SESEC VI Translation

Translation of Official Interpretation of TC260-005 Ethics-Safety Guidelines for Artificial Intelligence Applications 1.0

May | 2026

Seconded European Standardization Expert in China

(SESEC)

INTRODUCTION:

On 19 May 2026, the National Technical Committee of Cybersecurity (SAC/TC260) publishes a new practice guideline ***TC260-005 Ethics-Safety Guidelines for Artificial Intelligence Applications 1.0*** . The document is a principle-based reference for enterprises, regulators, testing institutions, and industry associations. It addresses ethical and safe AI application in the areas of personal information, automated decision-making, content labeling, algorithm governance, and intellectual property.

The guideline presents the current mainstream AI governance approach to the public, particularly the AI industry. It seeks to reshape industrial practices, correct unethical behavior, and motivate enterprises to adopt the guidelines to reduce compliance risks and build a healthy AI ecosystem serving the public and national interest. For foreign stakeholders, it offers an overview of China's AI governance approach. The document will be updated on a regular basis as AI governance matures.

Original version from TC260's social media: https://mp.weixin.qq.com/s/pgi2C_Fz_haiNObisMOhBg

DISCLAIMER:

This English version is an unofficial translation of the original Chinese document, produced by SESEC for reference purposes only. In the event of any discrepancies between the English and Chinese versions, the Chinese version shall prevail. SESEC accepts no responsibility or liability for any errors, inaccuracies, or misunderstandings arising from this translation.

Official Interpretation of TC260-005 Ethics-Safety Guidelines for Artificial Intelligence Applications 1.0

Issuing Authority:
National Technical Committee on Cybersecurity Standardization (SAC/TC260)
Core Principles:
Benefiting humanity, serving society, and promoting sustainable development

1. Background and Purpose of the Document:

- Rapid Technological Advancements
- Materializing Risks
- A New Phase of Governance

Expected Outcomes: Clarify value-oriented principles, standardize application activities, and support collaborative governance

2. Scope and Target Audience

- App Developers: App development, technological innovation, algorithm iteration, etc.
- Service Provider: Provides services to specific entities
- Application Users: People who use the system, product, or service in their work and daily lives

It can also serve as a reference for relevant regulatory authorities, industry organizations, third-party institutions, and others in advancing governance efforts.

3. Ethical and Safety Implications of Artificial Intelligence Applications

- Impact of Human Dominance: A Challenge to Human Dominance
- Impact on Public Order: Disruption of Basic Public Order
- The Influence of Individual Perceptions and Social Values: Leading to Overreliance and Disconnection
- The Impact of Social Polarization and Discrimination: Amplifying Prejudice and Exacerbating Polarization
- Impact on Life, Health, and Fundamental Rights: Violations of Personal Safety and Privacy
- Sustainable Ecological Impacts: Causing Systemic Ecological Stress

4. Nine Ethical Safety Principles

1) Promoting Human Well-being: Upholding the Principle of “Intelligence for Good” and a People-Centered Approach
2) Respect for the Right to Life: Life Above All Else
3) Upholding Fairness and Impartiality: Eliminating Prejudice and Discrimination
4) Manage Risks Appropriately: Prevent Illegal Activities and Abuse
5) Maintain Openness and Transparency: Clear and Traceable
6) Protecting Privacy and Security: Respecting Privacy Boundaries
7) Ensure Control and Trustworthiness: Control Remains with Humans
8) Agile Co-Governance: Collaborative Co-Governance
9) Inclusive and Shared Benefits: Rejecting Monopolies

5. Core Ethical Safety Guidelines

General Guidelines:

- Minimum Requirements: Maintain human control; prevent data misuse; focus on vulnerable groups.
- Key Scenarios: Life and health, social governance, information and news, knowledge production, and financial activities.

Guidance by Category:

- App Developers: Avoid focusing solely on metrics; exercise extreme caution; ensure transparency and control; and maintain traceability.
- Service Providers: Guarantee the right to opt out; apply data minimization; and establish emergency intervention mechanisms.
- App Users: Use apps rationally; comply with laws and regulations; protect themselves; and fulfill their obligations.

6. Conclusion

Promote balanced development and security, and jointly build a beneficial, secure, and equitable artificial intelligence ecosystem. (Note: Where matters involving personal information, intellectual property, and other related issues are concerned, such provisions must be applied in accordance with applicable laws and regulations.)

Introduction of SESEC Project

The Seconded European Standardization Expert in China (SESEC) is a visibility project co-financed by the European Commission (EC), the European Free Trade Association (EFTA) secretariat and the three European Standardization organizations (CEN, CENELEC and ETSI). Since 2006, there has been four SESEC projects in China, SESEC I (2006-2009). SESEC II (2009- 2012), SESEC III (2014-2017), SESEC IV (2018- 2022) and SESEC V (2022-2025). Dr. Betty XU is nominated as the SESEC expert and will spend the next 36 months on promoting EU-China standardization information exchange and EU-China standardization cooperation.

The SESEC project supports the strategic objectives of the European Union, EFTA and the European Standardization organizations (ESOs). The purpose of SESEC project is to:

- **Promote European and international standards in China;**
- **Improve contacts with different levels of the Chinese administration, industry and standardization bodies;**
- **Improve the visibility and understanding of the European Standardization System (ESS) in China;**
- **Gather regulatory and standardization intelligence.**

The following areas have been identified as sectoral project priorities by the SESEC project partners: Internet of Things (IoT) & Machine-to-Machine(M2M) communication, communication networks & services, cybersecurity & digital identity, Smart Cities (including transport, power grids & metering), electrical & electronic products, general product safety, medical devices, cosmetics, energy management & environmental protection (including eco-design & labeling, as well as environmental performance of buildings).