Artificial Intelligence Management System

Artificial Intelligence Policy & Procedure

Conforms to ISO 42001:2023

Document Control

Item	Description			
Document Title:	AIMS Manual			
Doc Ref.	ICESCO-AIMS-DOC01-V01		Version:	01
Classification	¡ Top Confidential	¡ Confidential	□ Internal Use	¡ Public
Status:	Current	**Type:**	Document	
Release Date:	01/12/2024			
Revision Date:	01/12/2024			

Version No.	Date	Author(s)	Position	Remarks
01	01/12/2024	Youssef Stelate	Software Developer	First Version of the Document according to ISO 42001:2023
01	01/12/2024	Amine Chegdali	Artificial Intelligence Manager	Reviewed
01	01/12/2024	Dr Sally Mabrouk	Digital transformation Director	Reviewed

Document Review and Approval History

Version No.	Date	Reviewer(s)	Remarks
01	01/12/2024	Dr Sally Mabrouk	Reviewed

Version No.	Date	Approver(s)	Name	Remarks	Signature
01	01/12/2024	**Digital transformation Director**	Dr Sally Mabrouk	Approved	

Table of Contents

1. Purpose

This policy and procedure express the commitment of ICESCO top management toward implementing an effective Artificial Intelligence Management System.

2. Scope

The scope includes all AI implementation within ICESCO organizational units.

3. Responsibilities

All ICESCO employees are responsible to comply with and implement the content of this policy and procedure.

4. Policy and Procedure

4.1 Introduction

ICESCO recognizes the transformative potential of artificial intelligence (AI) technologies in improving efficiency, innovation, and decision-making across various domains. This policy and procedure establish guidelines to ensure responsible and ethical development, deployment, and use of AI within ICESCO.

4.2 Ethical Principles

ICESCO is committed to upholding the following ethical principles in all AI-related activities:

Transparency: Ensure transparency in the design, development and deployment of AI systems, including disclosure of data sources, algorithms, and decision-making processes, where applicable.

Accountability: Hold individuals and entities accountable for the decisions and actions facilitated by AI systems, with clear allocation of responsibilities and mechanisms for recourse in case of errors or harm.

Fairness: Strive to mitigate biases in AI systems, ensuring fair and equitable outcomes across diverse populations and avoiding discrimination based on race, gender, ethnicity, religion, or other protected characteristics.

Privacy: Respect user privacy rights and safeguard sensitive information throughout the AI lifecycle, adhering to relevant data protection laws and best practices for data anonymization, encryption, and access control.

Safety: Prioritize the safety and well-being of individuals affected by AI systems, implementing robust testing, validation, and monitoring procedures to mitigate risks of physical, financial, or psychological harm.

4.3 Governance and Compliance

ICESCO shall establish a dedicated AI governance structure responsible for overseeing compliance with this policy and procedure, including:

- Appointment of an AI Manager tasked with reviewing AI initiatives, conducting risk assessments, and advising on ethical considerations.
- Integration of AI-related requirements into existing governance frameworks, such as data governance, risk management, and compliance programs.
- Regular audits and assessments to evaluate the effectiveness of AI policies and controls, with adjustments made, as necessary, to address emerging risks and regulatory changes.
- Continually improve and update all AIMS documentation and implementation.
- Comply with all related laws, regulation and any customer/users requirements.

4.4 Data Management

ICESCO shall adhere to the following principles for ethical and responsible data management in AI projects:

Data Quality: Ensure the accuracy, relevance, and representativeness of training data to minimize biases and improve the performance of AI systems.

Data Privacy: Obtain explicit consent for data collection, processing and sharing activities, with clear communication regarding the purpose and scope of data usage.

Data Security: Implement robust security measures to protect data against unauthorized access, breaches, and cyber threats, including encryption, access controls, and regular security assessments.

4.5 Collaboration and Partnerships

ICESCO shall collaborate with external stakeholders, including government agencies, industry partners, and civil society organizations, to advance responsible AI practices and contribute to the development of regulatory frameworks and industry standards.

4.6 Training and Awareness

ICESCO shall provide ongoing training and awareness programs to employees involved in AI-related activities, covering topics such as ethics, bias mitigation, privacy compliance, and cyber security to foster a culture of responsible innovation.

4.7 Review and Revision

This AI policy and procedure shall be reviewed periodically to ensure alignment with evolving ethical standards, technological advancements, and regulatory requirements. Revisions shall be made as necessary to reflect changes in the organizational landscape and emerging risks associated with AI technologies.

4.8 Adaption and Communication

This AI policy and procedure shall be communicated to all employees, contractors, and stakeholders involved in AI-related activities, with acknowledgment of receipt and understanding required upon

adoption. Any updates or amendments to the policy and procedure shall be promptly communicated to affected parties.

4.9 Contact Information

For questions, feedback, or concerns regarding this AI policy and procedure, please contact dt@icesco.org

5. Reference:

Standards	Clause Numbers
ISO 42001:2023	5.2 Policy

6. Related Documents and Forms:

Documents and Forms Name	Documents and Forms Code
-	-

7. PPRC Compliance

Compliance Measurement

The artificial intelligence management team will verify compliance to this policy and procedure through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy and procedure owner.

Exceptions

Any exception to the policy and procedure must be approved and recorded by the artificial intelligence Manager in advance and reported to the Management Review Team.

Non-Compliance

An employee found to have violated this policy and procedure may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy and procedure are updated and reviewed as part of the continual improvement process.