

网络安全标准实践指南

Guide pratique sur les normes de cybersécurité

——个人用户使用人工智能服务安全指南

Guide de sécurité destiné aux particuliers
pour l'utilisation des services d'intelligence
artificielle

v1.0-202608

全国网络安全标准化技术委员会秘书处

Secrétariat du Comité technique national 260 sur la cybersécurité de
l'Administration chinoise de la normalisation

2026年8月

Août 2026

本文档可从以下网址获得：

Ce document est disponible sur le site web suivant :

www.tc260.org.cn/



全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC



前 言

Avant-propos

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

Les « Lignes directrices pratiques relatives aux normes de cybersécurité » (ci-après dénommées les « Lignes directrices pratiques ») constituent un document technique lié aux normes, élaboré et publié par le Secrétariat du Comité technique national de normalisation en matière de cybersécurité (ci-après dénommé le « Comité de normalisation en matière de cybersécurité »). Elles visent à promouvoir les normes et les connaissances en matière de cybersécurité, et à fournir des lignes directrices pratiques normalisées concernant les lois, les réglementations, les politiques et les normes en matière de cybersécurité, ainsi que les points sensibles et les événements liés à la cybersécurité.

本文件起草单位：北京中关村实验室、北京快手科技有限公司、中国电子技术标准化研究院、中央网信办数据与技术保障中心、工业和信息化部电子第五研究所、北京航空航天大学、东莞市人工智能与数字经济集团有限公司、阿里云计算有限公司、北京天融信网络安全技术有限公司、蚂蚁科技集团股份有限公司、北京金山办公软件股份有限公司、北京智源人工智能研究院。

Le présent document a été rédigé par le laboratoire Zhongguancun de Pékin, la société Beijing Kwai Technology Co., Ltd., l'Institut chinois de normalisation des technologies électroniques, le Centre de soutien aux données et aux technologies du Bureau central du cyberspace, le



Cinquième institut d'électronique du ministère de l'Industrie et des Technologies de l'information, l'Université d'aéronautique et d'astronautique de Pékin, la société Dongguan Artificial Intelligence and Digital Economy Group Co., Ltd., la société Alibaba Cloud Computing Co., Ltd., Beijing Tianrongxin Network Security Technology Co., Ltd., Ant Technology Group Co., Ltd., Beijing Jinshan Office Software Co., Ltd. et l'Institut de recherche en intelligence artificielle de Pékin Zhiyuan.

本文件起草人：刘栋、谷晨、落红卫、马梦娜、余祥臣、刘勇、张妍婷、李芒、张宗洋、罗丽琪、崔栋、申东洋、吴波、王姣、彭骏涛、王龔、林冠辰、欧翹翎、安红云、吕梦、刘颖、杨熙、费凡芮、胡奥迪、张之义、周佳杭、陈海龙。

Auteurs du présent document : Liu Dong, Gu Chen, Luo Hongwei, Ma Mengna, Yu Xiangchen, Liu Yong, Zhang Yanting, Li Mang, Zhang Zongyang, Luo Liqi, Cui Dong, Shen Dongyang, Wu Bo, Wang Jiao, Peng Juntao, Wang Yan, Lin Guanchen, Ou Qiaoling, An Hongyun, Lv Meng, Liu Ying, Yang Xi, Fei Fanrui, Hu Audi, Zhang Zhiyi, Zhou Jiahang, Chen Hailong.





声 明

Déclaration

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

Les droits d'auteur du présent guide pratique appartiennent au Secrétariat du Comité des normes de cybersécurité. Sans l'autorisation écrite du Secrétariat, aucune partie du guide pratique ne peut être copiée ou traduite de quelque manière que ce soit. Veuillez indiquer « Source : Secrétariat du Comité technique national 260 sur la cybersécurité de l'Administration chinoise de normalisation » lors de la reproduction ou de la citation des points de vue et des données contenus dans le présent « guide pratique ».





目 录

Catalogue

1 范围	1
Champ d'application.....	1
2 规范性引用文件	1
Documents de référence normatifs.....	1
3 术语定义	2
Définition des termes	2
4 概述	2
Présentation générale	2
5 安全意识提升	3
Renforcement de la sensibilisation à la sécurité	3
6 安全使用指引	5
Recommandations pour une utilisation en toute sécurité	5
7 使用行为准则	8
Code de conduite d'utilisation.....	8
参考文献	12
Références	12





1 范围

Champ d'application

本文件提供了个人用户通过互联网使用人工智能服务的安全指引，包括安全意识提升、安全使用指引、使用行为准则等。

Le présent document fournit des recommandations de sécurité destinées aux utilisateurs individuels qui utilisent des services d'intelligence artificielle via Internet, notamment des actions de sensibilisation à la sécurité, des consignes d'utilisation sécurisée, des codes de conduite, etc.

本文件适用于指导个人用户安全地通过互联网使用人工智能服务，也可为人工智能服务的技术提供者、服务开发者、服务运营者保障个人用户的安全使用提供参考。

Le présent document a pour objectif de guider les utilisateurs particuliers dans l'utilisation sécurisée des services d'IA sur Internet ; il peut également servir de référence aux fournisseurs de technologies de services d'IA, aux développeurs de services et aux opérateurs de services afin de garantir la sécurité d'utilisation pour les utilisateurs particuliers.

2 规范性引用文件

Documents de référence normatifs

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

Le contenu des documents suivants constitue des clauses essentielles du présent document par le biais de références normatives figurant dans le texte. Parmi ceux-ci, pour les documents référencés comportant une date, seule la



version correspondant à cette date s'applique au présent document ; la dernière version (incluant toutes les modifications) du document référencé ne comportant pas de date s'applique au présent document.

GB/T 25069 信息安全技术术语

GB/T 25069 Terminologie technique relative à la sécurité de l'information

TC260-PG-20266A 网络安全标准实践指南——智能体部署使用安全指引

TC260-PG-20266A Guide de bonnes pratiques en matière de sécurité réseau - Recommandations de sécurité pour le déploiement et l'utilisation d'agents intelligents

3 术语定义

Définition du terme

GB/T 25069 界定的术语和定义适用于本文件。

Les termes et définitions figurant dans la norme GB/T 25069 s'appliquent au présent document.

4 概述

Présentation générale

本文件主要关注个人用户在通过互联网使用人工智能服务时，尤其是利用人工智能技术提供预测、建议、决策，或是生成文本、图片、音频、视频等内容的内容的服务，如何提升安全意识、安全使用服务，并给出了建议的使用行为准则，避免因不当使用人工智能服务对自身或他人产生不利影响。



Le présent document porte principalement sur la manière dont chaque utilisateur peut renforcer sa sensibilisation à la sécurité et utiliser en toute sécurité les services d'intelligence artificielle lorsqu'il y accède via Internet, en particulier ceux qui exploitent les technologies d'IA pour fournir des prévisions, des recommandations, faciliter la prise de décision ou générer du contenu tel que du texte, des images, des fichiers audio et des vidéos. Il propose également des codes de conduite recommandés, visant à éviter tout effet néfaste pour les utilisateurs eux-mêmes ou pour autrui résultant d'une utilisation inappropriée des services d'IA.

5 安全意识提升

Renforcement de la sensibilisation à la sécurité

个人用户在使用人工智能过程中，需要强化安全意识、建立安全理念，包括：

Les utilisateurs individuels doivent renforcer leur sensibilisation à la sécurité et mettre en place des mesures de sécurité lorsqu'ils utilisent l'intelligence artificielle, notamment :

- a) 正确认知人工智能，认识到人工智能的能力具有局限性，可能提供错误信息、出现理解偏差、输出幻觉，或无法按要求完成某些特定任务。

Pour bien comprendre l'intelligence artificielle, il faut reconnaître que ses capacités ont des limites : elle peut notamment fournir des informations erronées, être à l'origine de malentendus, créer des illusions ou se révéler incapable d'accomplir certaines tâches spécifiques comme prévu.

- b) 理性对待人工智能，避免盲目接受和信任人工智能生成的结果，增强对虚假、错误、误导性内容的识别能力。



Il convient d'adopter une approche rationnelle vis-à-vis de l'intelligence artificielle, d'éviter d'accepter et de se fier aveuglément aux résultats qu'elle génère, et de renforcer la capacité à identifier les contenus faux, erronés ou trompeurs.

- c) 适度使用人工智能，将其作为辅助真实生活的工具，避免沉迷依赖，正确认知人工智能情感服务原理，避免通过其过多替代现实交往与真实活动。

Utiliser l'intelligence artificielle avec modération, en tant qu'outil au service de la vie quotidienne, en évitant toute addiction et toute dépendance, en comprenant bien les principes qui régissent les services émotionnels basés sur l'intelligence artificielle, et en évitant qu'elle ne se substitue de manière excessive à la communication et aux activités réelles.

- d) 关注安全风险动态，增强对人工智能安全风险、伦理安全影响的认识，审慎提供隐私信息，意识到人工智能服务可能被恶意利用，例如生成仿冒亲友声音、伪造官方通知等。

Soyez attentifs à l'évolution des risques liés à la sécurité, sensibilisez-vous davantage aux risques de sécurité liés à l'intelligence artificielle et aux questions éthiques qui s'y rapportent. Soyez conscients du risque d'utilisation malveillante des services d'intelligence artificielle, comme la création de fausses voix de proches, la falsification de notifications officielles, et faites preuve de prudence lorsque vous communiquez des informations personnelles.

注：人工智能安全风险可参考《人工智能安全治理框架》，人工智能伦理安全影响可参考 TC260-005《人工智能应用伦理安全指引 1.0》

Remarque : pour ce qui est des risques liés à la sécurité de l'intelligence artificielle, il est possible de se référer au « Cadre de gouvernance en matière de



sécurité de l'intelligence artificielle » ; quant aux implications éthiques et sécuritaires de l'intelligence artificielle, il est possible de se référer à la norme TC260-005 « Lignes directrices éthiques et de sécurité pour les applications d'intelligence artificielle 1.0 ».

6 安全使用指引

Recommandations pour une utilisation en toute sécurité

个人用户在使用人工智能服务过程中，应持续强化安全使用措施，其安全使用指引主要包括：

Les utilisateurs particuliers doivent renforcer en permanence leurs mesures de sécurité lorsqu'ils utilisent des services d'intelligence artificielle.

Leurs consignes d'utilisation en matière de sécurité comprennent notamment :

- a) 使用从正规渠道获取的人工智能服务，优先选用最新版本；涉及生成式人工智能服务的，应选择已通过生成式人工智能服务备案的大模型，不通过来源不明的中转站、未授权代理等方式使用相关服务。

Utilisez des services d'intelligence artificielle provenant de sources légitimes et privilégiez les versions les plus récentes ; en ce qui concerne les services d'intelligence artificielle générative, il convient de choisir des modèles de grande taille enregistrés via ces services, et d'éviter d'utiliser des services provenant de sources inconnues, telles que des plateformes de partage ou des intermédiaires non agréés.

- b) 部署使用智能体时，宜参考 TC260-PG-20266A 《网络安全标准实践指南——智能体部署使用安全指引》，采用适宜的部署方式，并采用相应安全使用的措施。

Lors du déploiement et de l'utilisation d'agents intelligents, il est



recommandé de se reporter au document TC260-PG-20266A « Guide des bonnes pratiques en matière de sécurité réseau – Recommandations de sécurité pour le déploiement et l'utilisation d'agents intelligents », d'adopter des méthodes de déploiement appropriées et de mettre en œuvre les mesures de sécurité correspondantes.

- c) 查看用户协议和隐私协议，了解以下信息并进行相应处置：

Veillez prendre connaissance des conditions d'utilisation et de la politique de confidentialité, comprendre les informations suivantes et prendre les mesures qui s'imposent :

- 1) 人工智能服务的局限性、适用的人群等；

les limites des services d'intelligence artificielle, les populations concernées, etc. ;

- 2) 会被收集的个人信息以及使用方式等，特别关注个人信息是否会被共享等，并检查是否符合最小化收集原则；

Les types de données à caractère personnel qui seront collectées et les modalités de leur utilisation, en accordant une attention particulière à la question de savoir si ces données seront partagées, etc., et afin de vérifier si cela respecte le principe de minimisation lors de la collecte ;

注 1：个人信息收集、使用的要求可参考 GB/T 35273。

Remarque 1 : Les exigences relatives à la collecte et à l'utilisation des données à caractère personnel peuvent se référer à la norme GB/T 35273.

- 3) 个人提供的相关数据是否会被用作训练数据，是否具备撤回同意功能；

Si les données concernées fournies par les personnes concernées seront utilisées comme données d'apprentissage et si celles-ci ont la possibilité de retirer leur consentement ;



4) 投诉举报机制和渠道。

Mécanismes et canaux de signalement des plaintes.

注 2：渠道通常包括但不限于电话、邮件、交互窗口、短信等方式。

Remarque 2 : Les canaux comprennent généralement, sans s'y limiter, le téléphone, l'e-mail, les fenêtres interactives, les SMS et d'autres moyens de communication.

- d) 关注人工智能服务申请的访问权限（如麦克风、摄像头、相册、操作用户文件或数据等），关闭非必要的授权。

Faites attention aux autorisations d'accès demandées par les services d'intelligence artificielle (tels que les microphones, les caméras, les albums photos, l'accès aux fichiers ou aux données de l'utilisateur, etc.) et désactivez celles qui ne sont pas indispensables.

- e) 妥善保管敏感信息，在输入信息过程中，审慎提供隐私信息或敏感个人信息，防范隐私信息、商业秘密等意外泄露或被窃取。

Protégez correctement les informations sensibles, veillez à ne communiquer que avec prudence les informations privées ou les données personnelles sensibles lors de leur saisie, et prévenez toute fuite accidentelle ou tout vol d'informations privées, de secrets d'affaires, etc.

- f) 审慎对待人工智能服务输出的结果：

Approche prudente concernant les résultats fournis par les services d'intelligence artificielle :

- 1) 必要时可通过多个人工智能服务或其他渠道对结果进行交叉验证，检查其中是否存在幻觉、偏见、歧视等错误信息，是否存在伪造冒用等虚假信息；

Si nécessaire, une validation croisée des résultats peut être effectuée à l'aide de plusieurs services d'intelligence artificielle ou d'autres canaux afin de détecter les informations



erronées, telles que les illusions, les préjugés, la discrimination et les falsifications ;

- 2) 对于人工智能服务在法律、医疗、就业、教育、理财等方面的输出结果，仅将其作为参考，在涉及财产、人身安全时应通过其他独立渠道进行核实。

Les résultats fournis par les services d'intelligence artificielle dans des domaines tels que le droit, la santé, l'emploi, l'éducation et la finance ne doivent être utilisés qu'à titre indicatif. Lorsqu'il s'agit de biens et de sécurité des personnes, ces résultats doivent être vérifiés par d'autres sources indépendantes.

- g) 关注开发者提供的安全更新、补丁等，必要时进行安装和升级。

Soyez attentif aux mises à jour de sécurité, correctifs, etc. fournis par les développeurs, et procédez aux installations et mises à jour nécessaires.

- h) 个人权益受损时及时向主管部门或有关机构进行咨询求助或举报。

Lorsque vos droits individuels sont bafoués, consultez sans tarder un professionnel, demandez de l'aide ou signalez les faits au service compétent ou aux institutions concernées.

- i) 如作为未成年人、老年人等用户的监护人，协助其安全使用人工智能服务。

En tant que tuteurs d'utilisateurs tels que les mineurs et les personnes âgées, aidez-les à utiliser en toute sécurité les services d'intelligence artificielle.

7 使用行为准则



Code de conduite d'utilisation

个人用户在使用人工智能服务过程中，应主动约束自身使用行为，相关使用行为规范包括：

Les utilisateurs individuels doivent veiller activement à modérer leur comportement lorsqu'ils utilisent des services d'intelligence artificielle. Parmi les règles de conduite applicables, on peut citer :

a) 合法使用人工智能，尊重他人尊严与合法权益：

Utilisation légitime de l'intelligence artificielle, respect de la dignité ainsi que des droits et intérêts légitimes d'autrui :

1) 不恶意诱导人工智能产生有害行为、输出有害内容；

Ne pas inciter de manière malveillante l'intelligence artificielle à adopter des comportements nuisibles ou à produire des contenus préjudiciables ;

2) 不借助人工智能对他人进行误导、骚扰、操纵；

Ne pas utiliser l'intelligence artificielle pour induire en erreur, harceler ou manipuler autrui ;

3) 不利用人工智能伪造、冒用他人身份或仿冒权威主体；

N'utilisez pas l'intelligence artificielle pour falsifier des documents, usurper l'identité d'autrui ou vous faire passer pour des entités officielles ;

4) 不使用人工智能实施攻击、破坏、盗窃等违法违规行为；

Ne pas utiliser l'intelligence artificielle pour mener des activités illégales et irrégulières telles que des attaques, des actes de destruction et des vols ;

5) 不使用人工智能复刻他人画作、小说、歌曲、影视剧本、商标图案等信息，避免侵犯他人知识产权。

N'utilisez pas l'intelligence artificielle pour reproduire les



peintures, romans, chansons, scénarios de films, motifs de marques déposées et autres informations appartenant à des tiers, afin d'éviter toute atteinte aux droits de propriété intellectuelle d'autrui.

b) 在使用人工智能服务生成合成内容时：

Lorsque vous utilisez des services d'intelligence artificielle pour générer du contenu synthétique :

- 1) 积极履行生成合成内容标识义务，关注相关服务输出内容是否具备生成合成内容标识，不恶意裁剪、删除标识；

Respecter scrupuleusement l'obligation de générer des identifiants de contenu synthétique, vérifier si le contenu produit par les services concernés permet de générer de tels identifiants, et s'abstenir de tronquer ou de supprimer ces identifiants de manière malveillante ;

注：生成合成内容标识的样式见 GB 45438-2025 第 5 章。

Remarque : les règles relatives à la génération d'identifiants de contenu composites figurent au chapitre 5 de la norme GB 45438-2025.

- 2) 如发现生成内容存在准确性、科学性问题的，或包含违法不良信息时，不进行二次传播；

S'il s'avère que le contenu généré présente des problèmes d'exactitude ou d'ordre scientifique, ou qu'il contient des informations illégales ou préjudiciables, il ne sera plus diffusé ;

- 3) 不滥用人工智能输出，如发现模型生成违法不良信息，可通过投诉举报路径反馈至服务提供者，帮助建设良性人工智能生态；

N'abusez pas des résultats fournis par l'intelligence artificielle. S'il s'avère que le modèle génère des informations illégales et préjudiciables, vous pouvez le signaler au fournisseur de



services via la procédure de signalement prévue à cet effet, afin de contribuer à la mise en place d'un écosystème sain en matière d'intelligence artificielle ;

- 4) 在发布人工智能生成合成内容时，遵守发布平台的社区规范或管理要求，主动声明并使用服务提供者提供的标识功能，积极履行内容标识义务。

Lors de la publication de contenus composites générés par l'intelligence artificielle, respectez les normes communautaires ou les exigences de gestion de la plateforme de publication, déclarez activement ces contenus et utilisez la fonction d'identification fournie par le prestataire de services, et remplissez activement votre obligation d'identification des contenus.





参考文献

Références

[1] 人工智能安全治理框架

Cadre de gouvernance en matière de sécurité de l'intelligence artificielle

[2] GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35273 Technologies de la sécurité de l'information —
Spécification relative à la sécurité des données à caractère personnel

[3] GB 45438-2025 网络安全技术 人工智能生成合成内容标识方法

GB 45438-2025 Technologie de sécurité des réseaux — Méthode
d'identification des contenus synthétiques générés par l'intelligence
artificielle

[4] GB/T 45654-2025 网络安全技术 生成式人工智能服务安全基本要求

GB/T 45654-2025 Technologies de sécurité des réseaux – Exigences
fondamentales relatives à la sécurité des services d'intelligence
artificielle générative

[5] TC260-005 人工智能应用伦理安全指引 1.0

TC260-005 Lignes directrices en matière d'éthique et de sécurité pour les
applications d'intelligence artificielle 1.0