

Authority

1.1. This Corporate Guidance and Informational Document is issued by the Chief Information Officer pursuant to section 7 of POLICY.ED.2025.01 - UNOPS Legislative Framework Policy, to support the implementation of POLICY.ITG.2026.01 - UNOPS Artificial Intelligence Policy.

Effective date

2.1. This Corporate Guidance and Informational Document is effective from 14 October 2026.

Purpose

3.1. The purpose of this Corporate Guidance and Informational Document is to support the implementation of POLICY.ITG.2026.01 - UNOPS Artificial Intelligence Policy by giving UNOPS personnel practical guidance on the responsible use of artificial intelligence tools in their work.

3.2. This document covers: (a) which AI tools are available at UNOPS and how they are governed; (b) how to work with AI tools safely and effectively day-to-day; (c) how oversight applies to high-stakes decisions; (d) how to report AI-related concerns and incidents.

3.3. Where this document summarises a requirement of the AI Policy, the AI Policy governs.

Table of Content

- Authority (see page 1)
- Effective date (see page 1)
- Purpose (see page 1)
- Chapter 1 - AI tools at UNOPS (see page 2)
 - 1. Approved and non-approved AI tools and features (see page 2)
- Chapter 2 - Working with AI day-to-day (see page 3)
 - 5. Using AI tools (see page 3)
 - 6. Data hygiene: what goes into AI tools (see page 4)
 - 7. Attributing AI assistance in your work (see page 5)
 - 8. When an AI tool produces a problematic output (see page 5)
- Chapter 3 - Risk tiers and high-stakes oversight (see page 7)

Chapter 1 - AI tools at UNOPS

1. Approved and non-approved AI tools and features

4.1. The Approved Tools list in Annex I contains the authoritative and current record of allowed tools, including AI tools, at UNOPS.

4.2. If you want to use an AI tool that is not already on the Approved Tools list, the following applies:

(a) do not use the tool for any UNOPS work purpose until it has been approved; (b) submit a request through the UNOPS Service Point portal¹, describing the tool, its costs, if any, your intended use, the reason why approved AI tools cannot be used, and the type of data you would enter into it, using concrete examples if appropriate; (c) ITG will assess the tool against the criteria in the AI Policy, data handling practices, security controls, and supplier terms, and notify you of the decision; (d) if approved, the tool will be added to the Approved Tools list with applicable conditions noted; (e) if not approved, ITG will explain why and, where possible, suggest an alternative. If your request is urgent, this should be flagged in the initial request.

4.3. Some enterprise platforms and systems include built-in AI features. Before UNOPS procures any such system, ITG must give a written no-objection. This applies whether or not AI is the main purpose of the system.

4.4. Please request a no-objection from ITG before starting the procurement process for the relevant platform or system, ideally at the business-case or requirements stage, so ITG's review can shape the requirements and the questions put to suppliers. The following applies to seeking a no-objection:

- (a) raise the request through the UNOPS Service Point² portal;
- (b) in the request, include the name of the relevant platform or system and proposed supplier(s), the business need, the AI features involved, the data the system would process and its classification (e.g. whether Strictly Confidential or Confidential), who would use it, and the planned contract value and duration;
- (c) ITG checks whether the AI features meet UNOPS requirements for data handling, security, and supplier terms, considers the risk involved, and considers whether an existing approved AI tool

- 9. Working out your Risk Tier (see page 7)
- 10. Beneficiary-affecting decisions (see page 8)
- 11. What meaningful human review means (see page 8)
- 12. Documentation requirements for Tier 2 and Tier 3 decisions (see page 9)
- 13. Reporting concerns and incidents (see page 9)
- Annexes (see page 10)
 - Annex I - Approved Tools list (see page 10)
 - Annex II - Accountability Matrix (see page 10)
 - Annex III - AI Risk Tier quick reference (see page 10)

1. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6808>

2. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6804>

could meet the need;

(d) ITG issues a written no-objection, a no-objection with conditions, or a refusal with reasons. No award decision may proceed until a written no-objection is issued;

(e) ITG records the no-objection and any conditions, and the procuring unit keeps a copy.

Chapter 2 - Working with AI day-to-day

5. Using AI tools

5.1. AI tools generate responses from patterns in their training data and your input, and can produce confident-sounding output that is incomplete, out of date, or simply wrong. Use them where they improve the quality and efficiency of your work, and apply your own judgment when reviewing any AI tool's output.

5.2. To optimize any AI tool's output, apply the following practices:

- (a) write clear and specific prompts; the quality of an AI output is heavily influenced by the quality of the input, so be specific about what you want, what format you need, what constraints apply, and what the output will be used for, and refine your prompt rather than accepting a poor result;
- (b) provide context, because AI tools may not have information on UNOPS, your role, your project, or your specific situation unless you provide this information, so where relevant briefly explain the context, for example the audience, tone, and purpose of the document;
- (c) treat AI output as a draft, never as a final product, so read it critically, check claims, adjust tone, and correct errors, because the output you submit, publish, or act on shall reflect your judgment, and not the AI's generation;
- (d) learn to recognize when AI is not the right tool: while AI is useful for drafting, summarizing, translating, structuring, brainstorming, and processing large volumes of text, it is less reliable for tasks that require precise factual accuracy, current information, deep domain expertise, or nuanced contextual judgment.

5.3. Some AI uses are prohibited, regardless of the AI tool or Risk Tier. Read the list in paragraph 10 of the AI Policy before using AI in procurement, legal or compliance work, human resources,

- Annex IV - AI decision documentation record template (see page 12)
- Annex V - Contacts and reporting paths (see page 13)

investigations, or coding, and see Chapter 3 in this guidance for the oversight that applies to high-stakes decisions.

6. Data hygiene: what goes into AI tools

6.1. The main data hygiene rule is to check the data classification of the information you are about to enter into an AI tool (as set out in the Information Classification Policy), and to check whether that tool is approved for that classification. For example, a list of technical specifications for equipment can usually go in; a list of personnel with personal details cannot without the proper approval.

6.2. The Approved AI tools list at Annex I specifies the data classifications each AI tool is approved to process. If an AI tool is not approved for the classification of the data you want to enter, do not enter it.

6.3. As a practical guide:

- (a) names, job titles, org units and general organizational information are normally classified as Internal and can be entered into AI tools that the Approved Tools list shows as approved for Internal information;
- (b) project-specific operational data, including information about specific countries, partners, or delivery activities, should be assessed before entering into external AI tools, checking the Approved AI Tools list;
- (c) Confidential or Strictly Confidential information shall not be entered into any AI platform unless the Approved Tools list shows the tool as approved for that classification. In practice, this covers most personnel data beyond name and role, for example performance, health, disciplinary, contractual or personal circumstances information. It covers partners' confidential information, meaning information a partner has marked or communicated as confidential, or that is subject to a confidentiality clause in an agreement with that partner. Public information about a partner or project, such as the partner's name or a project description already published by UNOPS or the partner, is not partners' confidential information;
- (d) legal, compliance, or audit materials classified as Confidential or Strictly Confidential are subject to the most restrictive controls, so consult ITG before using AI tools in these contexts.
- (e) personal data is handled according to the classification assigned to it under the Information Classification Policy and the conditions stated for each tool in the Approved Tools list. Personal data about the health, performance, disciplinary record or personal circumstances of an individual is normally classified as Confidential or Strictly Confidential, so section 12.2 of the AI Policy

applies: it may only be entered into a tool that the Approved Tools list shows as approved for that classification. A use case that collects Personally Identifiable Information as part of delivery, for example from communities we serve or applicants, is a Tier 3 use case under section 7.1(f) of the AI Policy and must follow the oversight in Chapter 3.

6.4. Where you are uncertain, enter less data or anonymise and/or redact any portion which may contain Confidential or Strictly Confidential data. You can often get useful AI assistance by describing a situation in general terms rather than entering specific confidential details.

7. Attributing AI assistance in your work

7.1. Disclosure of AI use is mandatory for Tier 2 and Tier 3 use cases: the end users of the output must be told that AI was used, and for Tier 3 the further disclosure requirements in section 12.3 of this guidance apply. This applies whether the output is internal or external.

7.2. Beyond that, UNOPS does not require personnel to attribute AI assistance in every internal working document. As a practical guide:

- (a) for Tier 1 internal working documents, notes and drafts, no specific attribution is required. Even so, do not present substantially AI-generated work as entirely your own, and consider noting AI assistance where it is helpful for colleagues to know;
- (b) for formal reports, briefings or publications submitted to partners or external audiences, AI assistance should be highlighted where it was material to the final work product, using natural and proportionate phrasing, for example “this report was drafted with AI assistance and reviewed by [name or function]”;
- (c) if in doubt, disclose, because transparency is consistent with UNOPS values and builds trust.

8. When an AI tool produces a problematic output

8.1. AI tools make mistakes. An inaccurate, incomplete or poorly reasoned output that you identify during your own review and do not rely on, distribute or act on is not an AI-related incident. Catching it is the human review that sections 7 to 9 of the AI Policy require. An AI-related incident, as defined in section 3.1(d) of the AI Policy, is an event



where the use of an AI tool has caused, or could still cause, harm: a confidentiality or privacy breach, a materially wrong or harmful output that was used, bias or loss of impartiality in a decision, or use of an AI tool in a way that is inconsistent with the AI Policy.

8.2. If you believe an incident has occurred: (a) do not use the output, and do not rely on, distribute, or act on an output you have reason to question; (b) report the issue to your supervisor and to ITG through the UNOPS Service Point³ portal, flagged as an AI incident, giving the AI tool name, a description of the prompt you used or a screenshot if possible, and a description of the problematic output; (c) where the output involves a potential data breach of Confidential or Strictly Confidential information, for example if an AI tool returns information that should not be in its output, report it immediately rather than at the next opportunity to your supervisor and ITG.

8.3. The following are examples of AI-related incidents that must be reported under section 13.1 of the AI Policy:

- (a) Confidential or Strictly Confidential information, or partners' confidential information, was entered into an AI tool not approved for that classification, even if no harm is yet apparent;
- (b) an AI tool returned information in its output that should not have been available to it, for example another user's or organization's data, or UNOPS information appearing in a tool not approved for it;
- (c) an AI-generated summary, analysis, translation or figure containing a material error was relied on in a decision, sent to a partner or published before the error was found;
- (d) an AI tool used to screen, score or rank people, suppliers or communities we serve produced results that appear to favour or disadvantage a group, or produced results that cannot be explained or audited;
- (e) an agentic AI tool took an action that was not intended or not reviewed, such as sending a message, changing or deleting records, or committing code;
- (f) AI was used in a Tier 3 decision without the human review and documentation required by section 7.2 of the AI Policy, or an AI tool not on the Approved Tools list was used for UNOPS work;
- (g) an AI tool produced threatening, discriminatory, defamatory or otherwise harmful content and that content reached other people.

8.4. The following are not AI-related incidents and should not be reported as such: a wrong reference, figure or claim that you spot in review and correct or discard; a draft of poor quality that you rewrite; an AI tool refusing a prompt, running slowly or being unavailable (raise a support request instead); or disagreement with the tone or style of an output.

3. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6811>

8.5. ITG maintains an AI-related incident register and uses incident reports to strengthen AI governance.

8.6. On receiving a report, ITG records the incident in the AI-related incident register, assesses it, and determines whether escalation is required. Where the incident involves a Tier 3 use case, a potential or confirmed breach of Confidential or Strictly Confidential information, or potential harm to an individual, ITG may suspend use of the AI tool or the use case pending assessment. Where the incident involves suspected misconduct, you may report it directly to IAIG, and the Protection against Retaliation Policy applies to that report. ITG will also refer a report it receives to IAIG where it identifies suspected misconduct. Where partner information or requirements are affected, ITG notifies the Partnership and Futures Group (PFG).

Chapter 3 - Risk tiers and high-stakes oversight

9. Working out your Risk Tier

9.1. Some uses of AI tools come with elevated risks and, as such, must be carefully monitored. AI tools should be used with two key considerations in mind: (1) check the Risk Tier before you start, and (2) keep a suitably qualified person in control, who is also tasked with the review of the AI tool's output. Be particularly careful in monitoring the use and output of agentic tools that can act autonomously with little human intervention, because the more a tool acts on its own, the closer the oversight needed.

9.2. Every use of an AI tool falls into one of three Risk Tiers, and the tier sets the oversight you must apply. Annex III is a quick reference you can use to determine the Risk Tier - sections 6 to 9 of the AI Policy give the full framework.

9.3. To identify the nature of your use to the relevant Risk Tier, look at what the output is used for and how sensitive the information is, then match it against the tiers in Annex III. Where a use could sit in two tiers, the higher Risk Tier must be applied.

9.4. If you are unsure which tier applies to your use case, contact ITG through the UNOPS Service Point portal⁴ before proceeding.

4. <https://unops.atlassian.net/servicedesk/customer/portal/1506>

10. Beneficiary-affecting decisions

10.1. Beneficiary-affecting decisions carry two requirements. First, any use where AI output directly informs or supports a decision on the selection, prioritisation or treatment of project communities we serve or vulnerable peoples is a Tier 3 use case under section 7.1(c) of the AI Policy, and the oversight in sections 11 and 12 of this guidance applies. Second, where that use could give rise to discrimination, systemic bias or an violation of recognised human rights, an ethical review is also required before deployment under section 11.2 of the AI Policy. If you are not sure whether the second limb applies, contact ITG through the UNOPS Service Point portal⁵ and ITG will decide whether an ethical review is needed.

11. What meaningful human review means

11.1. The AI Policy requires documented human sign-off for Tier 3 decisions. Meaningful human review means that: (a) the reviewing person has actually read and understood the AI output; (b) the human review is completed by a person with the relevant subject-matter expertise and signed off by the person holding the delegated authority for the decision. These roles may be performed by the same person or, where the person with authority does not hold that expertise, by two persons acting together; (c) the reviewing person has applied independent judgment and has not simply accepted the AI output because it appeared reasonable; (d) if the reviewer disagrees with the AI output, or has concerns about it, those specific concerns are documented.

11.2. Signing a document that was AI-generated without engaging with its substance does not constitute meaningful human review. The accountability for the decision rests with the person who signs off, regardless of how and by whom the analysis was completed.

5. <https://unops.atlassian.net/servicedesk/customer/portal/1506>

12. Documentation requirements for Tier 2 and Tier 3 decisions

12.1. For a Tier 2 decision, keep a short record in the project or case file noting that an AI tool was used, which tool it was, and that you reviewed the output and applied your own judgment. A note in the file or the email trail is enough. Let the end users (the people who receive or are affected by the output) know that AI was used.

12.2. For a Tier 3 decision, complete the AI decision documentation record at Annex IV and keep it in the relevant project, case, or personnel file. The record captures the decision, the tool and what it contributed, who carried out the human review, why the reviewer was satisfied the output could be relied on, and any concerns or changes. Register the use case in the AI Use Case Inventory through ITG if it is not already there.

12.3. For a Tier 3 decision, also tell the end users that AI was used. Where the decision affects identified individuals, disclose the use of AI to them on request. Where you collect or process personal data of people such as communities we serve or applicants, and information protection obligations or partner requirements call for it, inform those individuals that AI is used.

13. Reporting concerns and incidents

13.1. If you encounter a situation in which you believe AI has been used in a way that creates risk, whether for a decision, for a person, for UNOPS, or for partners, report it through the following pathway: (a) raise the concern with your supervisor; (b) contact ITG through the UNOPS Service Point⁶ portal; (c) a concern that an AI tool has been used in a manner inconsistent with the AI Policy, or that one of the situations described in paragraph 8.3 has occurred, is itself an AI-related incident under section 3.1(d) of the AI Policy, and section 8 of this guidance explains how you report it. Report it immediately, rather than at the next opportunity, where it involves a potential breach of Confidential or Strictly Confidential information or potential harm to an individual; (d) if the concern has ethical dimensions, you may also contact the Ethics Office directly.

6. <https://unops.atlassian.net/servicedesk/customer/portal/1506>

13.2. Personnel who raise concerns in good faith are protected from retaliation. The contacts and escalation paths at Annex V set out the right pathway for each type of query.

Annexes

Annex I - Approved Tools list

<https://app-list.itg.unops.org>

Annex II - Accountability Matrix

Annex II - AI Accountability Matrix

Annex III - AI Risk Tier quick reference

Item	Tier 1 - low risk	Tier 2 - medium risk	Tier 3 - high risk
When it applies	General productivity tasks; no confidential data; human reviews output before use	AI materially informs but does not solely determine an outcome; Confidential data; or AI is embedded in an operational workflow	AI directly informs procurement, legal, compliance, financial authorization, or decisions significantly affecting rights or conditions of service, or candidate assessment and selection; substantiation of an allegation of misconduct; beneficiary-affecting decisions; decisions or actions with a direct and significant effect on delivery of a UNOPS project or service to partners or communities we serve; Strictly Confidential data involved; or collection of Personally Identifiable Information as part of delivery

Item	Tier 1 - low risk	Tier 2 - medium risk	Tier 3 - high risk
Classification criteria	Low consequence; no Confidential or Strictly Confidential data; output reviewed before use	Moderate consequence; operational data; AI is one input among several	High consequence; high-stakes domain; output shapes a significant decision; or Strictly Confidential data or the collection of PII is involved, whatever the consequence
Oversight required	Review output before use; apply your judgment	Document that output was reviewed and human judgment applied; inform supervisor; disclose the use of AI to end users	Documented human sign-off by qualified person; complete AI decision documentation record; register use case with ITG; manager notification
Typical examples	Drafting an email; summarizing a document; translating content; brainstorming	Analyzing project data; drafting a partner report; using AI in an operational workflow	Procurement evaluation; legal determination; decisions significantly affecting rights or conditions of service, or candidate assessment and selection; substantiating a misconduct allegation; beneficiary selection

Annex IV - AI decision documentation record template

Field	Detail
Date	
Decision or work product	(Brief description of the decision or output that was AI-assisted)
AI tool used	
Nature of AI contribution	(What did the AI tool do? For example, drafted analysis, generated a classification, summarized data)
Data entered into the AI tool	(General description of data type and classification; do not reproduce confidential content)
Risk Tier assigned	Tier 3
Reviewing person	(Name, role, and functional authority)
Nature of human review conducted	(How did the reviewing person assess the AI output? What was checked? What independent judgment was applied?)
Were there concerns or deviations from the AI output?	(If yes, describe. If no, state "none".)
Final decision or outcome	(Brief description of the decision taken or work product finalized)
Record retained in	(File reference or location)

Field
Detail

ITG use case registration

(Applicable to Tier 3: confirmation that the use case has been registered in the AI Use Case Inventory)

Annex V - Contacts and reporting paths

Query type
Action
Contact

Request to use a new AI tool not on the Approved Tools list

Submit a tool assessment request

UNOPS Service Point portal⁷

Question about which Risk Tier applies to a use case

Submit a Risk Tier query

UNOPS Service Point portal⁸

Technical question about an approved AI tool

Submit a support request

UNOPS Service Point portal⁹

Reporting an AI-related incident (see the examples in paragraph 8.3 of this guidance)

Submit an incident report, flagged as an AI incident

UNOPS Service Point portal;¹⁰ notify supervisor

Reporting an AI-related incident that also involves suspected fraud, misconduct or wrongdoing

Report to IAIG in accordance with the Protection against Retaliation Policy; you may also report to your supervisor and ITG

IAIG

7. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6811>

8. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6804>

9. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6804>

10. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6811>

Query type	Action	Contact
Raising an ethical concern about an AI use case	Contact ITG or the Ethics Office directly	UNOPS Service Point portal ¹¹ or Ethics Office
Requesting support to develop an AI use case	Submit a use case proposal to ITG	UNOPS Service Point portal ¹²
Requesting AI training for your team	Submit a training request	UNOPS Service Point portal ¹³
Submitting feedback on this document or the AI Policy	Submit feedback	UNOPS Service Point portal ¹⁴
General AI questions not covered above	Submit a general query	UNOPS Service Point portal ¹⁵

UNOPS Service Point¹⁶

11. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6804>

12. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6804>

13. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6804>

14. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6804>

15. <https://unops.atlassian.net/servicedesk/customer/portal/1506/group/2988/create/6804>

16. <https://unops.atlassian.net/servicedesk/customer/portal/1506>