



AMERICAN
UNIVERSITY
OF BEIRUT

GUIDELINES FOR THE RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE (AI)

Version Number:	0000
Document Category:	
Document Owner:	Name
Implementation Office(s):	Name
Last Review Date:	DD/MM/YY
Next Review Date:	DD/MM/YY

TABLE OF CONTENTS

I.	Disclosure Note	3
II.	Purpose	3
III.	Definitions	3
IV.	Before Using AI	4
V.	Principles.....	4
VI.	Transparency and Disclosure and Documentation	5
VII.	Data-Centric Governance.....	7
VIII.	AUB-Approved AI Tools	7
IX.	Prohibited Uses	8
X.	Unit heads Responsibilities	9
XI.	Relationship to existing policies	9

I. DISCLOSURE NOTE

This document was developed by AUB subject matter experts. Generative AI was used solely for structuring, editing, and language refinement. The framework, principles, and guidance reflect human judgment and have been fully reviewed and validated by AUB.

II. PURPOSE

- (A) This document provides institution-wide guidance for the responsible, secure, ethical, and transparent use of Artificial Intelligence (AI) and generative AI tools at the American University of Beirut (AUB), particularly from a data governance, tools, operational risk, and responsible use perspective.
- (B) It applies to anyone using AI in connection with university work, including teaching and learning support, research administration, service, clinical, administrative, and operational activities. It is intended to help AUB users adopt AI responsibly while protecting institutional, personal, and regulated data.
- (C) It is intended to:
 - 1. Enable innovation, productivity, and operational efficiency across teaching, research, clinical, and administrative functions.
 - 2. Provide clear guidance to faculty and staff on responsible AI use.
 - 3. Ensure alignment with AUB's Data Governance Policy, Data Classification standards, and Information Security framework.
 - 4. Clarify how this guidance relates to more specific teaching, research, clinical, and other domain-specific guidance
- (D) This document complements, and does not replace, more specific guidance applicable to teaching and learning, research, clinical operations, student conduct, procurement, data governance, information security, or other specialized areas. Where more specific guidance applies, users should follow that guidance in addition to this framework.
- (E) This is an enabling framework with guardrails, not a restrictive policy.
- (F) These Guidelines are intended to be a living document. They will be reviewed and updated periodically to reflect advances in AI technologies, evolving legal and regulatory requirements, institutional experience, emerging risks, and feedback from the AUB community.

III. DEFINITIONS

Capitalized terms shall have the meaning attributed to them in this section:

- **Artificial Intelligence (AI)** refers to systems designed to perform tasks that normally require human intelligence, such as analysis, language processing, summarization, prediction, or decision support.
- **AI-Assisted Decision-Making** refers to the use of AI to support analysis, recommendations, prioritization, or decisions that may affect individuals, operations, resources, access, services, or institutional outcomes.
- **AI Output** refers to content, analysis, recommendations, summaries, code, or other material generated or assisted by an AI system.

- **Disclosure** refers to a statement or acknowledgment that AI was used in developing, analyzing, drafting, or producing content, where relevant to the audience or context.
- **External AI Tools** refers to public or third-party AI tools that are not managed or approved by AUB for institutional data, such as public versions of ChatGPT, Gemini, Claude, or similar services.
- **Generative AI (GenAI)** refers to AI systems capable of generating new content such as text, images, audio, code, summaries, or structured analysis based on user input.
- **Human Oversight** refers to human review, validation, judgment, and accountability for AI-assisted work before it is used, shared, or relied upon.
- **Institutional Data** refers to data created, collected, processed, or used in connection with AUB activities, including administrative, academic, research, clinical, financial, HR, student, or operational data.
- **Restricted / Regulated Data** refers to non-public or restricted / regulated information that requires protection under AUB policies, legal obligations, contractual commitments, research protocols, or privacy and security requirements.
- **AUB-Approved AI Tools** refer to AI tools that are integrated within institutionally managed or supported platforms and have been reviewed or supported for use within AUB's governance and security framework.

IV. BEFORE USING AI

- (A) Before using AI for university work, you should consider the following:
1. What am I using AI for?
 2. What data, document, or material will I enter into the tool?
 3. Is the data public, restricted, regulated, copyrighted, licensed, or otherwise protected?
 4. Is the tool approved or appropriate for this type of data and use?
 5. Could the output affect a person's rights, grades, access, employment, care, finances, opportunities, or institutional decisions?
 6. Do I need to document or disclose the use of AI?
 7. Which AUB guidance applies in this context: course, research, clinical, administrative, procurement, data governance, or information security?
- (B) The expectations for validation, documentation, and disclosure increase as AI contributes more significantly to the creation of content, analysis, or decisions.
- (C) Data classification, tool approval, and potential impact on individuals or institutional decisions may override the level of AI contribution.

V. PRINCIPLES

- (A) **Human-Centric Use:** AI supports decision-making and does not replace human judgment.
- (B) **Accountability and Responsibility:** Users remain responsible for the accuracy, appropriateness, and impact of AI-assisted outputs.

- (C) **Transparency:** Be appropriately transparent about the use of AI. Transparency may be achieved through disclosure to the intended audience, internal documentation, or both, depending on the significance of AI's contribution and the context of use.
- (D) **Data Protection and Privacy:** Comply with AUB standards for data governance, classification, information security, privacy, and retention.
- (E) **Integrity and Responsible Use: Integrity:** Use AI honestly, ethically, and responsibly while preserving academic, research, professional, clinical, and institutional integrity. AI must not be used to misrepresent authorship, bypass learning or assessment, or compromise institutional trust.
- (F) **Fairness and Bias Awareness:** Review AI outputs for bias, accuracy, representativeness, and appropriateness.
- (G) **Risk Awareness:** Understand risks such as hallucination, prompt injection, data leakage, over-reliance, and inappropriate disclosure.
- (H) **Intellectual Property and Copyright:** Avoid using copyrighted, licensed, proprietary, or third-party material without authorization, and review outputs to reduce the risk of unintentionally reproducing protected content.

VI. TRANSPARENCY AND DISCLOSURE AND DOCUMENTATION

- (A) Transparency is the guiding principle. Depending on the context and the significance of AI's contribution, transparency may be achieved through internal documentation, external disclosure, or both.
- (B) The following guide is intended to help users determine how AI use should be documented or disclosed based on the degree of AI contribution to the final output. It does not override AUB data classification, tool approval, applicable policies, or human oversight requirements.
- (C) Disclosure expectations vary based on the extent to which AI materially influences the final output and the audience affected by that output. Internal working use may require documentation only, while externally shared, consequential, or high-impact outputs may require explicit disclosure.
- (D) Important: A use that appears minimal may still be inappropriate if it involves restricted, regulated, protected, licensed, or otherwise protected information, or if the output could affect individuals or institutional decisions.

Level	Description of AI Use	Human Role	Internal Documentation	Disclosure
Level 1 Minimal Use	AI provides assistance (grammar, spelling, formatting, brainstorming, translation, simple summaries). AI	Human creates and controls the work.	• Optional internal note •	Not required

	does not contribute substantive content.			
Level 2 Moderate Use	AI assists with parts of the work rather than creating its overall structure or primary content such as drafting individual sections, generating ideas, producing tables, summarizing literature, or suggesting improvements.	Human remains the primary author, integrates AI contributions, and validates all content.	• Identify tool used and nature of contribution internally • Retain original AI output where relevant •	Disclose AI-assisted content when appropriate
Level 3 Significant Use	AI provides the foundation for a substantial portion of the work, such as producing the initial draft, primary analysis, structured report, workflow, or presentation that is then substantially reviewed and revised by a human.	Human critically reviews, restructures, validates, and assumes full responsibility for the final output.	• Document validation methods and rationale • Maintain an edit log or version history • Clearly disclose	Required where AI materially contributed to the work
Level 4 Comprehensive Use	AI generates most or nearly all of the content or workflow with only limited human modification, or AI is used to automate significant content	Human provides oversight, ensures compliance, validates outputs, and remains accountable for their use.	• Maintain full documentation, including tools, prompts, and validation steps • Store outputs in institutional repositories where applicable •	Provide explicit disclosure to relevant stakeholders

	generation or decision-support processes.			
--	---	--	--	--

VII. DATA-CENTRIC GOVERNANCE

(A) AI use must align with AUB data classification standards.

Risk Level	Data Type	Examples	AI Usage Guidance
Low	Public	Publicly available documents, public website content, general public information	AI tools may be used freely, provided no restricted or regulated data is introduced.
Medium	Restricted	Internal reports, internal planning documents, non-public operational information, internal teaching support materials	Use with caution. Use AUB-approved tools whenever possible and avoid external tools where the content includes restricted institutional information.
High	Regulated	Student records, patient data, HR data, financial data, restricted research data, unpublished exams or answer keys, student work, confidential submissions	Only use AI in approved environments; external tools are not permitted.

(B) Teaching and learning materials may fall into different risk categories depending on context. Public syllabi or public course descriptions are different from unpublished exams, answer keys, student submissions, copyrighted or licensed content, and confidential course or assessment materials.

(C) Key rule: When in doubt, treat data as regulated or restricted and use only approved environments.

VIII. AUB-APPROVED AI TOOLS

(A) AI-powered agents, workflow automation platforms, copilots, and autonomous systems may improve efficiency and service delivery. However, these technologies must be adopted within approved institutional environments and remain subject to appropriate governance and oversight.

(B) AUB supports the use of AI tools integrated within institutionally managed platforms, including:

1. Microsoft 365 Copilot

2. Cisco Webex AI Assistant
 3. AI capabilities embedded in AUB-supported systems (e.g., Banner, Epic, Moodle)
- (C) These institutional platforms support a growing range of AI-enabled capabilities that can help improve operational efficiency, productivity, and user experience across the university.
- (D) Examples include drafting, summarizing, and refining emails, reports, presentations, and other documents, Meeting transcription, summarization, action-item capture, and follow-up support, Search and knowledge assistance across approved institutional content, Workflow support and productivity assistance within enterprise platforms, AI-enabled features embedded in academic, administrative, and clinical systems as they become available
- (E) These tools ensure:
1. Data remains within AUB-controlled environments
 2. Data is not used for public AI model training
 3. Access is permission-based
 4. Encryption in transit and at rest
 5. Compliance with international standards (e.g., GDPR, ISO 27001, SOC)
- (F) These are the AI tools currently supported by AUB. As the institutional AI toolset evolves, the ITO website will provide updated implementation guidance, including available tools, supported features, and access instructions.
- (G) Use of External AI Tools (e.g., ChatGPT, Gemini, Claude) is allowed only for public data. They must not be used with restricted or regulated data.
- (H) Faculty and staff should prioritize approved enterprise AI and automation platforms over unmanaged tools or personal accounts when implementing AI-enabled workflows, especially when working with institutional data.

IX. PROHIBITED USES

- (A) Entering restricted or regulated data into external AI tools.
- (B) Automating decisions affecting individuals without human oversight.
- (C) Misrepresenting AI-generated or AI-assisted content as fully human-authored where disclosure is required.
- (D) Using AI in ways that violate academic, research, professional, clinical, or institutional integrity requirements.
- (E) Using AI tools in ways that violate applicable intellectual property, copyright, licensing, privacy, or data protection obligations.
- (F) Using personal AI accounts for institutional work involving non-public data.
- (G) Uploading institutional data, prompts, files, outputs, or organizational knowledge into external AI services where such information may be retained, shared, or used for model training.
- (H) Deploying AI agents, automation tools, or autonomous workflows without appropriate authorization, governance, or oversight.
- (I) Circumventing approved AUB AI environments when processing restricted or regulated information.

X. UNIT HEADS RESPONSIBILITIES

- (A) Unit Heads are responsible for ensuring that AI technologies are adopted in alignment with institutional policies, approved platforms, and applicable governance requirements.
- (B) Department leaders should:
 - 1. Promote responsible use of approved enterprise AI tools.
 - 2. Ensure personnel understand applicable data-protection requirements.
 - 3. Coordinate with IT when implementing AI-enabled workflows, agents, or automation solutions.
 - 4. Avoid fragmented adoption of unmanaged AI tools and personal accounts for institutional activities.
- (C) Where appropriate, develop unit specific guidance, procedures, or operating practices that align with these Guidelines and address the unit's particular AI use cases, risks, regulatory obligations, and operational requirements.

XI. RELATIONSHIP TO EXISTING POLICIES

These Guidelines provide recommended practices for the responsible use of AI and do not establish new disciplinary or compliance requirements. Where AI use is governed by applicable AUB policies, procedures, contractual obligations, research ethics requirements, academic integrity rules, information security requirements, or legal and regulatory obligations, those requirements continue to apply. Any concerns arising from the use of AI should be addressed through the relevant institutional processes and responsible offices.
