



POLICY.ITG.2026.01
UNOPS Artificial Intelligence Policy

Headquarters, Copenhagen

13 Oct 2026

1. Authority

1.1. This Policy is promulgated by the Chief Information Officer (CIO) pursuant to POLICY.ED.2025.01 - UNOPS Legislative Framework Policy, on the basis of a delegation of authority by the Executive Director.

2. Effective date

2.1. This Policy shall become effective on 14 Oct 2026.

[signature redacted]

Tushar Arvind Dighe

Chief Information Officer

1. Purpose

1.1. This Policy establishes the organizational requirements for the responsible, proportionate, and effective use of artificial intelligence (AI) tools by UNOPS personnel in the conduct of UNOPS work and for the appropriate mitigation of risks associated with artificial intelligence.

1.2. This Policy sets the rules, accountabilities, and boundaries required to support the continued and scaled adoption of AI while managing the associated risks.

1.3. UNOPS is committed to using AI tools proportionately, applying them where they add value and having regard to efficiency and environmental impact in the approval and use of AI tools.

2. Application

2.1. This Policy applies to all UNOPS personnel, as defined in section 3, regardless of duty station, modality of engagement, or contract type, where AI tools are used in connection with the performance of UNOPS work.

2.2. This Policy applies to the use of AI tools across all functional areas of UNOPS, including, but not limited to, project delivery, procurement, financial management, human resources, legal and compliance functions, and internal operations.

3. Definitions

3.1. In this Policy, the following terms have the meanings set out below:

(a) **“AI tool”** means any software application, system, or service that uses artificial intelligence techniques - including machine learning, large language models, natural language processing, computer vision, or automated reasoning - to generate outputs, support decisions, or perform tasks. An AI tool may be a standalone application or a feature embedded within a broader software platform or enterprise system. For the avoidance of doubt, standard spelling, grammar, and autocorrect features embedded in office productivity tools do not constitute AI tools for the purposes of this Policy, unless those features perform substantive content generation, analysis, or decision support. Also, for the avoidance of doubt, an AI tool includes an agentic AI tool;

(b) **“AI Use Case Inventory”** means the centralized record, maintained by the Information Technology Group (ITG) in accordance with section 4.4. (b), of registered AI tool use cases at UNOPS, including the Risk Tier assigned to each use case and the approved AI tool that can be used;

(c) **“AI-assisted decision”** means any decision made by UNOPS personnel in which an AI tool was used to generate, analyze, summarize, or otherwise materially inform the content or substance of the decision;

(d) **“AI-related incident”** means any event that arises from the use of an AI tool and results in, or has the potential to result in, one or more of the following: a breach of information confidentiality



or privacy; a materially incorrect or harmful output being relied on, acted on, distributed or otherwise used; a built-in bias or compromise of impartiality in a decision-making process; or the use of an AI tool in a manner otherwise inconsistent with this Policy;

(e) **“agentic AI tool”** means an AI tool that is capable of pursuing a goal by planning and carrying out a sequence of steps, invoking other tools, systems, or services, or otherwise taking actions with limited or no human intervention between the instruction and the outcome. The degree of autonomy of an agentic AI tool is a relevant factor in determining the Risk Tier of a use case involving that tool and the level of human review required;

(f) **“approved AI tool”** means an AI tool that has been assessed by ITG and listed in the approved AI tools list maintained by ITG in accordance with section 4 of this Policy;

(g) **“automated decision”** means a decision that is generated by an AI tool without meaningful human review of the specific outputs on which the decision is based, prior to the decision taking effect;

(h) **“ethical review”** means a documented review of a proposed AI tool use case for potential adverse effects on the rights, dignity, or interests of individuals or communities;

(i) **“human review”** means the meaningful assessment by a qualified UNOPS personnel member of AI-generated outputs prior to their use in a decision or work product, including the exercise of independent judgment as to whether those outputs are accurate, appropriate, and consistent with UNOPS values and obligations. The mere receipt or acknowledgement of an AI-generated output does not constitute human review;

(j) **“partners’ confidential information”** means any information that a partner has designated or communicated as confidential, or that is subject to confidentiality obligations under an agreement with that partner;

(k) **“Risk Tier”** means the classification assigned to a particular AI tool use case under the three-tier framework established in section 6 of this Policy, reflecting the nature of the decision supported and the sensitivity of the information involved;

(l) **“third-party AI platform”** means an AI tool or service provided by an external vendor, accessed by UNOPS personnel via the internet, an application programming interface (API), or a cloud-hosted interface, in circumstances where information entered by the user may be transmitted to and processed by systems outside UNOPS direct technical control;

(m) **“UNOPS personnel”** means all individuals engaged by UNOPS under any modality of employment or contractual engagement, including staff members, individual contractors, retainer contractors, hosted entity personnel, and personnel of project implementation units operating under UNOPS authority, where those individuals use AI tools in connection with UNOPS work;

(n) **“use case”** means a specific activity, task, process, workflow, or decision for which an AI tool is used or proposed to be used in connection with UNOPS work.

3.2. For the definitions of **Public information**, **internal information**, **Confidential information**, **Strictly Confidential information** and **Personally Identifiable information (PII)**, please refer to the Information Classification Policy.

4. Accountability

4.1. UNOPS personnel are responsible for:

- (a) reading this Policy, understanding the requirements it sets for the use of AI tools and discussing how those requirements apply to their role, with the support of their managers;
- (b) using only approved AI tools for work purposes and in accordance with the conditions set out in the approved AI tools list or tools temporarily authorized under section 5.4.;
- (c) using approved AI tools in accordance with the oversight requirements applicable to the Risk Tier of each use, as set out in sections 6 to 9;
- (d) ensuring that information is only entered into AI tools in accordance with this Policy;
- (e) reporting AI-related incidents to their line manager and to ITG in accordance with section 13;
- (f) not using an AI tool to perform work that they are not themselves qualified and competent to perform, unless under the close supervision of a person who holds the relevant qualifications and demonstrable expertise in that area;
- (g) completing mandatory AI literacy training as required by UNOPS.

4.2. Managers are responsible for ensuring that personnel under their authority are aware of and comply with this Policy, and for ensuring that AI tool use within their teams is consistent with the Risk Tier requirements established in this Policy.

4.3. Using an AI tool does not shift accountability for the work completed away from the personnel member who produces it.

4.4. ITG is responsible for the operational governance of AI at UNOPS, including:

- (a) maintaining and updating the approved AI tools list;
- (b) maintaining the AI Use Case Inventory;
- (c) administering the AI risk tiering process established in section 6;
- (d) managing the AI-related incident register;
- (e) conducting or commissioning assessments of AI tools proposed for inclusion in the approved AI tools list;
- (f) conducting or commissioning ethical reviews in accordance with this Policy;
- (g) providing guidance and support to UNOPS personnel on the application of this Policy.

4.5. A detailed accountability matrix setting out roles and responsibilities across all relevant functions is maintained by ITG in the AI Policy Guidance.

5. Approved use of AI tools

5.1. The use of approved AI tools shall be in accordance with this Policy and with the conditions set out in the approved AI tools list, including the Risk Tier or Risk Tiers for which each approved AI tool may be used. A single approved AI tool may be approved for use across more than one Risk Tier.

5.2. UNOPS personnel who wish to use an AI tool not included in the approved AI tools list shall submit a request to ITG, describing the cost, if any, the intended use, the reason why approved AI tools cannot be used for such use and the nature of any information to be processed in the AI tool. ITG shall assess the request in accordance with this Policy and inform the requesting personnel of its decision.

5.3. No enterprise platform or system that contains embedded AI features shall be procured unless ITG has provided a written no-objection. The process for seeking a no-objection is set out in the AI Policy Guidance.

5.4. In exceptional and time-sensitive circumstances, ITG may authorize the temporary use of an AI tool that is not included in the approved AI tools list, pending completion of its assessment, where ITG determines that the proposed use is operationally necessary and that adequate safeguards are in place.

5.5. A temporary authorization shall be documented, limited in scope and duration, and shall specify the permitted use case, applicable Risk Tier, permitted information classification, required human review, and any other conditions or safeguards determined by ITG.

5.6. UNOPS personnel shall enter only the minimum information necessary for the intended purpose into any AI tool, and shall, wherever practicable, anonymize or pseudonymize information before it is entered.

5.7. Practical guidance on working with AI tools in UNOPS operational context, including how to handle AI outputs and how to attribute AI assistance in work products, is provided in the AI Policy Guidance.

6. Oversight requirements - risk tiers

6.1. All uses of approved AI tools in connection with UNOPS work shall be in accordance with the oversight requirements set out below.

6.2. The UNOPS personnel member proposing the use shall classify it into one of three Risk Tiers, based on the decision or output it supports and the sensitivity of the information involved. The Risk Tiers determine the oversight requirements for that use and attach to the use case, not to the AI tool. Where the use falls within a use case type recorded in the AI Use Case Inventory, the member shall apply the tier recorded for that type.

6.3. Where a single use case meets the criteria of more than one Risk Tier, the higher Risk Tier shall apply.

6.4. Where a UNOPS personnel member is uncertain as to the appropriate Risk Tier, they shall consult ITG before proceeding with the use of the AI tool.

6.5. ITG shall maintain a detailed Risk Tiering methodology as an internal management instrument, providing further guidance on the classification of specific use case types. Practical guidance for staff on applying the Risk Tier framework is provided in the AI Policy Guidance.

6.6. Where an approved AI tool is an agentic AI tool, the degree of autonomy with which it acts shall be taken into account in assigning the Risk Tier. The greater the autonomy and the closer the tool's actions are to a consequential decision or action, the higher the applicable Risk Tier and the more stringent the human review requirement.

6.7. ITG shall periodically review each approved AI tool to assess whether it continues to perform consistently with the basis on which it was approved. Tools approved for Tier 3 use cases shall be reviewed at least annually.

7. Tier 3 - high risk

7.1. Tier 3 applies to use cases that attract a high degree of risk, where one or more of the following conditions are met:

- (a) the AI-generated output directly informs or supports a decision relating to any of the following:
 - (i) procurement evaluation, procurement award, or vendor selection;
 - (ii) legal interpretation or compliance determination;
 - (iii) financial authorization;
 - (iv) the substantiation of any allegation of misconduct;
- (b) the AI-generated output directly informs or supports a decision that significantly affects the rights, interests, or conditions of service of UNOPS personnel, or the assessment or selection of candidates for UNOPS positions;
- (c) the AI-generated output directly informs or supports a decision that affects the selection, prioritization, or treatment of the communities we serve or vulnerable people;
- (d) the AI-generated output directly informs or supports a decision or action that has a direct and significant effect on the delivery of a UNOPS project or service to partners or the communities we serve;
- (e) the use case involves Strictly Confidential Information, subject to section 12;
- (f) the use case involves the collection or processing of Personally Identifiable Information as part of delivery.

7.2. The following oversight requirements apply to all Tier 3 use cases:

- (a) an AI-generated output shall not be used in a decision unless a person with relevant subject-matter expertise has conducted human review of the output and a person holding the delegated authority for the decision has documented their sign-off. These roles may be performed by the same person or, where the person with authority does not hold the relevant expertise, by two persons acting together;
- (b) the UNOPS personnel member responsible for the decision shall complete and retain an AI decision documentation record;

- (c) the relevant manager shall be notified of the AI-assisted decision before it is implemented;
- (d) the use case type shall be registered in the AI Use Case Inventory maintained by ITG, if not already registered;
- (e) the use of AI shall be disclosed to the end users, and where the AI-assisted decision directly affects identified individuals, the use of AI shall be disclosed to those individuals upon request;
- (f) where the use case involves collecting or processing PII of individuals such as applicants, and where information protection obligations or partner requirements so require, those individuals shall be informed of the use of AI.

8. Tier 2 - medium risk

8.1. Tier 2 applies to use cases that attract a medium degree of risk, where one or more of the following conditions are met:

- (a) the AI tool processes UNOPS Confidential Information or partners' confidential information, subject to section 12;
- (b) the AI-generated output materially informs, but does not solely determine, an operational decision with consequences for UNOPS delivery, reputation, or partner relationships;
- (c) the AI tool is embedded in an operational system or workflow in a manner that affects how UNOPS work is processed or recorded.

8.2. The following **oversight requirements** apply to all Tier 2 use cases:

- (a) the relevant UNOPS personnel shall document that the AI-generated output underwent human review before any AI-assisted decision was made;
- (b) the relevant UNOPS personnel shall make the relevant manager aware of the use of the AI tool in the relevant workflow;
- (c) the use of AI shall be disclosed to the end users.

9. Tier 1 - low risk

9.1. Tier 1 applies to use cases that attract a low degree of risk, being all use cases where the conditions in sections 7 and 8 are not met. These include general productivity or knowledge work tasks, such as drafting, summarizing, translating, researching, or formatting content.

9.2. Tier 1 use cases are subject to the requirement that the UNOPS personnel member shall review AI-generated output before use and shall not treat those outputs as authoritative without human review.

10. Prohibited uses of AI tools

10.1. The following uses of AI tools are prohibited, regardless of the AI tool involved or the Risk Tier assigned to the use case:

- (a) using AI tools to support procurement evaluation, scoring, or award decisions in a manner that compromises the impartiality, transparency, or auditability of the procurement process, as required under UNOPS procurement policy;
- (b) relying on AI-generated legal, compliance, or regulatory guidance as a final determination, without documented human review by a person with relevant qualifications;
- (c) making automated decisions in matters that significantly affect the rights, interests, conditions of service, or well-being of UNOPS personnel or the communities we serve;
- (d) using AI tools in a manner that violates the UNOPS legislative framework or UNOPS obligations under partner agreements;
- (e) using AI tools in a manner that materially compromises, or is reasonably likely to materially compromise, the rights, safety or dignity of individuals, the intellectual property rights or confidential business information of UNOPS or third parties, or the integrity, impartiality, transparency or auditability of a UNOPS decision-making process;
- (f) relying on an AI tool to determine or substantiate the outcome of an investigation into possible fraud, misconduct, or wrongdoing, without documented human review by a person with the relevant authority;
- (g) using an AI coding tool to produce or modify software code that the UNOPS personnel member would not be competent to produce and to review without the assistance of the AI tool, unless under the close supervision of a person who holds the relevant qualifications and demonstrable expertise in that area.

11. Ethics and human rights

11.1. UNOPS is committed to ensuring that its use of AI tools does not undermine the rights, dignity, safety, security, or interests of the communities it serves, the partners with whom it works, or the individuals who work for or with UNOPS.

11.2. Any AI tool use case that may directly affect the selection, prioritization, scoring, or treatment of communities we serve, vulnerable populations, or individuals in a manner that could give rise to discrimination, systemic bias, or violation of recognized human rights shall be subject to an ethical review before operational deployment.

11.3. The ethical review shall be conducted or commissioned by ITG in consultation with the Ethics Office, the relevant functional lead and, where appropriate, the General Counsel, the Risk and Compliance Group, and the People and Culture Group. The review shall assess:

- (a) the nature and degree of potential risk to affected individuals or groups, including the risk of harm, discrimination or systemic bias;

(b) whether the AI tool's outputs can be explained to affected individuals in terms they can reasonably understand;

(c) the adequacy of human oversight mechanisms and final human decision-making authority for the proposed use case;

(d) whether the proposed use is consistent with UNOPS values, human rights obligations, and applicable UN system ethical frameworks.

11.4. Where an ethical review identifies risks that cannot be adequately mitigated, ITG may impose conditions or refuse the use case, and no use case subject to ethical review shall be deployed until the review has been completed and any required conditions have been met.

11.5. UNOPS personnel who have concerns about the ethical implications of an AI tool use case may raise those concerns with their line manager or ITG.

11.6. ITG shall maintain a record of all ethical reviews conducted under this section as part of the AI Use Case Inventory.

12. Handling of confidential and partner information in AI tools

12.1. UNOPS applies a zero-trust orientation to third-party AI platforms. For the purposes of this Policy, information entered into an AI tool or service provided by an external vendor is considered transmitted outside UNOPS direct technical control, regardless of any vendor representations to the contrary, unless ITG has assessed and specifically approved the information transmission and protection controls applicable to that platform.

12.2. UNOPS personnel shall not enter Confidential or Strictly Confidential Information into any AI tool unless both of the following conditions are met:

(a) the tool is listed in the approved AI tools list as approved for use with such information;

(b) ITG has documented the technical and contractual controls applicable to that information.

12.3. UNOPS personnel shall not enter information that is subject to confidentiality obligations under a partner agreement into any AI tool, unless ITG has specifically approved the tool for that purpose and the partner's applicable information protection requirements have been assessed.

12.4. When using any approved AI tool, UNOPS personnel shall ensure that only the minimum amount of confidential information, strictly confidential information, and partners' confidential information necessary for the intended purpose is entered into the approved AI tool.

13. Incident reporting and escalation

13.1. Any AI-related incident shall be reported by the relevant UNOPS personnel member to their manager and to ITG as soon as practicable after the AI-related incident is identified. The reporting channel is set out in the AI Policy Guidance.



13.2. ITG shall assess the reported AI-related incident and determine whether escalation is required. AI-related incidents that involve any of the following shall be escalated in accordance with escalation procedures:

- (a) Tier 3 use cases;
- (b) potential or confirmed breaches of Confidential or Strictly Confidential Information;
- (c) potential harm to individuals arising from an AI-generated output.

13.3. ITG shall issue a Corporate Guidance and Informational Document setting out the applicable escalation procedures.

13.4. ITG shall maintain an AI-related incident register recording all reported AI-related incidents, the assessments conducted, any identified root causes of the AI-related incident, the actions taken, and any consequential changes to the approved AI tools list, Risk Tiering, or this Policy.

13.5. Where an AI-related incident also involves suspected misconduct, the protections and procedures of the Protection against Retaliation Policy apply to reports made to the Internal Audit and Investigations Group (IAIG) in accordance with that instrument.

13.6. UNOPS personnel who report AI-related incidents to their manager, ITG or IAIG shall not be subject to any reprisals for doing so.

13.7. ITG shall review the AI-related incident register no less than annually to identify patterns, systemic risks, and opportunities to strengthen governance.

14. Alignment with UN system norms

14.1. This Policy shall be read consistently with the applicable UN system instruments and guidance on the governance and ethical use of artificial intelligence, including the Global Digital Compact (2024), the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021), and the Principles for the Ethical Use of Artificial Intelligence in the United Nations System endorsed by the United Nations System Chief Executives Board for Coordination in 2022.

14.2. ITG shall monitor developments in UN system guidance and normative work on AI, including the work of the UN Office for Digital and Emerging Technologies, the Independent International Scientific Panel on Artificial Intelligence, the Global Dialogue on Artificial Intelligence Governance, and relevant inter-agency working groups. ITG shall assess the implications for this Policy of any material developments and shall initiate a review where warranted.

14.3. Where UNOPS receives or develops partner-specific guidance on AI relevant to a particular mandate or operational context, that guidance shall be assessed by ITG and, where appropriate, reflected in updates to the approved AI tools list linked in the AI Policy Guidance.

15. Exceptions

15.1. In accordance with POLICY.ED.2025.01 - UNOPS Legislative Framework Policy, only the Executive Director, the Deputy Executive Director (Management and Policy), and the Chief Information Officer may grant an exception to a requirement of this Policy.



15.2. Any request to ITG for an exception shall be made by the Director or Regional Director of the requesting unit. The request shall be in writing and set out:

- (a) the specific provision of this Policy from which an exception is sought;
- (b) the operational or programmatic justification for the exception;
- (c) the proposed alternative controls or safeguards to be applied instead of the relevant requirement;
- (d) the proposed duration and scope of the exception.

15.3. The CIO shall consider the request and may approve it, reject it, or approve it subject to conditions. The decision shall be recorded in writing by ITG.

15.4. Exceptions shall not be granted routinely and shall be restricted to circumstances where the operational justification is compelling and adequate alternative controls are in place.

15.5. Requests to use an AI tool not currently on the approved AI tools list are addressed under section 5 and do not constitute exceptions to this Policy.