aprobat; participanții informați; protecția datelor.	A2-A3 / R2

Referințe normative și documentare

Lista de mai jos reflectă sursele oficiale consultate la elaborarea versiunii 1.0. Politica trebuie menținută în concordanță cu forma în vigoare a actelor normative.

1. Regulamentul (UE) 2024/1689 privind inteligența artificială - text consolidat la 27 iulie 2026 (EUR-Lex). [Sursa oficială](#)
2. Regulamentul (UE) 2026/1744 - Digital Omnibus on AI, modificarea Regulamentului (UE) 2024/1689 (EUR-Lex). [Sursa oficială](#)
3. Comisia Europeană - cadrul de reglementare AI Act și calendarul de aplicare, actualizat în 2026. [Sursa oficială](#)
4. Comisia Europeană - AI Act enforcement framework, inclusiv aplicarea regulilor pentru sistemele high-risk din Anexa III de la 2 decembrie 2027. [Sursa oficială](#)
5. Comisia Europeană - AI literacy / Articolul 4 și practici de alfabetizare IA. [Sursa oficială](#)
6. Regulamentul (UE) 2016/679 (GDPR), inclusiv art. 22 privind procesul decizional individual automatizat (EUR-Lex). [Sursa oficială](#)
7. European Data Protection Board - Avizul 28/2024 privind anumite aspecte ale protecției datelor în contextul modelelor IA. [Sursa oficială](#)
8. Legea învățământului superior nr. 199/2023, cu modificările și completările ulterioare. [Sursa oficială](#)
9. H.G. nr. 305/2024 - Codul-cadru de etică și deontologie universitară. [Sursa oficială](#)
10. Ordinul nr. 6.869/2024 - Regulamentul-cadru privind organizarea și funcționarea comisiilor de etică universitară, în forma consolidată. [Sursa oficială](#)

Notă de conformitate

Versiunea 1.0 a fost redactată având în vedere cadrul normativ disponibil la data de 14 septembrie 2026. În special, regulile AI Act privind sistemele high-risk din Anexa III - inclusiv anumite utilizări din educație și ocuparea forței de muncă - au un calendar de aplicare distinct. Universitatea aplică însă din prezent un standard intern de guvernare pregătit, pentru a evita implementarea unor sisteme care ar necesita ulterior re proiectare sau retragere.

Înainte de aprobarea finală, se recomandă avizarea documentului de către responsabilul cu protecția datelor, juridic/conformitate, IT/securitate și Comisia de Etică Universitară, precum și corelarea cu Carta Universității, Codul de etică, regulamentele de studii, procedurile de evaluare și politicile de securitate existente.

PREȘEDINTE SENAT

RECTOR

DATA

