Ref. Ares(2026)6517244 - 29/06/2026

European Union Agency for Cybersecurity (ENISA)
Agamemnonos 14 | Chalandri 15231 | Attiki | Greece | info@enisa.europa.eu | www.enisa.europa.eu

ENISA AI POLICY

PUBLIC VERSION

TABLE OF CONTENTS

1. INTRODUCTION

1.1 BACKGROUND and Scope

Artificial Intelligence (AI) has evolved rapidly over recent years, reshaping how organisations make decisions, provide efficiencies and operate at scale. Following the broader European Commission's AI strategy[1] and similarly to other EU agencies, ENISA wishes to unlock efficiency gains, improve quality, and accelerate digital transformation through the use of AI (from simplification of administrative tasks to the strengthening of ENISA's operations). However, effective AI adoption is only possible when sufficient guidance on the responsible, secure, and aligned use of AI is provided.

For this reason, ENISA adopted in April 2026 its AI Policy with a view to ensure the responsible, secure and trustworthy use of AI within the Agency and in its relations with the stakeholders.

This document is the public version of ENISA's AI Policy, aimed to provide relevant information to all interested parties. ENISA contractors and other third parties involved in ENISA's work, such as members of ENISA's Ad Hoc Working Groups, shall abide by its provisions.

The policy applies in all cases when AI tools are used for professional purposes at the Agency.
It applies to third party AI tools used by ENISA, as well as AI tools developed by or on behalf of ENISA for ENISA's own use.

1.2 LEGAL AND POLICY FRAMEWORK

ENISA complies with the relevant EU legal framework on AI, in particular the AI Act[2] and the Data Protection Regulation for EU institutions (EUDPR)[3]. In addition, this Policy is aligned with the principles for trustworthy AI as presented in the European Commission's High Level Expert Group report[4], as well as the European Commission's policy on AI[5].

This policy builds on the European Commission guidelines on the use of online available generative AI tools. On matters relevant to Intellectual Property Protection (IPR), the Policy should be read in conjunction with the ENISA's IPR policy[6].

[1] See the EU AI continent plan in: https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan; see the EU Apply AI strategy in: https://digital-strategy.ec.europa.eu/en/policies/apply-ai.
[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689.
[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001, https://eur-lex.europa.eu/eli/reg/2018/1725/oj/eng .
[4] High-level expert group on artificial intelligence | Shaping Europe's digital future.
[5] Artificial Intelligence at the Commission - AI@EC.
[6] ENISA IPR POLICY.

1.3 DEFINITIONS

For the scope of this Policy, the definitions of the AI Act apply. Annex 1 provides the ones that are most relevant to ENISA's AI Policy. With regard to the notion of AI systems, it should be noted that the terms "AI tool" and "AI system" are used interchangeably throughout the Policy.

2. GENERAL POLICY RULES

The following policy rules apply to all cases of AI use within the Agency. **All parties subject to this policy** shall comply with these rules when using AI in the performance of tasks on behalf of ENISA.

2.1 AI SYSTEMS CLASSIFICATIONS (AI ACT)

In line with the AI system classification under the AI Act (see Annex 2), the following rules apply.

- ENISA shall in principle **only use AI systems that fall under the "minimal or low risk" level** in relation to the AI Act.
    - All the Use Cases under this Policy (Chapter 3) are considered of minimal or low risk.
- ENISA shall in principle **not use any AI system that poses high-risks**.

Any deviation from the above rule must be explicitly authorised by ENISA.

ENISA shall follow the guidance of the Commission's AI office and EDPS regarding the AI risk assessment and the classification of AI systems.

2.2 AI INPUT

The input provided to AI tools (e.g., user prompts or input data) is essential for the output that is obtained from these tools. Depending on the Use Case and the specific prompt, AI input may create confidentiality breaches or lead to copyright infringements. The following policy rules apply.

1. **EU Classified information must <u>never</u> be used in AI tools.**

2. **Sensitive information related to ENISA or third parties (e.g., Member States, EU entities, private entities, etc.) must <u>not</u> be used as input to AI tools[7].**

    - TLP marked information (TLP: AMBER, TLP: AMBER+STRICT, TLP: RED) and Sensitive-non-classified information – SNC (e.g., ENISA internal sensitive documents, procurement and HR related information, etc.) falls under this category.
    - ENISA financial data of any type whatsoever and information originating from contracts and other legal instruments that are or have been binding on the Agency falls under this category. The same applies to information stemming from offers submitted in the framework of public procurement procedures as well as any other

[7] See also European Commission's Standard c(2025) 3738 final on the security of sensitive non-classified information in AI systems, Artificial Intelligence at the Commission - AI@EC - AI Guide on the principles for the handling of SNC data in AI systems.pdf - All Documents.

type of data that is generally afforded protection as confidential or otherwise privileged.
- Personal data falls under this category (unless it is own personal data of the user who conducts the prompt or information already available in the public).
  This concerns all types of personal data, including images and videos.

3. **All parties subject to this Policy must ensure that no information, data or content protected by third-party intellectual property rights, in particular copyright, is entered into AI tools unless the necessary licence for pre-existing rights or authorisation to do so is in place.**

- Any information that is not owned by the party who conducts the prompting on behalf of ENISA or by ENISA or is not in the public domain must be avoided.
- ENISA public reports or legislative documents (e.g., EU Regulations, Court decisions, etc.) or other publicly available documents or publicly available databases are examples of information sources that can be used freely as AI input.
- Work that is subject to copyright, e.g., scientific articles or books, must not be used as input to AI, including any possible adaptation or translation of copyrighted works, unless the necessary licence for pre-existing rights or authorisation to do so is in place.

2.3 AI OUTPUT

The output of an AI tool may be used in different ways, as provided in the permitted AI Use Cases (Chapter 3). With due consideration to the intended use, the following policy rules apply.

1. **All parties subject to this policy must always critically assess the AI output for any biases or inaccurate information.**

- This includes human verification of the AI output, especially if this is to be used in ENISA works that are aimed for external audience (general public of specific stakeholder groups).

2. **All parties subject to this policy must never directly replicate the AI output in ENISA's public documents, email correspondence or any other form of communication.**

- This point covers any type of AI output, including when AI has been used for simple office support tasks, as well as for editing, proofreading and translation.
- All ENISA public reports must undergo human verification and proofreading before publication, including images, graphs, tables, references and footnotes therein.
- Any data aggregation (including in databases and graph material) conducted with the use of AI must undergo human verification.
- Any source code generated with the use of AI must undergo human verification and testing.

3. **All parties subject to this policy must ensure traceability of their use of AI in their work, where possible.**

- They must ensure that the AI prompts are registered and maintained for traceability, where applicable (e.g., if the results will be used by ENISA).

2.4 TRANSPARENCY

Transparency on the use of AI is essential for all Use Cases. **The use of AI in the context of ENISA works must always be acknowledged.**

- This includes any type of ENISA works[8], such as ENISA public reports, source code of ENISA tools, ENISA infographics, etc.

3. AI USE CASES @ ENISA

3.1 PERMITED AI USE CASES

On the basis of the general AI policy rules (Chapter 2), the **permitted AI Use Cases** within ENISA are presented here below. The list of Use Cases will be monitored and updated by ENISA.

3.1.1 Use case 1: Research & learning

This case represents the use of AI to consolidate information, e.g,. in the form of a literature review, desktop research/stock taking and in order to support understanding or learning on a specific topic. The output of this AI operation may be used only for learning or to support relevant ENISA's work. It may include structuring or summarisation of publicly available information, such as open documents.

🟢 Research & learning with the use of AI is permitted.

3.1.2 Use case 2: Support in standard office tasks

This case represents the use of AI tools for simple day-to-day tasks, such as support in creating drafts of simple emails, editing presentations, reviewing briefings or providing summaries of documents. The AI use in all these cases is only on a supportive role rather than core content generation. The outcome shall always be reviewed and not directly replicated.

🟢 AI support for day-to-day simple office tasks is permitted.

3.1.3 Use case 3: Editorial support in ENISA's public documents

This case represents the use of AI in the development process of ENISA documents to be published or other relevant material, such as ENISA's public reports, infographics, communication material, training material. It includes generation of both text, multimedia or any other relevant public ENISA material.

🔴 Use of AI to create (draft) or draft significant portions of ENISA's public documents is not permitted.

🟡 AI can be used for assistance in initial drafting or support in structuring certain parts of the document with proper validation and acknowledgement.

[8] See more details on ENISA's works categories in the ENISA's IPR policy.

- AI can be used for text editing ensuring that sensitive information is not used as input and with proper validation of the output.
- AI can be used for ENISA public multimedia generation with proper labelling and acknowledgment.
- Reviewing of final drafts of public ENISA documents with the use of AI is permitted.
- Proofreading of final drafts of public ENISA documents with the use of AI is permitted.

3.1.4 Use case 4: Editorial support in ENISA's internal documents

This case represents the use of AI in the development process of internal documents, such as ENISA's corporate documents (e.g., ENISA's policies, decisions, etc.), position documents, internal communication material, etc. It includes generation of both text, multimedia or any other relevant internal material.

- Commission's internal AI tools can be used for assistance in initial drafting or support in structuring certain parts of the document with proper validation and acknowledgement.
- Reviewing, proofreading and translation of internal documents is only permitted with the use of Commission's internal AI tools and with due consideration of the sensitivity of the information.

3.1.5 Use case 5: Support in public data aggregation & analysis

This case represents the use of AI to aggregate information from different public sources (e.g. various reports or raw data in different formats) with a view to provide an analysis or a consolidated output based on the insourced data. It includes use of AI to prepare graphs, plots and tables, to identify trends and patterns from open sources and to motivate relevant conclusions and recommendations.

- Use of AI as the sole method for public data analysis is not permitted.
- AI can be used for plots and graphs to support the narrative of the data analysis.
- Public data aggregation with the use of AI to support data analysis is permitted.

3.1.6 Use case 6: Support in source code generation

This case represents the use of AI to support source code generation, e.g., for platforms or services that are developed by or on behalf of ENISA, either for internal use or for use by external stakeholders.

- AI can be used at initial coding phase for structuring and generating chunks of code with proper validation with the exclusion of specific routines and modules aiming to process sensitive information.
- Testing of ENISA's open-source code with the use of AI is permitted.
- Reviewing of ENISA's open-source code with the use of AI is permitted.
- AI assistance in basic system development and configuration tasks (e.g., scripting, SQL queries) is permitted.

3.2 REQUESTS FOR AI USE CASES

ENISA may accommodate other AI uses cases not explicitly mentioned in p.3.1 of this Policy upon relevant request submitted to the Agency. The request shall be complemented by at least the following information, based on which the Agency will conduct a necessary verification in accordance with its internal procedures.

- Intended purpose
- Data sources (to be fed into the AI tool)
- Expected output
- Recipients of the final result
- AI tool to be used
- Risk assessment (business related)
- Security requirements (if applicable)
- Data protection requirements (if applicable).

4. AI TOOLS @ ENISA

As provided in the definitions (Annex 1), an AI system (or tool) is any type of system that can operate at a certain level of autonomy, exhibits adaptiveness after deployment and generates outputs based on the given input.

For the scope of this Policy, this notion is used to cover both third-party AI tools that are available to ENISA, as well as any AI tool that is fully or partially developed by ENISA or on behalf of ENISA for ENISA's own use.

4.1 THIRD PARTY AI TOOLS

As a general rule, ENISA shall use only third-party AI tools that are explicitly authorised by the Agency.

4.1.1 European Commission tools

The European Commission offers specific AI language tools for translations, summaries, etc[9]. It also offers a general-purpose AI tool (GPT@EC). GPT@EC uses both internal Large Language Models (LLMs) and external ones (cloud based). These tools have been developed under the control of the European Commission and with custom specifications. They are offered under a specific SLA and Data Processing Agreement to ENISA.

The European Commission tools offer the highest level of customisation and control for the Agency and are primarily recommended for use for all permitted Use Cases.

Sensitive information may only be processed with the internal LLMs of the EC tools.

[9] These tools may be considered specialised generative AI in certain cases, but for the purpose of this policy we consider them all as falling under the category of generative AI. For more information, see: Digital Europe - AI-based Multilingual Services

4.1.2 Other third-party AI tools

This category includes third-party off-the-shelf tools, offered freely or under a commercial license.

All parties subject to this policy can only use AI tools in the context of ENISA's works **after prior approval by ENISA**.

All parties subject to this policy must refrain from using personal accounts or free AI tools with the exception of the use of AI for research and learning.

4.2 AI TOOLS DEVELOPED BY ENISA

This section refers to tools that are developed by ENISA or on behalf of ENISA under the control of the Agency, i.e., on infrastructure and/or with the use of AI tools controlled fully or partially by ENISA. Such systems may be developed in house or procured to a contractor.

The development of AI tools by ENISA falls under the general ENISA IT Strategy and Information Security Policy. Security of infrastructure and secure code development environment must in all cases be ensured, including when contractors are used.

New AI tools are developed by ENISA only upon prior approval and on the basis of specific business cases. The relevant guidance of the European Commission on procuring AI systems shall be followed in all cases to ensure compliance with the AI Act.

5. POLICY UPDATE

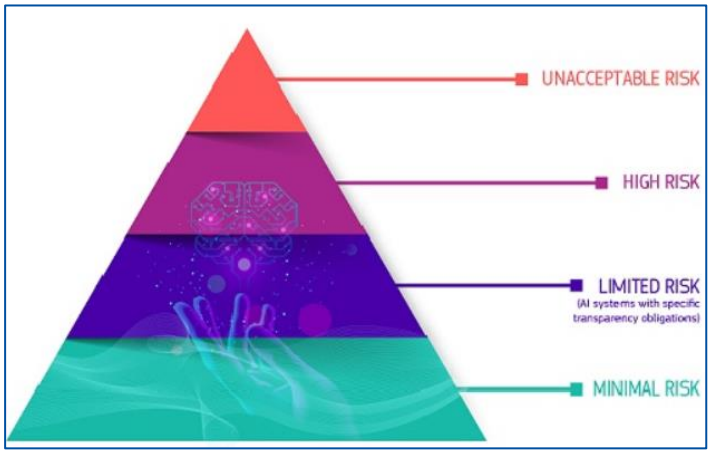
ENISA's AI policy will be reviewed by ENISA bi-annually or earlier if needed to adapt to new or emerging requirements. This public version of the AI policy will be accordingly updated and made available to all interested stakeholders.

ANNEX 1 - DEFINITIONS

Terminology	Description
AI system *(referred also as AI too within this Policy)*	A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments
General-purpose AI mode	An AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market
General purpose AI system *(generative AI applications)*	An AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems
Provider *(of an AI system)*	A natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge
Deployer *(of an AI system)*	A natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.
Input data	Data provided to or directly acquired by an AI system on the basis of which the system produces an output
Training data	Data used for training an AI system through fitting its learnable parameters
Risk	The probability of an occurrence of harm and the severity of that harm

ANNEX 2 – AI SYSTEMS CLASSIFICATION

According to the **AI Act**, a risk-based approach to AI systems classification is applied as shown in the figure below. It is important to stress that the "risk" is defined in the context of the AI Act with regard to harm **to public interests and fundamental rights** that are protected by Union law. Such harm might be material or immaterial, including physical, psychological, societal or economic harm.



Source: EU AI Act – AI system classification[10]

Unacceptable risk relates to AI use cases that pose a clear threat to the safety, livelihoods and rights of people. The use of such systems is prohibited in the EU (Article 5 AI Act).

High risk relates to AI use cases where the AI system can seriously affect the safety or fundamental rights of people. While these systems/uses are not prohibited by default, they must be approached with extreme caution. Providers of high-risk AI systems are subject to strict rules and conditions as mandated in the AI Act (Chapter III). Deployers of high-risk AI systems are also subject to specific obligations for the use of these AI systems, including the conduction of Fundamental Rights Assessments.

Limited risk is relevant to use cases of AI systems that are not high risk, but are still subject to transparency obligations (Chapter IV AI Act). Examples of such systems include chatbots interacting with humans, emotion recognition systems, generative AI that can produce deepfakes, etc.

Minimal or no risk AI systems relate to most routine AI use cases such as spam filters, translation tools, workflow automation tools, etc. The AI Act does not mandate specific obligations to providers and deployers of such systems.

[10] AI Act | Shaping Europe's digital future.