ARTIFICIAL INTELLIGENCE RISK ASSESSMENT GUIDE

Institutional guidance for the preliminary review, risk scoring, control, decision, and review of artificial intelligence applications

Version	01
Publication Date	29 June 2026
Comments and Contact	AI Competency Unit
Document Coordination	AI Competency Unit
Technical and Legal Review	IT Directorate and Office of Legal Counsel

How to Use This Guide

This Guide explains when artificial intelligence tools, embedded AI features, and AI-supported use cases used or planned for use at Bahçeşehir University are subject to institutional assessment and how the Risk Assessment Form in Annex 1 is to be applied.

The full form is not required for routine low-risk use

Routine uses that involve publicly available information or information containing no personal data, do not make decisions about individuals, do not perform transactions in institutional systems, and produce outputs that can be readily checked shall be conducted under the relevant user guides. A separate full risk assessment is not required for such uses.

Assessment Workflow

Step	Responsible Party	Output
1. Preliminary notification	Requesting unit / application owner	Purpose of use, need, target users, and expected benefit
2. Preliminary classification	Requesting unit and AI Competency Unit	Preliminary risk level: low, controlled, high, or unacceptable
3. Risk scoring	Assessment team	Likelihood and impact scores for individual risks, together with the control plan
4. Expert review	IT Directorate, Office of Legal Counsel, and relevant expert units	Technical, legal, data-protection, ethical, pedagogical, or other opinions
5. Decision	Authorised unit or body according to the risk level	Decision on use, pilot, revision, temporary suspension, or rejection
6. Recording and monitoring	AI Competency Unit and application owner	Inventory record, monitoring method, and review date

Table of Contents

1. Purpose and Status of the Document

The purpose of this Guide is to establish a common method for systematically identifying, assessing, scoring, and deciding upon the risks of an artificial intelligence tool, an embedded AI feature, or an AI-supported use case before it is placed into institutional use at Bahçeşehir University.

This Guide and the Artificial Intelligence Risk Assessment Form in Annex 1 constitute the implementation instrument for the Artificial Intelligence Risk Assessment Template referred to in the Responsible Artificial Intelligence Implementation Procedures and Principles.

The Guide shall be applied together with the Bahçeşehir University Artificial Intelligence Policy, the Responsible Artificial Intelligence Implementation Procedures and Principles, the Artificial Intelligence Steering Committee Working Procedures and Principles, and other University regulations on personal data protection, information security, academic integrity, scientific ethics, and intellectual property rights.

2. Scope and Assessment Threshold

2.1. Cases in Which the Guide Applies

This Guide applies in the following cases:

- AI tools and systems that the University plans to purchase, license, develop, or make available for institutional use;
- Embedded AI features subsequently added to purchased or existing software;
- AI applications that will provide services to students, staff, researchers, alumni, external stakeholders, or the public;
- Applications that use institutional data, personal data, or non-public information;
- Applications integrated with the University's information systems, data sources, agents, connectors, or automations;
- Use cases that support academic, administrative, financial, or managerial decisions or may affect individuals;
- A material change to the purpose, data scope, user group, vendor, model, integration, or transaction authority of an approved application;
- Controlled- and high-risk applications that require reassessment under the review schedule.

2.2. Uses Not Requiring a Full Assessment

A separate full risk assessment is not required for routine low-risk uses. Nevertheless, the requirements concerning approved tools, data security, output verification, human responsibility, and the relevant user guides shall apply.

Technical availability does not mean institutional suitability
The fact that an AI feature is visible or available within software does not mean that its use is automatically approved, that the required licence is in place, or that data may be processed through that system.

3. Key Concepts

Application owner	The unit or person institutionally responsible for the purpose, scope, controls, human oversight, monitoring, and reporting of material changes relating to the AI application.
Institutional AI Inventory	The central register maintained and updated by the AI Competency Unit, containing ownership, purpose, data used, risk level, assessment decision, and review information for AI tools and use cases used, developed, assessed, piloted, or planned at the University.
Institutional risk level	The low, controlled, high, or unacceptable level assigned to the application as a whole, taking into account its purpose, the persons and groups affected, the data used, the system's level of autonomy, and its potential consequences.
Individual risk score	The score obtained by multiplying the likelihood and impact ratings of a specific risk, used to prioritise that risk and prepare the control plan.
Material change	A change in the purpose of use, user group, data source, model, vendor, integration, transaction authority, scale, or security conditions that may affect the previous assessment.

4. Assessment Process and Responsibilities

4.1. Requesting Unit and Application Owner

- Describe the need to be addressed, the purpose of use, target users, and expected institutional benefit.

- Ensure the accuracy of the information and documents in the Form and report the risks and existing controls.
- Implement the approved controls, limits, and conditions and ensure human oversight.
- Report material changes, errors, incidents, and unexpected effects without delay.

4.2. AI Competency Unit

- Coordinate the application, preliminary review, and risk-classification process.
- Ensure that the necessary expert opinions are obtained and monitor assessment records.
- Record controlled- and high-risk applications in the Institutional AI Inventory from the assessment stage onward.
- Prepare high-risk or strategic applications for the agenda of the Artificial Intelligence Steering Committee.

4.3. Expert Units and Authorised Bodies

Depending on the nature of the application, the IT Directorate, the Office of Legal Counsel, and the relevant academic or administrative units shall provide opinions on information security, technical architecture, personal data protection, contracts, ethics, academic integrity, assessment and evaluation, intellectual property rights, procurement, licensing, and accessibility.

Where a decision of the Senate, Rectorate, an ethics committee, a disciplinary body, a procurement authority, or another authorised body is required under applicable legislation or University regulations, the assessment conducted under this Guide does not replace that decision.

5. Institutional Risk Levels

Level	Core criterion	Illustrative use	Minimum process
Level 1: Low risk	Publicly available information or information containing no personal data; no decisions about individuals; no transactions in institutional systems; outputs are readily verifiable.	Ideation, first drafts, summaries of public text, language improvement, and coding with sample data.	The full form is not required; user guides and general controls apply.
Level 2: Controlled risk	Service to a specific course, unit, or user group; internal content; direct interaction with users; limited but meaningful impact.	Course assistant, internal document assistant, or student-service assistant that does not evaluate individuals.	Preliminary assessment, application owner, data and access boundaries, pilot, and periodic monitoring.
Level 3: High risk	Special categories or large-scale personal data; profiling or prediction; effects on academic or working life; health; biometrics; transaction authority; or serious impact.	Decision support for grades, scholarships, or progression; recruitment or performance support; health or psychological-support data; or an agent that performs transactions in an institutional system.	Full assessment, expert opinions, documented human oversight, controlled pilot, and Committee assessment.
Level 4: Unacceptable use	Complete delegation of the final human decision to AI; unauthorised emotion or personality inference; unauthorised surveillance; fabrication of data or evidence; circumvention of security controls; or merely nominal human oversight.	It may not be placed into institutional use. Research-only examination may be assessed separately, provided it is not used on real persons and the required approvals are obtained.	The process is stopped; the scope is redesigned or the request is rejected.

6. Risk Scoring and Interpretation

In Annex 1, likelihood and impact are rated from 1 to 5 for each individual risk. The risk score is calculated by multiplying the likelihood and impact ratings. Scoring is used to prioritise risks, identify additional controls, and monitor residual risk after mitigation.

The institutional risk level and the individual risk score are not the same

An individual risk score does not reduce the application's overall risk level. Where the application has a high-risk or unacceptable-risk trigger, the corresponding higher level applies even if the numerical score is lower.

7. Decision, Recording, and Review

One of the following decisions shall be made as a result of the assessment:

- Suitable for use,
- Suitable for use subject to specified conditions,
- Suitable for a pilot application,
- Additional information or revision required,
- Temporarily unsuitable,
- Unsuitable for use.

The decision shall specify the application owner, scope of use, required controls, permitted data and user boundaries, monitoring method, suspension conditions, and review date.

Controlled- and high-risk applications shall be entered in the Institutional AI Inventory from the assessment stage onward. The inventory record number in the Form shall be completed by the AI Competency Unit after the assessment is finalised.

The application shall be reassessed where there is a material change in its purpose, user group, data source, model or service provider, integration, transaction authority, scale of use, security conditions, or contractual conditions.

8. Review and Document Management

AI applications placed into use shall be monitored in proportion to their risk levels. Monitoring periods, responsible parties, and expected outputs shall be specified in the Artificial Intelligence Review and Monitoring Calendar.

This Guide shall be reviewed at least annually, taking into account technological developments, legislative changes, implementation experience, risk and incident records, user feedback, and changes to the University's Artificial Intelligence Policy and Roadmap.

ANNEX 1

ARTIFICIAL INTELLIGENCE RISK ASSESSMENT FORM

Application-level record of risks, controls, decisions, and review

Completion sequence

Section A defines the application and use case; Section B determines the preliminary risk level; Sections C and D score individual risks and establish the control plan; Section E completes the data-protection screening; and Sections F and G conclude the decision, recording, and approval process.

Section A - General Information

Assessment No.	[AIR-YYYY-###]
Date	[DD.MM.YYYY]
Requesting Unit	[Unit name]
Application Owner	[Unit / Name and Surname / Title]
Assessor(s)	[Name and Surname / Title]
Tool / Use-Case Name	[Name]
Vendor and Version / Plan	[Vendor, version, or subscription plan]
Subject Type	☐ New tool ☐ Embedded AI feature ☐ Use case ☐ Change ☐ Periodic review
Need to Be Addressed	[Current problem, need, or opportunity]
Purpose and Scope of Use	[Purpose, scope, and expected output of the tool or use case]
Expected Institutional Benefit	[Education, research, service, efficiency, quality, or other benefit]
Success Measures	[Indicators by which the application will be considered successful]
Target Users	☐ Academic staff ☐ Administrative staff ☐ Researchers ☐ Students ☐ External stakeholders ☐ Public
Affected Groups	☐ Students ☐ Staff ☐ Patients ☐ Applicants ☐ Research participants ☐ Public ☐ Other: _____
Nature of the Information or Data to Be Used	☐ Public / low-risk ☐ Internal / controlled ☐ Personal data ☐ Special categories of personal data ☐ Confidential / restricted institutional information ☐ Research data ☐ Intellectual property ☐ Third-party information protected by contract ☐ Security or access information ☐ No data will be used ☐ Other: _____
Data-Processing Location	☐ Türkiye ☐ Abroad ☐ Unknown / to be confirmed
Use of Data for Model Training	☐ Contractually excluded ☐ Can be disabled in settings ☐ Cannot be prevented ☐ Unknown
System Function / Level of Autonomy	☐ Drafting or content support ☐ Recommendation ☐ Decision support ☐ Automated transaction / action
Current Status	☐ Concept / preliminary review ☐ Pilot ☐ Production use ☐ Change assessment ☐ Periodic review

Section B - Preliminary Classification

B.1. Unacceptable-Use Check

If any of the following is marked, the scope of use shall be redesigned or the request rejected. Research-only examination may be assessed separately, provided it is not used on real persons and the necessary ethical, legal, and security approvals are obtained.

Unacceptable use	Mark
Complete delegation to an AI system of final decisions that materially affect individuals, such as grading, admission, scholarships, discipline, recruitment, performance, promotion, or termination of employment.	☐
Creation of a general trustworthiness, value, suitability, or behaviour score for individuals.	☐
Unauthorised inference of individuals' emotions, personality, or sensitive characteristics in educational or workplace settings and use of such inferences in decision-making.	☐
Unauthorised biometric monitoring, mass surveillance, or manipulation of behaviour by exploiting individuals' vulnerabilities.	☐
Processing personal, confidential, or non-public institutional data through AI systems without the required assessment and authorisation.	☐
Fabrication of data, sources, citations, evidence, identities, or official records through AI, or circumvention of security controls.	☐
A decision process in which human oversight is merely nominal and AI output is applied without challenge.	☐

B.2. High-Risk Indicators

If any of the following questions is answered "Yes", the application shall, as a rule, be classified as high risk and Sections C-E shall be completed in full. The final classification shall be based on the specific use case.

Question	Yes	No
Does it affect decisions concerning assessment and evaluation, admission, scholarships, academic progression, discipline, or access to services?	☐	☐
Does it affect recruitment, assignment, performance, promotion, or the employment relationship?	☐	☐
Does it involve data or processes relating to health, psychological counselling, or special support needs?	☐	☐
Does it process special categories of personal data or personal data on a large scale or in a systematic manner?	☐	☐
Does it generate profiles, predictions, classifications, or risk assessments concerning individuals?	☐	☐
Does it use biometric data, identity verification, or behaviour-monitoring functions?	☐	☐
Does it have authority to create, modify, or delete records or perform transactions in institutional information systems?	☐	☐
Could an erroneous output have a significant effect on individuals' rights or on the University's legal, financial, academic, security, or reputational position?	☐	☐
Is the output difficult to verify or explain independently?	☐	☐

B.3. Preliminary Risk-Level Result

Risk level	Criterion and applicable process
☐ Level 4 - Unacceptable use	At least one item in B.1 is marked. The scope of use shall be redesigned or the request rejected; the justification shall be recorded in Section F.

Risk level	Criterion and applicable process
☐ Level 3 - High risk	A high-risk indicator is present in B.2. A full assessment, relevant expert opinions, a controlled pilot, documented human oversight, and, where required, Committee assessment shall apply.
☐ Level 2 - Controlled risk	The application serves a specific course, unit, or user group; uses an internal source; involves direct interaction, an agent or integration, or a limited but meaningful impact. Preliminary assessment, ownership, data and access boundaries, a pilot, and periodic monitoring shall apply.
☐ Level 1 - Low risk	Only publicly available information or information containing no personal data is used; no decisions are made about individuals; no transactions are performed in institutional systems; and outputs are readily verifiable. As a rule, a full assessment is not required.

Section C - Scoring Scales and Risk Matrix

Scoring note
The scores in this Section are used to prioritise individual risk findings. An individual risk score does not reduce the application's overall risk level determined in B.3.

C.1. Likelihood Scale

Score	Level	Description
1	Rare	May occur only in exceptional circumstances.
2	Low	Unlikely to occur; few known instances exist.
3	Moderate	May reasonably occur during normal use.
4	High	Expected to occur in many use situations.
5	Almost certain	Unavoidable during normal use unless measures are taken.

C.2. Impact Scale

Score	Level	Description
1	Very low	Negligible impact; no personal data; minor and readily reversible internal efficiency effect.
2	Low	Limited, local, and readily remediable impact; no significant consequence for rights, security, or services.
3	Moderate	Unit-level disruption; adverse effect on a limited number of persons; meaningful service, learning, or reputational impact.
4	High	Possible personal data breach; loss of rights for individuals; significant academic, legal, financial, security, or reputational impact.
5	Critical	Breach involving special categories or large-scale data; serious consequences for individuals; severe legal, security, accreditation, or business-continuity impact.

C.3. Risk Matrix (Score = Likelihood x Impact)

Impact \ Likelihood	1	2	3	4	5
5 - Critical	5	10	15	20	25
4 - High	4	8	12	16	20

Impact \ Likelihood	1	2	3	4	5
3 - Moderate	3	6	9	12	15
2 - Low	2	4	6	8	10
1 - Very low	1	2	3	4	5

C.4. Individual Risk Bands and Required Actions

Score	Level	Required action
1–4	Low	Acceptable. Existing controls shall be maintained and recorded.
5–9	Moderate	Acceptable with additional controls. Measures and responsible parties shall be identified.
10–15	High	A risk-mitigation plan is mandatory. Review by the relevant expert unit and a conditional decision are required.
16–25	Very high	Unacceptable individual risk. The use shall be redesigned; residual risk may not remain in this band.

Section D - Risk Register

The register below is pre-populated with common risk categories. Rows that do not apply shall be marked "N/A", and use-case-specific risks shall be added. L = Likelihood, I = Impact; Residual = the expected score after controls.

No.	Risk description	L	I	Score	Existing controls and additional measures	Owner / Due date	Residual
1	Unauthorised entry of personal, confidential, or restricted information into the tool						
2	Use of erroneous or fabricated output without verification						
3	Unfair or discriminatory assessment resulting from biased output						
4	Human oversight being insufficient or merely nominal						
5	Facilitation of academic-integrity violations						
6	Failure to provide the required AI disclosure or labelling						
7	Input or output that infringes copyright, licence terms, or intellectual property rights						
8	Account compromise, data leakage, phishing, or unauthorised access						
9	Service interruption and excessive vendor dependency						
10	Insufficient contractual safeguards for data processing, retention, or transfer						

No.	Risk description	L	I	Score	Existing controls and additional measures	Owner / Due date	Residual
11	Institutional reputational damage arising from inappropriate or synthetic content						
12	Student-facing use conflicting with the rules applicable to students						
13	[Use-case-specific risk]						
14	[Use-case-specific risk]						

Section E - Personal Data Protection and Data-Security Screening

If any question is answered "Yes", the use case shall be assessed, according to its nature, by the Office of Legal Counsel, the IT Directorate, and the University's relevant data-protection processes. Where personal data are processed, the legal basis, purpose limitation, data minimisation, retention, transfer, security measures, and required information processes shall also be examined.

Question	Yes	No	Explanation / Evidence
Will personal data be processed?	☐	☐	
Will special categories of personal data be processed?	☐	☐	
Will data relating to persons under the age of 18 be processed?	☐	☐	
Will data be transferred abroad?	☐	☐	
Is there profiling or automated assessment of individuals?	☐	☐	
Does it require a new data-collection activity?	☐	☐	
Do privacy notices or data-processing records need to be updated?	☐	☐	
Is there uncertainty concerning retention, deletion, subprocessors, or model-training conditions?	☐	☐	

Section F - Assessment Outcome and Decision

Final Institutional Risk Level	☐ Level 1 - Low ☐ Level 2 - Controlled ☐ Level 3 - High ☐ Level 4 - Unacceptable use
Highest Individual Risk Score	Initial score: _____ Residual score: _____
Decision	☐ Suitable for use ☐ Suitable subject to specified conditions ☐ Suitable for a pilot application ☐ Additional information or revision required ☐ Temporarily unsuitable ☐ Unsuitable for use
Conditions / Justification	[Decision conditions, grounds for rejection, or revisions to be completed]
Approved Scope of Use	[Purpose, user group, permitted functions]
Data and Access Boundaries	[Permitted data types, sources, and access groups]
Mandatory Controls	[Human oversight, technical, legal, pedagogical, or other controls]

Monitoring Indicators and Suspension Conditions	[Performance, error, complaint, data, and security indicators]
Institutional AI Inventory Record No.	[To be completed by the AI Competency Unit after the assessment is finalised.]
First Review Date	[According to the Artificial Intelligence Review and Monitoring Calendar]

Section G - Opinions, Approval, and Signatures

Signatures and opinions shall be completed according to the application's risk level and nature. Rows that do not apply may be marked "N/A".

Role	Name and Surname / Title	Opinion / Decision	Date	Signature
Requesting Unit Manager				
Application Owner				
AI Competency Unit				
IT Directorate (where required)				
Office of Legal Counsel / relevant data-protection process (where required)				
Academic, ethical, pedagogical, or other expert opinion (where required)				
Artificial Intelligence Steering Committee / Authorised Approval Authority (where required)				

Authorised bodies and authorities

This assessment does not replace decisions required from the Senate, Rectorate, ethics committee, disciplinary body, procurement authority, or other authorised bodies and authorities under applicable legislation or University regulations.

Methodological References

1. Bahçeşehir University Artificial Intelligence Policy.
2. Bahçeşehir University Responsible Artificial Intelligence Implementation Procedures and Principles.
3. European Union Artificial Intelligence Act (Regulation (EU) 2024/1689) - risk-based approach and high-risk use areas.
4. Turkish Personal Data Protection Authority - Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence (2021) and the Guide on Generative Artificial Intelligence and the Protection of Personal Data (2025).
5. Council of Higher Education - Ethical Guide on the Use of Generative Artificial Intelligence (2024).
6. ISO/IEC 23894:2023 – Artificial Intelligence: Guidance on Risk Management.
7. ISO/IEC 42001:2023 – Artificial Intelligence Management Systems.
8. NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0, 2023).